root@computaxion:~# nmap Nmap 7.80 (https://nmap.org)

hola una vez más, en este vídeo vamos a utilizar la herramienta número uno, cuando se trata de escaneos, como ven yo voy a trabajar con la versión 7.8, que ya viene instalada dentro de kali Linux, en este vídeo vamos a utilizar algunos comandos como referencia para aprender a utilizarla, cabe destacar que nmap es una herramienta muy amplia y sería imposible mostrar todos los comandos que trae, por ende vamos a utilizar alguno de ellos para ver su potencial y a la vez tratar de completar la primer fase la cual se trata de escaneo y recolección de información. Para poder realizar el siguiente pasó que es intentar explotar una máquina.

Con nmap puede escanear una simple ip o un rango completo de ip, como también puede escanear un host o puede usar un archivo con varias direcciones ip, también puede generar archivos de todo lo que valla escaneando, también puede excluir un rango de ip, y muchas cosas más.

Lo primero será ejecutar el comando nmap para ver las opciones que nos brinda.

root@computaxion:~# nmap

Nmap 7.80 (https://nmap.org)

Usage: nmap [Scan Type(s)] [Options] {target specification}

TARGET SPECIFICATION:

Can pass hostnames, IP addresses, networks, etc.

Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254

-iL <inputfilename>: Input from list of hosts/networks

-iR <num hosts>: Choose random targets

--exclude <host1[,host2][,host3],...>: Exclude hosts/networks

--excludefile <exclude\_file>: Exclude list from file

HOST DISCOVERY:

Hay más opciones pero se las dejo resumidas

Lo segundo que vamos a hacer es escanear toda la red para elegir un objetivo a analizar./ rango de ip

root@computaxion:~# nmap 192.168.171.0/24

Starting Nmap 7.80 (https://nmap.org) at 2019-09-15 11:55 EDT

Nmap scan report for 192.168.171.1

Host is up (0.00069s latency).

Not shown: 996 filtered ports

PORT STATE SERVICE

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

2869/tcp open icslap

MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.171.2

Host is up (0.00030s latency).

Not shown: 999 closed ports

PORT STATE SERVICE

53/tcp open domain

MAC Address: 00:50:56:F3:A1:03 (VMware)

Nmap scan report for 192.168.171.129

Host is up (0.00076s latency).

Not shown: 991 closed ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

139/tcp open netbios-ssn

143/tcp open imap

443/tcp open https

445/tcp open Microsoft-ds

5001/tcp open commplex-link

8080/tcp open http-proxy

8081/tcp open blackice-icecap

MAC Address: 00:0C:29:51:79:D9 (VMware)

Nmap scan report for 192.168.171.165

Host is up (0.00070s latency).

Not shown: 991 closed ports

PORT STATE SERVICE

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open Microsoft-ds

49152/tcp open unknown

49153/tcp open unknown

49154/tcp open unknown

49155/tcp open unknown

49156/tcp open unknown

49157/tcp open unknown

MAC Address: 00:0C:29:EC:45:1E (VMware)

Nmap scan report for 192.168.171.169

Host is up (0.00081s latency).

Not shown: 994 closed ports

PORT STATE SERVICE

81/tcp open hosts2-ns

111/tcp open rpcbind

139/tcp open netbios-ssn

445/tcp open Microsoft-ds

2049/tcp open nfs

8080/tcp open http-proxy

MAC Address: 00:0C:29:46:71:3A (VMware)

Nmap scan report for 192.168.171.254

Host is up (0.00029s latency).

All 1000 scanned ports on 192.168.171.254 are filtered

MAC Address: 00:50:56:E3:E7:9E (VMware)

Nmap scan report for 192.168.171.166

Host is up (0.000013s latency).

Not shown: 999 closed ports

PORT STATE SERVICE

111/tcp open rpcbind

Nmap done: 256 IP addresses (7 hosts up) scanned in 22.44 seconds

Ahora vamos a intentar obtener el tipo de sistema operativo que están usando esas máquinas, /maquina windows7

root@computaxion:~# nmap -O 192.168.171.165

Starting Nmap 7.80 (https://nmap.org) at 2019-09-15 14:54 EDT

Nmap scan report for 192.168.171.165

Host is up (0.00037s latency).

Not shown: 991 closed ports

PORT STATE SERVICE

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open Microsoft-ds

49152/tcp open unknown

49153/tcp open unknown

49154/tcp open unknown

49155/tcp open unknown

49156/tcp open unknown

49157/tcp open unknown

MAC Address: 00:0C:29:EC:45:1E (VMware)

Device type: general purpose

Running: Microsoft Windows 7|2008|8.1

OS CPE: cpe:/o:microsoft:windows\_7::- cpe:/o:microsoft:windows\_7::sp1 cpe:/o:microsoft:windows\_server\_2008::sp1 cpe:/o:microsoft:windows\_server\_2008:r2 cpe:/o:microsoft:windows\_8 cpe:/o:microsoft:windows\_8.1

OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 2.94 seconds

Con este comando vamos a ver qué servicios y versión están ejecutándose en el objetivo/maquina windows7

root@computaxion:~# nmap -sV 192.168.171.165

Starting Nmap 7.80 (https://nmap.org) at 2019-09-15 14:51 EDT

Nmap scan report for 192.168.171.165

Host is up (0.00048s latency).

Not shown: 991 closed ports

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open Microsoft-ds Microsoft Windows 7 - 10 Microsoft-ds

49152/tcp open msrpc Microsoft Windows RPC

49153/tcp open msrpc Microsoft Windows RPC

49154/tcp open msrpc Microsoft Windows RPC

49155/tcp open msrpc Microsoft Windows RPC

49156/tcp open msrpc Microsoft Windows RPC

49157/tcp open msrpc Microsoft Windows RPC

MAC Address: 00:0C:29:EC:45:1E (VMware)

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 60.62 seconds

con el comando -A: Habilita la detección del sistema operativo, la detección de versiones, el escaneo de scripts y el trazado de ruta /maquina windows7

esta opcion es muy intrusiba y puede ser detectada por ids o administrador.

root@computaxion:~# nmap -A 192.168.171.165

Starting Nmap 7.80 ( https://nmap.org ) at 2019-09-15 15:47 EDT

Nmap scan report for 192.168.171.165

Host is up (0.00083s latency).

Not shown: 991 closed ports

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds Windows 7 Home Basic 7600 microsoft-ds

49152/tcp open msrpc Microsoft Windows RPC

49153/tcp open msrpc Microsoft Windows RPC

49154/tcp open msrpc Microsoft Windows RPC

49155/tcp open msrpc Microsoft Windows RPC

49156/tcp open msrpc Microsoft Windows RPC

49157/tcp open msrpc Microsoft Windows RPC

MAC Address: 00:0C:29:EC:45:1E (VMware)

Device type: general purpose

Running: Microsoft Windows 7|2008|8.1

OS CPE: cpe:/o:microsoft:windows\_7::- cpe:/o:microsoft:windows\_7::sp1 cpe:/o:microsoft:windows\_server\_2008::sp1 cpe:/o:microsoft:windows\_server\_2008:r2 cpe:/o:microsoft:windows\_8 cpe:/o:microsoft:windows\_8.1

OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1

Network Distance: 1 hop

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

|\_clock-skew: mean: 59m59s, deviation: 1h43m55s, median: 0s

|\_nbstat: NetBIOS name: nil, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:ec:45:1e (VMware)

| smb-os-discovery:

| OS: Windows 7 Home Basic 7600 (Windows 7 Home Basic 6.1)

| OS CPE: cpe:/o:microsoft:windows\_7::-

| Computer name: computaxion2019

| NetBIOS computer name:

| Workgroup: GRU-COMPUTAXION\xE5\x89\x87COMPUTAXION2019\x00

|\_ System time: 2019-09-15T16:48:31-03:00

| smb-security-mode:

| account\_used: guest

| authentication\_level: user

| challenge\_response: supported

|\_ message\_signing: disabled (dangerous, but default)

| smb2-security-mode:

| 2.02:

|\_ Message signing enabled but not required

| smb2-time:

| date: 2019-09-15T19:48:32

|\_ start\_date: 2019-09-15T18:40:26

TRACEROUTE

HOP RTT ADDRESS

1 0.83 ms 192.168.171.165

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 67.51 seconds

con nmap tenemos algunas opciones para guardar el escaneo, el siguiente comando va a guardar el contenido en formato TXT

root@computaxion:~#nmap 192.168.171.165 > /root/nmap.txt

y este otro comando lo utilizamos con los parámetros que nos ofrece nmap.

root@computaxion:~#nmap 192.168.171.165 -oA /root/nmap