Instituto Politécnico Nacional

Unidad Profesional Interdisciplinaria en Ingeniería y Tecnologías Avanzadas

Seguridad de Redes

Profesor. Polanco Montelongo Francisco Antonio

Alumno: Hernández Guzmán Bryan Alexis

Grupo: 3TV4

Práctica: NMAP

Introducción:

Nmap es una utilidad completamente gratuita y de código abierto, nos permite descubrir redes y host, así como realizar auditoría de seguridad. Este programa es compatible con sistemas operativos Linux, Windows y también macOS, pero en todos ellos se utiliza a través de la línea de comandos, aunque tenemos la posibilidad de instalar ZenMap que es la utilidad gráfica de Nmap para hacer los escaneos de puertos a través de la interfaz gráfica de usuario. Si no quieres pelearte con comandos a través de consola, esta interfaz gráfica de usuario te podría ser útil para los primeros pasos con este gran programa, no obstante, cuando tengas más experiencia seguramente ejecutes todas las órdenes directamente desde terminal.

Descripción:

Nmap nos permite detectar hosts de una red local, y también a través de Internet, de esta forma, podremos saber si dichos hosts (ordenadores, servidores, routers, switches, dispositivos IoT) están actualmente conectados a Internet o a la red local. Esta herramienta también permite realizar un escaneo de puertos a los diferentes hosts, ver qué servicios tenemos activos en dichos hosts gracias a que nos dirá el estado de sus puertos, podremos saber qué sistema operativo está utilizando un determinado equipo, e incluso podremos automatizar diferentes pruebas de pentesting para comprobar la seguridad de los equipos.

Elaboración:

Utilizamos ifconfig para conocer la ip y la mascar de red de nuestra maquina virtual:

```
bryan@bryan-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::c20:4827:7fba:8988  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:48:48:28  txqueuelen 1000  (Ethernet)
        RX packets 449549  bytes 642683340 (642.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 107729  bytes 6807693 (6.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Bucle local)
        RX packets 14646  bytes 3606585 (3.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14646  bytes 3606585 (3.6 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Aquí primeramente hacemos la prueba sin meter la ip y la mascara de red de nuestra máquina para visualizar los hosts y se puede observar que no hay ninguno levantado, por obvias razones.

Después se procede a meter la ip y la máscara de subred y puede visualizar desde donde estoy conectado además de ver las 256 direcciones ip y un host levantado

```
bryan@bryan-VirtualBox:~$ nmap -sn
Starting Nmap 7.80 ( https://nmap.org ) at 2023-01-07 05:17 CST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.00 seconds
bryan@bryan-VirtualBox:~$ nmap -sn 10.0.2.15/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-01-07 05:20 CST
Nmap scan report for bryan-VirtualBox (10.0.2.15)
Host is up (0.00096s latency).
Nmap done: 256 IP addresses (1 host up) scanned in 3.36 seconds
```

Al agregar sudo al comando, quí podemos observar que cambiar de 1 a 4 host levantados debido a un escaneo más preciso

```
bryan@bryan-VirtualBox:~$ sudo nmap -sn 10.0.2.15/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-01-07 05:21 CST
Nmap scan report for _gateway (10.0.2.2)
Host is up (0.00024s latency).
MAC Address: 52:54:00:12:35:02 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00026s latency).
MAC Address: 52:54:00:12:35:03 (QEMU virtual NIC)
Nmap scan report for 10.0.2.4
Host is up (0.00022s latency).
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)
Nmap scan report for bryan-VirtualBox (10.0.2.15)
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.05 seconds
```

Conclusión:

En esta practica pudimos observar la ejecución de este comando, reconozco la importancia de esto, sin embargo igual hay que reconocer la responsabilidad que hay al usar este tipo de comandos ya que como la propia historia lo dice puede ser utilizado como fines maliciosos, sin embargo, el uso responsable de este, nos otorga una mejor visualización de lo que nos podemos encontrar si hubiese el caso en que tengamos que reparar alguna cosas o que pueda haber algún problema de ciberseguridad, para todo esto puede ser de mucha utilidad.

Referencias:

https://www.redeszone.net/tutoriales/configuracion-puertos/nmap-escanear-puertos-comandos/