FIDE VIRTUAL

Curso introductorio de Ethical Hacking

Semana 01

Profesor: Randall Barnett Villalobos

Aplicación de la etapa de Reconocimiento

Sesión 04

FIDE VIRTUAL

Objetivos del módulo

- Familiarizar al estudiante con el uso del motor de scripting de Nmap (NSE).
- Familiarizar al estudiante con los scripts de Nmap y la instalación de OpenVAS para escanear vulnerabilidades.

Requerimientos iniciales

- Se requiere que el estudiante trabaje con las máquinas virtuales configuradas en la sesión anterior.
- Se requiere que ambas máquinas virtuales puedan comunicarse en red (comprobación con ping).
- Se requiere que le estudiante descargue Ubuntu Desktop (explicación más adelante).
- Se requiere que el estudiante detenga cualquier ejecución de Antivirus o Firewall en su computadora anfitrión, para que estos interrumpan la ejecución normal del laboratorio.

Uso de Nmap Scripting Engine (NSE)

Uso scripts de Nmap para que tu escaneo tenga una mejor performance, al detectar vulnerabilidades.

FIDE VIRTUAL

Uso de scripts

- Nmap es muy reconocida en el mundo de seguridad informática por su funcionalidad de escaneo de redes, puertos y servicios.
- No obstante, la herramienta ha ido mejorando con el correr de los años, ofreciendo cada vez más posibilidades que resultan muy interesantes.

NSE

- El Nmap Scripting Engine (NSE) es una de las características más potentes y flexibles de Nmap. Permite a los usuarios escribir (y compartir) scripts simples para automatizar una amplia variedad de tareas de red.
- Esos scripts han sido diseñados para:
  - Detección de redes
  - Detección de versionamiento de aplicaciones
  - Detección de vulnerabilidades
  - Detección de “puertas traseras” (Backdoors)
  - Explotación de vulnerabilidades

Uso de scripts

- Actualmente Nmap incorpora el uso de scripts para comprobar algunas de las vulnerabilidades más conocidas, por ejemplo:
  - Auth: ejecuta todos sus scripts disponibles para autenticación
  - Default: ejecuta los scripts básicos por defecto de la herramienta
  - Discovery: recupera información del target o víctima
  - External: script para utilizar recursos externos
  - Intrusive: utiliza scripts que son considerados intrusivos para el target
  - Malware: revisa si hay conexiones abiertas por códigos maliciosos o backdoors (puertas traseras)
  - Safe: ejecuta scripts que no son intrusivos
  - Vuln: descubre las vulnerabilidades más conocidas
  - All: ejecuta absolutamente todos los scripts con extensión NSE disponibles

Mira el video

Explicación del uso de NSE.

Instalación de OpenVas

Análisis de vulnerabilidades

FIDE VIRTUAL

Descarga e instalación de Ubuntu

- Deberá descargar Ubuntu Desktop de la siguiente dirección web:
  - https://ubuntu.com/download/alternative-downloads
- Descargue la siguiente versión:
  - Ubuntu 18.04.4 Desktop (64-bit)
- Una vez descargado, abra una sesión en VirtualBox y cree una máquina virtual nueva, de 20Gb de disco duro y 4 Gb de RAM.
- El lugar de instalación y el nombre de la máquina quedan a su criterio. Asegúrese que una vez instalada, que se encuentre en la misma red que Kali Linux y la máquina con Metasploitable.

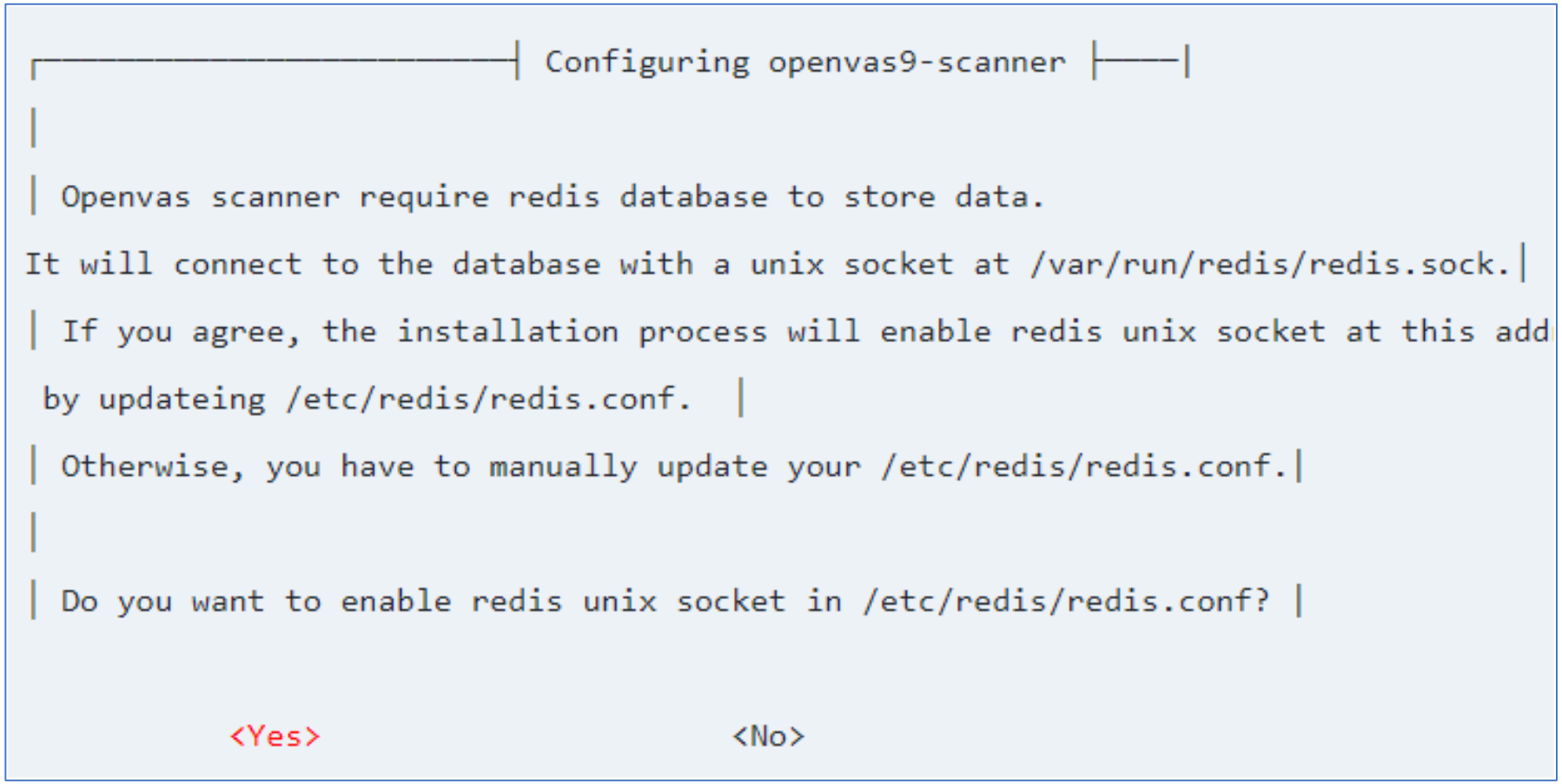
Paso 1: Actualiza Ubuntu

- Antes de instalar paquetes en Ubuntu, se recomienda que primero actualice el sistema. Para hacer eso, ejecuta los siguientes comandos:
  - `sudo apt update`
  - `sudo apt dist-upgrade`

Paso 2: Instalar y configurar OpenVAS

- Para instalarlo, deberá agregar su repositorio a su sistema.
  - `sudo apt-get install software-properties-common`
  - `sudo add-apt-repository ppa: mrazavi / openvas`
- Después de agregar el repositorio, actualice los archivos de Ubuntu e instale OpenVAS con el siguiente comando:
  - `sudo apt-get update`
  - `sudo apt-get install openvas9`
- Durante la instalación, se le pedirá que configure la base de datos Redis para OpenVAS como se muestra a continuación:

Pulse “Yes”


Configuring openvas9-scanner
Openvas scanner require redis database to store data.
It will connect to the database with a unix socket at /var/run/redis/redis.sock.
If you agree, the installation process will enable redis unix socket at this add
by updateing /etc/redis/redis.conf.
Otherwise, you have to manually update your /etc/redis/redis.conf.
Do you want to enable redis unix socket in /etc/redis/redis.conf?
<Yes>
<No>

Paso 2: Instalar y configurar OpenVAS

- Para cumplir con el mensaje de ayuda anterior, instale estos paquetes a continuación:
  - `sudo apt install sqlite3`
  - `sudo apt install texlive-latex-extra --no-install-recommends`
  - `sudo apt install texlive-fonts-recommended`
  - `sudo apt install libopenvas9-dev`

Paso 2: Instalar y configurar OpenVAS

- Después de instalar los paquetes anteriores, ejecute los siguientes comandos para descargar las Pruebas de vulnerabilidad de red de OpenVAS Feed y sincronizar los datos del protocolo de automatización de contenido de seguridad y certificar los datos de vulnerabilidad utilizando los siguientes comandos:
  - `sudo greenbone-nvt-sync`
  - `sudo greenbone-scapdata-sync`
  - `sudo greenbone-certdata-sync`

Paso 2: Instalar y configurar OpenVAS

- Después de eso, reinicie el escáner OpenVAS, OpenVAS GSA y OpenVAS Manager con el siguiente comando:
  - `sudo service openvas-scanner restart`
  - `sudo service openvas-manager restart`
  - `sudo service openvas-gsa restart`
- Para validar si el servicio OpenVAS se está ejecutando, ejecute los siguientes comandos:
  - sudo service openvas-scanner status

```
openvas-scanner.service - LSB: remote network security auditor - scanner
   Loaded: loaded (/etc/init.d/openvas-scanner; generated)
   Active: active (running) since Tue 2020-03-10 10:19:30 CDT; 19s ago
     Docs: man:systemd-sysv-generator(8)
```

Paso 2: Instalar y configurar OpenVAS

- Finalmente, reconstruya la base de datos OpenVAS, para que el administrador pueda acceder a los datos NVT descargados previamente.
  - `sudo openvasmd --rebuild --progress`
- Abra su navegador web y busque el nombre de host del servidor o la dirección IP seguida del puerto:
  - https://localhost:4000
- Eso abrirá el portal OpenVAS. Inicie sesión con el nombre de usuario y contraseña predeterminados:
  - Nombre de usuario: admin
  - Contraseña admin

Conclusión

FIDE VIRTUAL

Conclusión

- Una forma de proteger la información es a través de la identificación, valoración, priorización y corrección de las debilidades identificadas en los activos.
- Esta actividad se conoce como Vulnerability Assessment, y tiene como objetivo encontrar las debilidades en las plataformas de software o hardware para solucionar las fallas, antes de que puedan generar un impacto negativo.

Gracias