PONTIFICIA UNIVERSIDAD CATÓLICA MADRE Y MAESTRA

FACULTAD DE CIENCIAS E INGENIERÍA

Sistemas Operativos II

ISC ISC365-101

L7 – Uso de nmap.

Presentado por:

Junior Hernandez 2018-0999 10135069

Entregado a:

Juan Ramón Felipe Núñez Pérez

Fecha de realización:	19 de octubre del 2022
Fecha de entrega:	26 de noviembre del 2022

Santiago de los caballeros; República Dominicana.

Introducción

Nmap es una herramienta que posibilita mapear redes y hacer auditorías de estabilidad y descubrimientos de red. Esta es extensamente usada en toda clase de aplicaciones que van a partir del uso en servidores web hasta el desempeño de redes en una organización.

En esta práctica se va a hacer uso de este instrumento, se explicará cuál es su desempeño y se darán ciertos ejemplos de su uso.

Usaremos esta herramienta para analizar tres redes/maquinas "representativas" del universo. El

profesor no puede especificar tales redes/maquinas, las escoges tu.

En cada caso indicaras al menos:

servicios que se suministran, versiones de algunos servicios, version del sistema operativo, alguna informacion sobre firewall, si se tiene, y penetrar ese firewall, si hay firewall investigar spoofing de direcciones MAC, obtener alguna informacion sobre la red (direcciones ip, servicios, etc) listar servicios Porque ?

udp - si se tienen

Se puede probar con linea de comando o version gui (eje zenmap)

Pero resultados se copian, junto con uso de nmap, en el reporte

Para facilitar el trabajo puedes googlear por ejemplos del uso de nmap y usar algunos de los ejemplos encontrados.

Nmap

Nmap o Network Mapping es una herramienta de código abierto que permite la exploración de redes y la auditoria de seguridad. Fue diseñado para escanear rápidamente cualquier tipo de redes, aunque también puede ser utilizado para escanear hosts solitarios.

A partir de esta herramienta se puede detectar los servicios ofrece la red, que tipo de firewalls están en uso, así como los puertos abiertos, el sistema operativo y algunas características de hardware.

Esta se utiliza generalmente para administrar sistemas y es usado para realizar ataques y tareas de seguridad informática en general. Esta puede ser usada para hacer auditoria de la seguridad de una red mediante la identificación de todo nuevo servidor que se conecte.

Este se encuentra disponible para casi todas las plataformas UNIX y Windows.

Algunas de sus aplicaciones son las siguientes:

- Imprescindibles para todo administrador de sistema, y es usado para pruebas de penetración y tareas de seguridad informática en general.
- Es también una herramienta muy utilizada para hacking.
- Se puede utilizar para verificar la presencia de posibles aplicaciones no autorizadas ejecutándose en el servidor, así como los crackers pueden usarlo para descubrir objetivos potenciales.
- Permite hacer el inventario y el mantenimiento del inventario de computadores de una red.
- Se puede usar entonces para auditar la seguridad de una red, mediante la identificación de todo nuevo servidor que se conecte.
- Nmap es difícilmente detectable, ha sido creado para evadir los Sistema de detección de intrusos (IDS) e interfiere lo menos posible con las operaciones normales de las redes y de las computadoras que son analizadas.

Nmap es una herramienta fantástica en cuanto a todo lo que tiene que ver con escaneo de redes y por ello también puede ser utilizado para hacking ético o con otros fines de seguridad. Su existencia hace que sea peligroso dejar credenciales por defecto en servidores web, routers, FTPs, SSHs, bases de datos.

Para esta practica se estara utilizando una maquina virtual corriendo en VirtualBox con el sistema operativo de Ubuntu de 64 bits.

Probando Nmap:

```
junior@junior-VirtualBox:~$ nmap www.pucmm.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-20 18:27 AST
Nmap scan report for www.pucmm.com (45.33.30.197)
Host is up (0.072s latency).
Other addresses for www.pucmm.com (not scanned): 45.33.18.44 72.14.178.174 96.1
26.123.244 198.58.118.167 173.255.194.134 45.33.2.79 72.14.185.43 45.33.20.235
45.33.23.183 45.79.19.196 45.56.79.23
rDNS record for 45.33.30.197: li1047-197.members.linode.com
Not shown: 997 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 13.20 seconds
```

Cuando ejecuto un escaneo en la red pucmm, además de los puertos http y https, pucmm abre el puerto 22/tcp para construir la red con el servicio Secure Shell y el puerto 8181 para brindar servicios de monitoreo. Tal vez para administrar una red informática para varios laboratorios de la universidad.

```
junior@junior-VirtualBox:~$ nmap www.google.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-20 18:21 AST
Nmap scan report for www.google.com (142.250.217.196)
Host is up (0.074s latency).
Other addresses for www.google.com (not scanned): 2607:f8b0:4008:80a::2004
rDNS record for 142.250.217.196: mia07s61-in-f4.1e100.net
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 8.28 seconds
```

Como puede ver, el uso de nmap apuntando a www.google.com muestra que Google solo abrió dos puertos. 80/tcp para servicios http y 443/tcp para servicios https.

```
junior@junior-VirtualBox:~$ nmap scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-20 18:33 AST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.12s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb
2f
Not shown: 996 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 28.53 seconds
```

Ahora debería ver un escaneo de la red de prueba proporcionada por nmap. En esta red podemos ver que los servicios ssh y http están activos, además de analizar transacciones de paquetes usando el puerto 9929 y usando el puerto 31337 para Elite.

Finalmente, con la red anterior y el sistema operativo y la detección de versión, el escaneo de secuencias de comandos y el parámetro -A de traceroute y -T4 para ejecutarse más rápido:

```
junior@junior-VirtualBox:~$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-20 18:42 AST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.13s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb
2f
Not shown: 996 filtered ports
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; pr
otocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
80/tcp    open  http       Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
9929/tcp  open  nping-echo Nping echo
31337/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nma
p.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.88 seconds
```

Como puede ver, agregamos más información sobre el servicio cuando obtenemos los puertos abiertos. Al igual que con ssh, se basa en OpenSSH y lo encontrarás ejecutándose en Ubuntu. Puede ver http y cómo usa Apache httpd 2.4.7. También podemos ver que el Elite está tcpwrapped. Finalmente, puede ver lo que dije anteriormente que el servidor ejecuta Linux.