Práctica 3

Escáner de detección de puertos y análisis de vulnerabilidades

INDICE

1. OBJETIVO.

El objetivo de esta práctica, es que el alumno se familiarice con la implementación y configuración de técnicas de escaneo de redes y vulnerabilidades. Para la realización de la práctica, el alumno utilizará dos herramientas, Nessus y Nmap, que son software libre, gratuitas y las más potentes existentes en la actualidad.

Para la realización de esta práctica utilizaremos los paquetes oficiales de Nessusd (programa para la detección de vulnerabilidades) para Ubuntu. En los siguientes apartados se indicará como realizar la instalación de paquetes estándar.

Al igual que para Nessus, para Nmap utilizaremos los paquetes oficiales para Ubuntu. En los siguientes apartados se indicará como realizar la instalación estos paquetes estándar.

2. NESSUS.

Nessus es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en nessusd, el daemon Nessus, que realiza el escaneo en el sistema objetivo, y nessus, el cliente (basado en consola o gráfico) que muestra el avance y reporte de los escaneos. Desde consola nessus puede ser programado para hacer escaneos programados con cron.

En operación normal, nessus comienza escaneando los puertos con nmap o con su propio escaner de puertos para buscar puertos abiertos y después intentar varios exploits para atacarlo. Las pruebas de vulnerabilidad, disponibles como una larga lista de plugins, son escritos en NASL (Nessus Attack Scripting Language, Lenguaje de Scripting de Ataque Nessus por sus siglas en inglés), un lenguaje scripting optimizado para interacciones personalizadas en redes.

Opcionalmente, los resultados del escaneo pueden ser exportados en reportes en varios formatos, como texto plano, XML, HTML, y LaTeX. Los resultados también pueden ser guardados en una base de conocimiento para referencia en futuros escaneos de vulnerabilidades.

Algunas de las pruebas de vulnerabilidades de Nessus pueden causar que los servicios o sistemas operativos se corrompan y caigan. El usuario puede evitar esto desactivando "unsafe test" (pruebas no seguras) antes de escanear.

3. NMAP.

Nmap es un programa de código abierto que sirve para efectuar rastreo de puertos TCP y UDP atribuido a Fyodor. Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática.

Sus características principales son:

1. Descubrimiento de servidores: Identifica computadoras en una red, por ejemplo listando aquellas que responden a ping.
2. Identifica puertos abiertos en una computadora objetivo.
3. Determina qué servicios está ejecutando la misma.
4. Determinar qué sistema operativo y versión utiliza dicha computadora, (esta técnica es también conocida como fingerprinting).
5. Obtiene algunas características del hardware de red de la máquina objeto de la prueba (sistema operativo, fecha, hora, ...)

4. INSTALACIÓN DE SOFTWARE.

En este punto se describirá el proceso de instalación y configuración de **Nessus** (nessusd demonio y nessus interfaz gráfico de configuración) y **Nmap** (nmap demonio y nmapfe interfaz gráfico de configuración).

Para la instalación de este software es necesario que el usuario de instalación disponga de permisos de administrador, para el Laboratorio, se utilizara la aplicación **sudo**, que permite ejecutar programas con permisos de administrador cuando el usuario no es administrador.

4.1. Instalación de Nessus.

Para la instalación de nessusd hay que realizar las siguientes tareas:

- Instalación del paquete nessusd

Para la instalación de nessusd, el alumno ejecutará la siguiente línea de configuración

```
# sudo apt-get install nessusd
```

- Instalación del interfaz gráfico

Para la instalación de nessus, el alumno ejecutara la siguiente línea de configuración

```
# sudo apt-get install nessus
```

- Instalación de pluggins de vulnerabilidades

Para la instalación de los pluggins de vulnerabilidades, el alumno ejecutara la siguiente línea de configuración

```
# sudo apt-get install nessus-plugins
```

- Creación de usuario

Para poder acceder al demonio y poder realizar escáneres de vulnerabilidades, es necesario disponer de un usuario definido en nessusd. A continuación se indica el comando a ejecutar para realizar la definición de un usuario, que para el laboratorio será (curso/curso)

```
# sudo nessus-adduser
```

- Arrancar el demonio de Nessus (nessusd)

A continuación se indica el comando a ejecutar para arrancar el demonio nessusd.

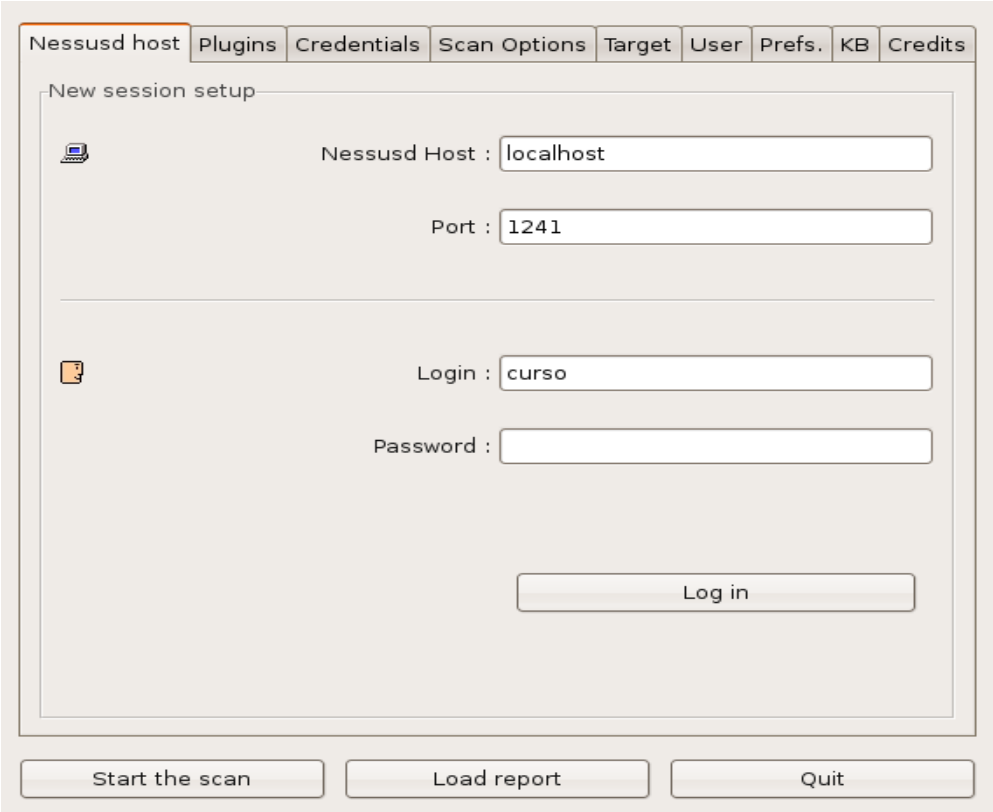
```
# sudo /etc/init.d/nessusd start
```

- Arrancar el interfaz gráfico de configuración (nessus)

A continuación se indica el comando a ejecutar para arrancar el interfaz gráfico de configuración

```
# nessus
```

Una vez ejecutado, nos aparecerá una ventana como la que se muestra a continuación



En esta pantalla, introduciremos el usuario y password definidos, y una vez introducidos, realizaremos el login, si todo es correcto, a partir de este punto estaremos en condiciones de realizar el escaneo de vulnerabilidades.

Se puede encontrar más documentación sobre el proceso de instalación y configuración de Nessus tanto del demonio como del cliente en la URL

http://www.nessus.org/documentation/

4.2. Instalación de Nmap.

Para la instalación de nmap hay que realizar las siguientes tareas:

- Instalación del paquete nmap

Para la instalación de nmap, el alumno ejecutara la siguiente línea de configuración

```
# sudo apt-get install nmap
```

- Instalación del interfaz gráfico (nmapfe)

Para la instalación del interfaz gráfico de configuración, el alumno ejecutara la siguiente línea de configuración

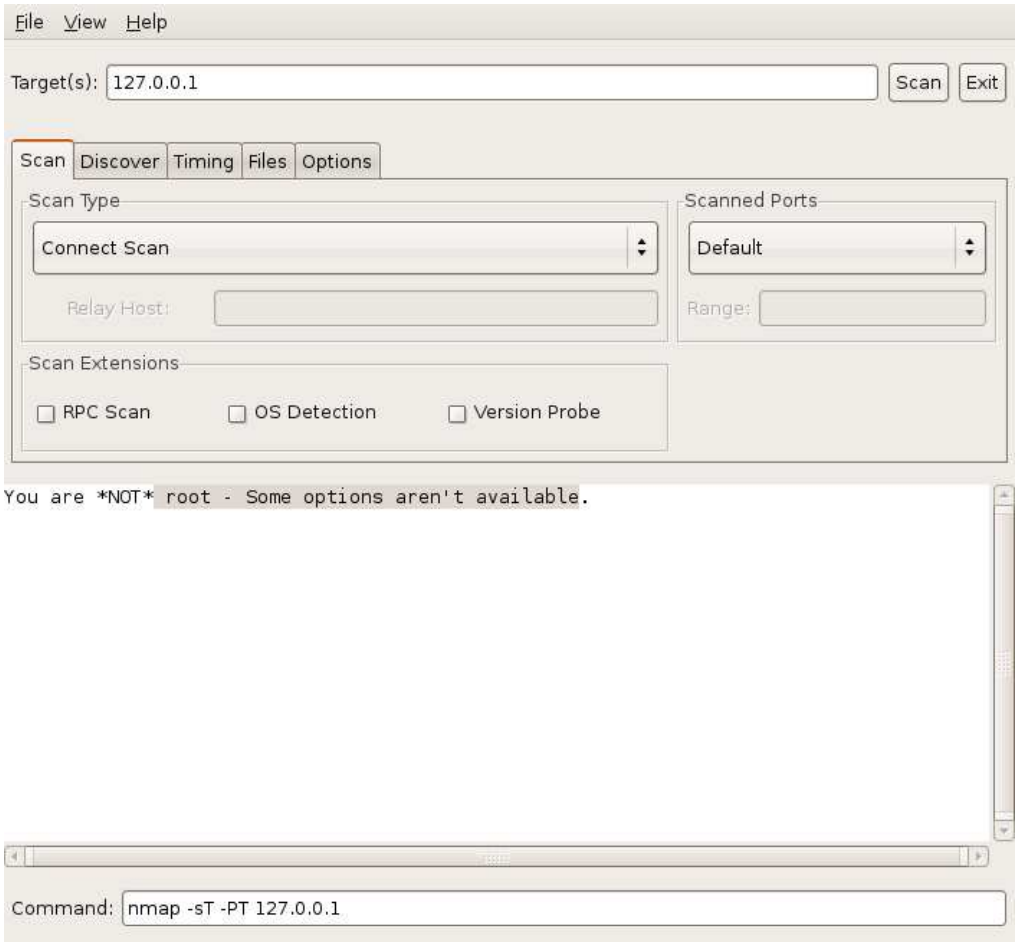
```
# sudo apt-get install zenmap
```

- Arrancar el programa Nmap

A continuación se indica el comando a ejecutar para arrancar el demonio nessusd.

```
# sudo zenmap
```

Una vez ejecutado, nos aparecerá una ventana como la que se muestra a continuación



Se puede encontrar más documentación sobre el proceso de instalación y configuración de nmap en la URL

http://nmap.org/book/man.html

5. DESARROLLO DE LA PRÁCTICA.

5.1. Escáner de red con Nmap.

A continuación se presentan los escaneos a realizar utilizando como herramienta NMAP.

5.1.1. ESCANER DE RED (ICMP).

Utilizando Nmap realizar un escáner “ICMP ECHO” de la red 10.0.12.0/24, y obtener el número de IPs disponibles es esta red.

5.1.2. ESCANER DE RED (SYN TCP).

Utilizando Nmap, realizar un escáner “TCP SYN PING” de la red 10.0.12.0/24, y obtener el número de IPs disponibles es esta red.

5.1.3. ESCANER TCP DE HOST.

Utilizando Nmap y las dos primeras IPs detectadas en el punto5.1.1, realizar un escaneo de puertos TCP de estas dos máquinas, completando una tabla donde se indique dirección IP, puerto, estado del puerto y servicio asociado al puerto.

5.1.4. DETECCIÓN DE SISTEMA OPERATIVO.

Utilizando Nmap, realizar un escaneo de sistema operativo de la red 10.0.11.0/24. Con los datos obtenidos se completará una tabla donde se indiquen dirección IP y sistema operativo que se está ejecutando en la máquina.

5.1.5. ESCANER IPV6.

Utilizando Nmap, realizar un escaneo IPv6 del PC en el que cada alumno se encuentre trabajando, una vez realizado se indicarán las IPv6 disponibles en cada PC.

5.1.6. ESCANER DE SERVIDOR WEB.

Utilizando Nmap, realizar un escaneo de los puertos comprendidos entre el 15 y el 85 de un servidor WEB cualquiera, donde se realice una detección de Sistema Operativo. Con los datos obtenidos se completará una tabla donde se indique, el servidor web, dirección o direcciones IP asociadas, puertos disponibles y Sistema Operativo utilizado por el servidor WEB

.

5.2. Escáner de vulnerabilidades y red con Nessus.

A continuación se presentan los escaneos a realizar utilizando como herramienta Nessus.

5.2.1. ESCANER DE VULNERABILIDADES DE PC.

Utilizando Nessus realizar un escáner de los 1024 primeros puertos de TCP del PC. Con los datos obtenidos, completar una tabla que indique, dirección IP del host, puertos tcp disponibles y riesgos de seguridad detectados por Nessus.

Una vez detectados los riesgos de seguridad, por cada uno de estos, el alumno hará una breve descripción de que consiste el problema, a que son debidos y como pueden ser solucionados.

5.2.2. ESCANER DE VULNERABILIDADES DE SERVIDOR WEB.

Utilizando Nessus, realizar un escaneo de las vulnerabilidades de un servidor WEB cualquiera de los puertos comprendidos entre el 15 y el 85, donde se realice una detección de Sistema Operativo. Con los datos obtenidos se completará una tabla donde se indique, el servidor web, puertos disponibles y Sistema Operativo utilizado, riesgos de seguridad.

Por cada uno de los riesgos de seguridad detectados, el alumno hará una breve descripción de en qué consiste el riesgo, a que es debido y como pueden ser solucionado.

5.2.3. ATAQUE A VULNERABILIDADES DETECTADAS POR NESSUS.

Utilizando la información proporcionada por Nesus y los boletines de seguridad disponibles en internet, indicar para cado uno de los riesgos y agujeros de seguridad detectados en los puntos anteriores, la siguiente información:

1. Identificación del riesgo/agujero de seguridad.
2. Descripción del problema.
3. Exploit disponibles.
4. Solución a los problemas detectados.

6. PRESENTACIÓN Y EVALUACIÓN.

Para la realización de esta práctica, el alumno dispondrá de 2 sesiones de laboratorio, tras las cuales deberá entregar una memoria justificativa con el resultado y la información solicitada en el punto 5. La fecha límite para la entrega de la memoria será la fecha del examen.

7. BIBLIOGRAFÍA.

- **Documentación Nessus**

  http://www.nessus.org/nessus/

- **Nessus Security auditing**

  Author: HD Moore, Jay Beale, Haroon Meer, Roelof Temmingh, Charl Van Der Walt, Renaud Deraison
  ISBN: 1931836086

  http://www.nessus.org/nessus/

- **Nmap**

  http://nmap.org/

- **Seguridad, exploit, vulnerabilidades**

  http://www.securityfocus.com/

  http://cve.mitre.org/

  http://secunia.com/