Manual Académico para la Instalación y Configuración de Metasploitable3

Resumen: El presente manual detalla de manera exhaustiva el procedimiento para la instalación y configuración de Metasploitable3, una máquina virtual intencionalmente vulnerable diseñada con propósitos educativos en el ámbito de la ciberseguridad. Se abordan los requisitos de software, el proceso de construcción automatizado mediante Vagrant y Packer, y su integración en un entorno de laboratorio controlado para la realización de pruebas de penetración. Este documento sigue un enfoque metodológico paso a paso, proporcionando comandos específicos, solución a errores comunes y las credenciales de acceso por defecto, todo ello enmarcado en un contexto de uso ético y responsable.

Palabras clave: Metasploitable3, Vagrant, VirtualBox, Ciberseguridad, Laboratorio Virtual, Pruebas de Penetración, Hacking Ético.

1. Introducción al Metasploitable3

Metasploitable3 es un proyecto de código abierto desarrollado por Rapid7, la misma organización detrás del conocido Metasploit Framework. Su propósito fundamental es servir como un objetivo de práctica para profesionales y estudiantes de ciberseguridad. A diferencia de sus predecesores, Metasploitable3 no se distribuye como una imagen de máquina virtual (VM) pre-construida, sino como un conjunto de scripts que automatizan su creación. Esto permite una mayor flexibilidad y un entorno más realista que simula un servidor empresarial moderno con múltiples vulnerabilidades intencionales, tanto en su versión basada en Microsoft Windows como en Ubuntu (Rapid7, s.f.).

El uso de Metasploitable3 está estrictamente limitado a entornos de laboratorio aislados y controlados. Su exposición a redes públicas o corporativas representa un riesgo de seguridad significativo debido a sus vulnerabilidades deliberadas. El objetivo de esta herramienta es pedagógico: permitir la práctica de técnicas de escaneo, explotación y post-explotación en un marco legal y ético, fomentando así el desarrollo de habilidades en hacking ético y defensa de sistemas.

2. Requisitos Previos de Software

Para la construcción de Metasploitable3, es indispensable contar con un conjunto de herramientas de virtualización y automatización. A continuación, se detallan los componentes necesarios, sus versiones recomendadas y los enlaces a sus sitios oficiales para su descarga.

- **VirtualBox:** Es el hipervisor sobre el cual se ejecutará la máquina virtual. Se recomienda la última versión estable para asegurar la compatibilidad con los plugins de Vagrant.
    - **Versión recomendada:** 7.0.x o superior.
    - **Fuente oficial:** Oracle Corporation. (s.f.). *Oracle VM VirtualBox*. Recuperado de https://www.virtualbox.org/
- **Vagrant:** Herramienta para la creación y gestión de entornos de desarrollo virtualizados. Vagrant orquesta el proceso de construcción e interacción con la VM.
    - **Versión recomendada:** 2.3.x o superior.
    - **Fuente oficial:** HashiCorp. (s.f.). *Vagrant*. Recuperado de https://www.vagrantup.com/
- **Git:** Sistema de control de versiones distribuido, necesario para clonar el repositorio de Metasploitable3 desde GitHub.
    - **Versión recomendada:** Última versión estable.
    - **Fuente oficial:** Git. (s.f.). *Git*. Recuperado de https://git-scm.com/

3. Descarga del Proyecto Metasploitable3

El primer paso práctico consiste en obtener los archivos de configuración del proyecto desde su repositorio oficial.

3.1. Clonación del Repositorio

Abra una terminal de comandos (o Git Bash en Windows) y ejecute el siguiente comando para clonar el repositorio en su sistema local:

```
git clone https://github.com/rapid7/metasploitable3.git
```

Este comando creará una carpeta denominada metasploitable3 en su directorio actual, conteniendo todos los archivos necesarios.

3.2. Estructura de Carpetas y Archivos

Una vez clonado, es importante comprender la estructura del proyecto:

- **Vagrantfile:** Es el archivo principal de configuración de Vagrant. Define las características de la máquina virtual, como el sistema operativo base, la configuración de red y los scripts de aprovisionamiento que se ejecutarán.
- **scripts/:** Contiene los scripts de aprovisionamiento (en formato Shell o PowerShell) que instalan el software vulnerable y configuran el sistema operativo de la VM.
- **packer/:** Alberga las plantillas de Packer utilizadas para construir las "boxes" o imágenes base de Vagrant, tanto para Windows como para Ubuntu.

4. Instalación de Dependencias Adicionales

Metasploitable3 requiere componentes adicionales para su construcción automatizada, los cuales deben ser instalados por separado.

4.1. Packer

Packer es una herramienta de HashiCorp que automatiza la creación de imágenes de máquinas idénticas para múltiples plataformas a partir de una única configuración. Metasploitable3 lo utiliza para construir la imagen base de la VM.

- **Instalación en Linux (ejemplo con APT para Debian/Ubuntu):**

wget -O- https://apt.releases.hashicorp.com/gpg | sudo gpg --dearmor -o /usr/share/keyrings/hashicorp-archive-keyring.gpg

echo "deb [signed-by=/usr/share/keyrings/hashicorp-archive-keyring.gpg] https://apt.releases.hashicorp.com $(lsb_release -cs) main" | sudo tee /etc/apt/sources.list.d/hashicorp.list

sudo apt update && sudo apt install packer

- **Instalación en Windows:**

    1. Descargue el ejecutable desde la página oficial: HashiCorp. (s.f.). *Install Packer*. Recuperado de https://developer.hashicorp.com/packer/downloads
    2. Descomprima el archivo .zip.
    3. Añada la ruta del ejecutable packer.exe a la variable de entorno PATH del sistema para poder invocarlo desde cualquier terminal.

4.2. Plugins de Vagrant

Vagrant requiere plugins para extender su funcionalidad. Para Metasploitable3, son necesarios los siguientes:

- **vagrant-releoad:** Permite reiniciar la VM durante el aprovisionamiento.
- **vagrant-vbguest:** Gestiona la instalación de las *Guest Additions* de VirtualBox, asegurando una correcta integración entre el sistema anfitrión y el invitado.

Instale estos plugins ejecutando los siguientes comandos en su terminal:

vagrant plugin install vagrant-reload

vagrant plugin install vagrant-vbguest

5. Construcción de la Máquina Virtual

Con todos los prerrequisitos y dependencias instalados, el siguiente paso es construir la máquina virtual. El proceso puede tardar un tiempo considerable (desde 30 minutos hasta varias horas) dependiendo de la velocidad de la conexión a internet y el rendimiento del equipo, ya que implica la descarga de la imagen del sistema operativo y la instalación de todo el software vulnerable.

Navegue hasta el directorio metasploitable3 que clonó previamente.

cd metasploitable3

5.1. Comandos de Construcción con Packer

El primer paso es construir la "box" de Vagrant utilizando Packer.

- **Para construir la versión de Linux (Ubuntu):**

packer build packer/templates/ubuntu-14.04-docker.json

- **Para construir la versión de Windows (Windows Server 2008 R2):**

packer build packer/templates/windows_2008_r2.json

Este proceso generará un archivo con extensión .box en el subdirectorio packer/.

5.2. Añadir la "Box" a Vagrant

Una vez que Packer ha finalizado, debe añadir la "box" generada al inventario de Vagrant.

- **Para la versión de Linux:**

vagrant box add metasploitable3-ubuntu-14.04 packer/metasploitable3-ubuntu-14.04.box

- **Para la versión de Windows:**

vagrant box add metasploitable3-win2k8 packer/metasploitable3-win2k8.box

5.3. Levantar la VM con Vagrant

Finalmente, utilice Vagrant para iniciar y aprovisionar la máquina virtual.

- **Para iniciar la versión de Linux:**

vagrant up ubuntu64

- **Para iniciar la versión de Windows:**

vagrant up win2k8

5.4. Posibles Errores Comunes y Soluciones

- **Error de descarga de la ISO:** Si Packer falla al descargar la imagen ISO del sistema operativo, verifique su conexión a internet. En ocasiones, los enlaces pueden volverse obsoletos; puede ser necesario actualizar la URL en el archivo JSON de Packer correspondiente.
- **Fallo en la instalación de las Guest Additions (vagrant-vbguest):** Asegúrese de tener la versión más reciente de VirtualBox y del plugin vagrant-vbguest. Un desajuste de versiones es la causa más común.
- **Aprovisionamiento interrumpido:** Si el proceso de vagrant up se interrumpe, puede intentar reanudarlo con el comando vagrant provision <nombre_vm>. Si los problemas persisten, es recomendable destruir la VM (vagrant destroy -f) y volver a intentarlo.

6. Configuración y Uso de la Máquina Virtual

Una vez que el comando vagrant up se completa exitosamente, la máquina virtual estará en funcionamiento.

6.1. Ciclo de Vida de la VM con Vagrant

- **Iniciar/Reanudar:** vagrant up <nombre_vm>
- **Detener (apagado seguro):** vagrant halt <nombre_vm>
- **Suspender (guardar estado):** vagrant suspend <nombre_vm>
- **Destruir (eliminar completamente):** vagrant destroy <nombre_vm> (Esta acción es irreversible y eliminará todos los datos de la VM).

6.2. Acceso a la Máquina Virtual

Las credenciales por defecto para acceder a los sistemas son:

- **Metasploitable3 Linux (Ubuntu):**
  - **Usuario:** vagrant
  - **Contraseña:** vagrant
- **Metasploitable3 Windows (Server 2008 R2):**
  - **Usuario:** vagrant
  - **Contraseña:** vagrant

Se puede acceder a la VM a través de la consola de VirtualBox o mediante SSH para la versión de Linux (vagrant ssh ubuntu64).

6.3. Integración en un Laboratorio con Kali Linux

Para crear un entorno de pruebas efectivo, se recomienda configurar las máquinas virtuales (Kali Linux como atacante y Metasploitable3 como objetivo) en la misma red virtual. La configuración más segura y común es una **Red Interna** o **Red NAT** en VirtualBox.

1. **Apague ambas máquinas virtuales.**
2. En la configuración de VirtualBox para cada VM, vaya a la sección "Red".
3. Seleccione un adaptador y configúrelo como "Red Interna". Asigne el mismo nombre de red a ambas máquinas (ej. pentest-lab).

4. Inicie ambas VMs. Se encontrarán en el mismo segmento de red, aisladas del sistema anfitrión y de la red externa, permitiendo que Kali Linux descubra y ataque a Metasploitable3 de forma segura.

7. Conclusión

La correcta instalación y configuración de Metasploitable3 mediante el uso de herramientas de automatización como Vagrant y Packer proporciona a los estudiantes y profesionales de ciberseguridad un entorno de laboratorio robusto, replicable y seguro. Este manual ha delineado el procedimiento técnico de manera formal y estructurada, desde los requisitos iniciales hasta la puesta en marcha y gestión de la máquina virtual. Se reitera que el conocimiento y las técnicas practicadas en este entorno deben ser aplicados siguiendo los más altos estándares éticos, con el objetivo de fortalecer las capacidades defensivas y promover un ciberespacio más seguro.

Referencias

Git. (s.f.). *Git*. Recuperado de https://git-scm.com/

HashiCorp. (s.f.). *Install Packer*. Recuperado de https://developer.hashicorp.com/packer/downloads

HashiCorp. (s.f.). *Vagrant*. Recuperado de https://www.vagrantup.com/

Oracle Corporation. (s.f.). *Oracle VM VirtualBox*. Recuperado de https://www.virtualbox.org/

Rapid7. (s.f.). *rapid7/metasploitable3*. GitHub. Recuperado de https://github.com/rapid7/metasploitable3