

Talleres Nucleo Linux UAGRM

“Introducción a Nmap”



Nombre : Felix Apaza (Fernando)

Contacto Grupo:

<https://www.facebook.com/groups/nucleolinux/> (Univ. De Santa Cruz)

<https://www.facebook.com/groups/nucleolinux.uagrm/> (UAGRM)

https://t.me/nucleolinux_uagrm/ (UAGRM)

Contacto personal:

Telegram: @FershoUno

GitHub : @FershoUno

Facebook: /FershoUno

“Escaneando la Red”



Nmap o “Network Mapper” traducido al español es un Mapeador de Red.

esta herramienta es de código abierto y que esta disponible la instalación para diferentes sistemas operativos como pueden ser

- Linux (todas las distribuciones)
- Microsoft Windows
- Mac OS X
- FreeBSD, OpenBSD y NetBSD
- Sun Solaris
- Amiga, HP-UX y otras plataformas

Esta herramienta no solo es un mapeador o escáner de red si no también es una herramienta para hacer auditorias, medir la seguridad de las redes encontrar vulnerabilidades para Websites entre otros.

Esta herramienta es muy usada para las tareas de seguridad o Hacking en general, desde los administradores de Sistemas hasta interesados con fines no respetables [Ciber delincuentes]

Nmap se encuentra disponible y preinstalado en varias distribuciones pero en este caso vamos a aprender a usar Nmap desde Kali Linux.

Escaneando la red con Nmap

Es importante hacer un escaneo de toda la red ya que así tenemos en conocimiento cuantos y cuales son los dispositivos que están conectados en la red para realizar los siguientes pasos.

Para poder empezar a hacer un escaneo de la red debemos conocer con que dirección vamos a trabajar por este caso sería el Gateway para saber podemos sacarlo de varias maneras

usando el comando **route**

```
root@root:~# route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
default _gateway 0.0.0.0 UG 600 0 0 wlan0
192.168.1.0 0.0.0.0 255.255.255.0 U 600 0 0 wlan0
root@root:~#
```

para ser mas preciso podemos agregar el parámetro **-n** para poder ver la dirección IP del router o puerta de enlace de la siguiente manera

```
root@root:~# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 192.168.1.1 0.0.0.0 UG 600 0 0 wlan0
192.168.1.0 0.0.0.0 255.255.255.0 U 600 0 0 wlan0
root@root:~#
```

otra forma de obtener la dirección del router o puerta de enlace sería con el comando

netstat y agregando el parámetro **-r** de esta manera

netstat -r

```
root@root:~# netstat -r
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
default _gateway 0.0.0.0 UG 0 0 0 wlan0
192.168.1.0 0.0.0.0 255.255.255.0 U 0 0 0 wlan0
root@root:~#
```

ahora queremos ser mas precisos con la puerta de enlace podemos agregar el parametro **n** junto al **-r** para que podamos obtener la puerta de enlace que sería así

```
root@root:~# netstat -rn
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
0.0.0.0 192.168.1.1 0.0.0.0 UG 0 0 0 wlan0
192.168.1.0 0.0.0.0 255.255.255.0 U 0 0 0 wlan0
root@root:~#
```

Ahora que sabemos por donde empezar, nosotros podemos hacer un escaneo de toda la red usando la dirección del router o puerta de enlace de esta manera:

nmap 192.168.x.x/24

si fuese con una puerta de enlace 192.168.1.1 como se muestra en la captura seria asi

nmap 192.168.1.1/24

```
root@root:~# nmap 192.168.1.1/24

Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-20 16:36 -04
Nmap scan report for 192.168.1.1
Host is up (0.0046s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
80/tcp    open  http
1900/tcp  open  upnp
MAC Address: 10:FE:ED:C0:7B:12 (Tp-link Technologies)

Nmap scan report for 192.168.1.102
Host is up (0.011s latency).
All 1000 scanned ports on 192.168.1.102 are closed
MAC Address: A4:BA:76:FB:62:01 (Huawei Technologies)

Nmap scan report for 192.168.1.103
Host is up (0.00053s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  iclslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
MAC Address: 08:00:27:CE:2E:32 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.108
Host is up (0.0000040s latency).
All 1000 scanned ports on 192.168.1.108 are closed

Nmap done: 256 IP addresses (4 hosts up) scanned in 11.81 seconds
root@root:~#
```

otra manera de escanear podemos usar un comodin “ * ” por ejemplo:

```
root@root:~# nmap 192.168.1.*

Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-20 16:38 -04
Nmap scan report for 192.168.1.1
Host is up (0.0097s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
80/tcp    open  http
1900/tcp  open  upnp
MAC Address: 10:FE:ED:C0:7B:12 (Tp-link Technologies)

Nmap scan report for 192.168.1.102
Host is up (0.021s latency).
All 1000 scanned ports on 192.168.1.102 are closed
MAC Address: A4:BA:76:FB:62:01 (Huawei Technologies)

Nmap scan report for 192.168.1.103
Host is up (0.00052s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  iclslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
MAC Address: 08:00:27:CE:2E:32 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.108
Host is up (0.0000040s latency).
All 1000 scanned ports on 192.168.1.108 are closed

Nmap done: 256 IP addresses (4 hosts up) scanned in 7.64 seconds
root@root:~#
```

nmap 192.168.x.*

o siguiendo el ejemplo de una puerta de enlace seria de esta manera

nmap 192.168.1.*

observamos que nos brinda el mismo resultado como se dijo es un comodín

para nuestro objetivo seria la dirección IP **192.168.1.103** [Oracle VirtualBox Virtual NIC]

bien entonces yo puedo escanear solo esa dirección IP con nmap de la siguiente manera

nmap 192.168.1.103

```
root@root:~# nmap 192.168.1.103
Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-20 17:20 -04
Nmap scan report for 192.168.1.103
Host is up (0.00050s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
554/tcp    open  rtsp
2869/tcp   open  iclslap
5357/tcp   open  wsdaapi
10243/tcp  open  unknown
MAC Address: 08:00:27:CE:2E:32 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 10.15 seconds
root@root:~#
```

nos muestra los puertos abiertos/estado del puerto/nombre de servicio/

ahora revisamos que dirección IP tiene la maquina virtual

```
C:\Windows\system32\cmd.exe
C:\Users\windows7>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Conexión de área local:
    Sufijo DNS específico para la conexión. . . :
    Vínculo dirección IPv6 local. . . : fe80::1945:877a:fb92:8b09%12
    Dirección IPv4. . . . . : 192.168.1.103
    Máscara de subred. . . . . : 255.255.255.0
    Puerta de enlace predeterminada. . . . . : 192.168.1.1

Adaptador de túnel isatap.{E0F4E7B3-1F06-4177-A2D3-FF174CB2E233}:
    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . . :

Adaptador de túnel Conexión de área local* 9:
    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . . :

C:\Users\windows7>
```

la dirección IPv4 es la dirección que el router asigna al dispositivo y es nuestro objetivo.

Por defecto Nmap nos va mostrar un escaneo por defecto, nosotros vamos a abrirnos paso para hacer un mejor escaneo

para esto vamos a empezar a seleccionar que puertos queremos que nos muestre o bien estas razones

- para buscar puertos que nos interese

- para optimizar el escaneo y disminuir el tiempo de espera

bien entonces vamos a usar el parámetro **-p** para poder decir a Nmap que puerto o puertos quiero que escanee Nmap o bien desde que puerto a que puerto quiero que Nmap haga el escaneo

usando el parametro **-p** seria de esta manera

```
# nmap -p139 192.168.1.103  
=> selecciono el puerto139
```

```
// -p139
```

```
root@root:~# nmap -p139 192.168.1.103  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-20 17:34 -04  
Nmap scan report for 192.168.1.103  
Host is up (0.00043s latency).  
  
PORT      STATE SERVICE  
139/tcp   open  netbios-ssn  
MAC Address: 08:00:27:CE:2E:32 (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds  
root@root:~#
```

como observamos solo nos mostro un solo puerto pero ahora quisiera escanear varios puertos para eso podemos agregar varios puertos por ejemplo -p22,139,445,8080

aplicando en Nmap seria de la siguiente manera

```
# nmap -p22,139,445,8080 192.168.1.103
```

```
root@root:~# nmap -p22,139,445,8080 192.168.1.103  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-20 17:39 -04  
Nmap scan report for 192.168.1.103  
Host is up (0.00045s latency).  
  
PORT      STATE SERVICE  
22/tcp    filtered ssh  
139/tcp    open  netbios-ssn  
445/tcp    open  microsoft-ds  
8080/tcp   filtered http-proxy  
MAC Address: 08:00:27:CE:2E:32 (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 2.65 seconds  
root@root:~#
```

como observamos nos muestra el puerto 22 filtrado ya que para un escaneo normal no mostraría ya que Nmap por defecto nos muestra puertos abiertos pero en este caso nos mostró Nmap por que se lo pedimos así como el puerto 8080.

tenemos otra opción de Nmap que podemos indicar desde que puerto a que puerto quiero que escanee solo tendría que agregar este parámetro **-p1-445** en Nmap

este **-p1-445** nos quiere decir que va escanear desde el puerto 1 al puerto 445

de esta manera se usaría para escanear en Nmap

nmap -p1-445 192.168.1.103

```
root@root:~# nmap -p1-445 192.168.1.103
Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-20 17:44 -04
Nmap scan report for 192.168.1.103
Host is up (0.00051s latency).
Not shown: 442 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 08:00:27:CE:2E:32 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 8.57 seconds
root@root:~#
```

Ahora que sabemos como Escanear puertos nos tocaria saber que servicios y versiones están detrás de esa dirección IP

entonces para eso existe un parámetro **-sV** que su función es mostrar Información de los puertos que estamos escaneando como puede ser Que Servicios y que Versiones de esos servicios están corriendo detrás de dichos puertos en Nmap seria de esta manera

nmap -sV 192.168.1.103


```

root@root:~# nmap -sV 192.168.1.103

Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-20 17:50 -04
Nmap scan report for 192.168.1.103
Host is up (0.00051s latency).
Not shown: 993 filtered 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 (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:CE:2E:32 (Oracle VirtualBox virtual NIC)
Service Info: Host: WINDOWS7-PC; 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 121.86 seconds
root@root:~#

```

Ahora nosotros podemos hacer una combinacion de 2 parametros en este caso quiero que Nmap me escanee los servicios y versiones pero de los puertos que yo quiero que lo haga ,para eso seria de la siguiente manera

nmap -sV -p139,445 192.168.1.103

```

root@root:~# nmap -sV -p139,445 192.168.1.103

Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-20 18:27 -04
Nmap scan report for 192.168.1.103
Host is up (0.00042s latency).
PORT      STATE SERVICE      VERSION
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 08:00:27:CE:2E:32 (Oracle VirtualBox virtual NIC)
Service Info: Host: WINDOWS7-PC; 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 9.39 seconds
root@root:~#

```

como vemos tenemos mejores resultados

Nmap nos trae diferentes tecnicas de escaneos como pueden ser las siguientes

Técnicas de Escaneo:

-sS | sT | sA | sW | sM : TCP SYN | Connect() | ACK | Window | Maimon scans

-sU : UDP Scan

-sN | sF | sX : TCP Null | FIN | Xmas scans

--scanflags <flags> : Customize TCP scan flags

-sl <zombie host[:probeport]>: Idle scan

-sY | sZ : SCTP INIT | COOKIE-ECHO scans

-sO : IP protocol scan

-b <FTP relay host> : FTP bounce scan

de entre ellas vamos a usar el Tipo de escaneo **-sS** [SYN]

y ademas podemos saber que sistema operativo esta corriendo detrás de la direccion IP

usando el parámetro **-O** haciendo la combinación de ambos quedaría de la siguiente manera

nmap -sS -O 192.168.1.103

```
root@root:~# nmap -sS -O 192.168.1.103
Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-20 18:54 -04
Nmap scan report for 192.168.1.103
Host is up (0.00050s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
554/tcp    open  rtsp
2869/tcp   open  iclslap
5357/tcp   open  wsdapi
10243/tcp   open  unknown
MAC Address: 08:00:27:CE:2E:32 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_7::-:professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista:sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or Windows 8, Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
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 14.63 seconds
root@root:~#
```

Como podemos observar el parámetro -O o bien nos puede mostrar precisamente que sistema operativo esta corriendo o nos da una probabilidad en porcentaje sobre que sistema operativo en casos como este nos dice

Running: Microsoft Windows 2008|8.1|7|Phone|Vista

entonces podemos asumir que es windows y que es una de las versiones antiguas y que podrían ser una de ellas lo cual se toma ventaja al ser antiguas puede existir un exploit que nos

de acceso remoto al ordenador y tener los privilegios de hacer y deshacer todo.

Nmap Scripting Engine (NSE)

Una vez que sabemos como hacer un reconocimiento dentro de una red privada

que mas podemos hacer?

Respuesta.- Nmap nos trae esta sección de Scripts es la parte quizás la mas potente y flexible de Nmap

este motor de scripts ayuda a los usuarios a escribir scripts , usarlos y compartirlos desde scripts simples usando el lenguaje de programación Lua.

El objetivo inicial con NSE era crear el sistema para el descubrimiento de redes, detección de versiones más sofisticadas, detección de vulnerabilidades. NSE también puede utilizarse para la explotación de vulnerabilidades.

Directorio de los Scripts de Nmap

Si se quiere conocer donde están los scripts de Nmap se tiene que acceder al directorio donde se encuentra todos los scripts de Nmap en la siguiente dirección:

Directorio => **# /usr/share/nmap/scripts**

```
Aplicaciones  Lugares  Terminal  mar 19:10
root@root: /usr/share/nmap/scripts
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@root:~# cd /usr/share/nmap/scripts/
root@root:/usr/share/nmap/scripts# ls
acarsd-info.nse          http-grep.nse           nntp-ntlm-info.nse
address-info.nse        http-headers.nse       nping-brute.nse
afp-brute.nse           http-huawei-hg5xx-vuln.nse nrpe-enum.nse
afp-ls.nse              http-icloud-findmyiphone.nse ntp-info.nse
afp-path-vuln.nse       http-icloud-sendmsg.nse ntp-monlist.nse
afp-serverinfo.nse      http-iis-short-name-brute.nse omp2-brute.nse
afp-showmount.nse       http-iis-webdav-vuln.nse omp2-enum-targets.nse
ajp-auth.nse            http-internal-ip-disclosure.nse omron-info.nse
ajp-brute.nse           http-joomla-brute.nse  openlookup-info.nse
ajp-headers.nse         http-litespeed-sourcecode-download.nse openvas-otp-brute.nse
ajp-methods.nse        http-ls.nse            openwebnet-discovery.nse
ajp-request.nse         http-majordomo2-dir-traversal.nse oracle-brute.nse
allseeingeye-info.nse   http-malware-host.nse oracle-brute-stealth.nse
amqp-info.nse           http-mcmp.nse          oracle-enum-users.nse
asn-query.nse           http-methods.nse       oracle-sid-brute.nse
auth-owners.nse        http-method-tamper.nse oracle-tns-version.nse
auth-spoof.nse         http-mobileversion-checker.nse ovs-agent-version.nse
backorifice-brute.nse   http-ntlm-info.nse     p2p-conficker.nse
backorifice-info.nse   http-open-proxy.nse    path-mtu.nse
bacnet-info.nse         http-open-redirect.nse pcanywhere-brute.nse
banner.nse              http-passwd.nse         pcworx-info.nse
bitcoin-getaddr.nse     http-phpmyadmin-dir-traversal.nse pgsql-brute.nse
bitcoin-info.nse        http-phpself-xss.nse    pjl-ready-message.nse
bitcoinrpc-info.nse     http-php-version.nse   pop3-brute.nse
bittorrent-discovery.nse http-proxy-brute.nse    pop3-capabilities.nse
bjnp-discover.nse       http-put.nse            pop3-ntlm-info.nse
broadcast-ataoe-discover.nse http-qnap-nas-info.nse ptp-version.nse
broadcast-avahi-dos.nse http-referer-checker.nse puppet-naivesigning.nse
broadcast-bjnp-discover.nse http-rfi-spider.nse    qconn-exec.nse
```

Todos estos Scripts tiene diferentes funciones tanto para Paginas Web como redes privadas y para eso existen diferentes categorías para el uso especifico que uno quiera darle.

Categorías de Scripts de Nmap

Nmap tiene categorías para el uso automatizado de Scripts para la facilidad el uso que son :

- **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 la víctima o *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.

[para un atacante no es conveniente usar todos los scripts la razon de que puede ser muy ruidoso]

Ejecución de un Script en Nmap

Nmap contiene Scripts que nos ayudan a la detección de servicios y que tan vulnerables son estos

la manera de hacer la ejecución

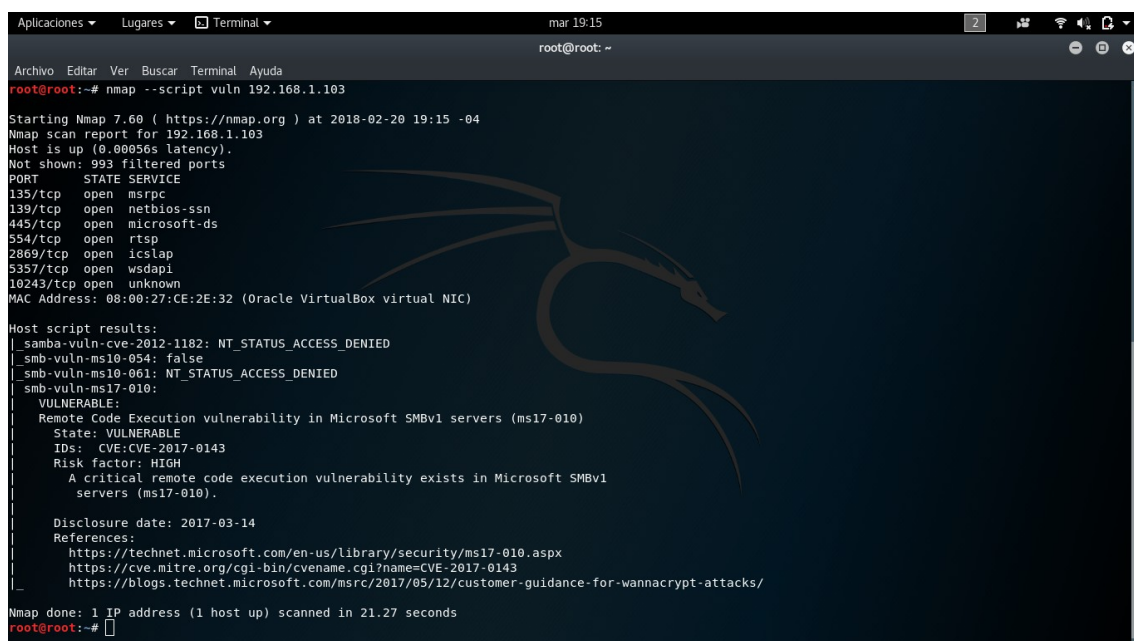
esta seria las maneras de poder ejecutar los scripts

--script [categoría / directorio / nombre / all]

Ejecutando Scripts de Nmap por Categorías

Nmap como ya se vio tiene categorías de Scripts en este caso podemos usar una categoría llamada Vuln que hace el uso de scripts para detección de vulnerabilidades como se muestra en el siguiente ejemplo:

nmap -script vuln [direccion_IP]



```
Aplicaciones Lugares Terminal mar 19:15
root@root: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@root:~# nmap --script vuln 192.168.1.103

Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-20 19:15 -04
Nmap scan report for 192.168.1.103
Host is up (0.00056s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
554/tcp    open  rtsp
2869/tcp   open  iclslap
5357/tcp   open  wsddapi
10243/tcp   open  unknown
MAC Address: 08:00:27:CE:2E:32 (Oracle VirtualBox virtual NIC)

Host script results:
|_ samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_ smb-vuln-ms10-054: false
|_ smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_ smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs: CVE:CVE-2017-0143
|     Risk factor: HIGH
|     A critical remote code execution vulnerability exists in Microsoft SMBv1
|     servers (ms17-010).
|
|   Disclosure date: 2017-03-14
|   References:
|     https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|     https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_
Nmap done: 1 IP address (1 host up) scanned in 21.27 seconds
root@root:~#
```

como podemos observar Nmap uso toda la categoría de Vuln para detectar alguna vulnerabilidad en la maquina virtual, en este caso la encontró usando el script **smb-vuln-ms17-010** esta vulnerabilidad si se explota con éxito podría darnos acceso remoto al ordenador.

Ejecutando Script desde un directorio

Para hacer la ejecución de un script desde un directorio cualquiera se agrega

nmap --script=directorio Direccion_IP

en este caso copie el mismo script **smb-vuln-ms17-010.nse** al escritorio entonces para ejecutar el script seria de la siguiente manera

#nmap --script=/root/Escritorio/smb-vuln-ms17-010.nse

```
root@root:~# nmap --script=/root/Escritorio/smb-vuln-ms17-010.nse 192.168.1.103

Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-20 19:23 -04
Nmap scan report for 192.168.1.103
Host is up (0.00055s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
554/tcp    open  rtsp
2869/tcp   open  iclslap
5357/tcp   open  wsdapi
10243/tcp  open  unknown
MAC Address: 08:00:27:CE:2E:32 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-vuln-ms17-010:
|_  VULNERABLE:
|    Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|    State: VULNERABLE
|    IDs:  CVE:CVE-2017-0143
|    Risk factor: HIGH
|    A critical remote code execution vulnerability exists in Microsoft SMBv1
|    servers (ms17-010).
|
|    Disclosure date: 2017-03-14
|    References:
|      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_
Nmap done: 1 IP address (1 host up) scanned in 5.19 seconds
root@root:~#
```

192.168.1.103

como podemos observar a la derecha esta el script , de esta manera es la que se ejecuta los scripts desde cualquier directorio

Ejecutando un Script por nombre desde Nmap

En este ejemplo se va usar un Script de Nmap para detectar si existe la vulnerabilidad MS17-010 que uso en Ransomware Wannacry en el 2017 que vendría ser el ejemplo anterior

nmap -script=smb-vuln-ms17-010.nse [direccion_IP]

```
root@root:~# nmap --script=smb-vuln-ms17-010.nse 192.168.1.103

Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-20 19:19 -04
Nmap scan report for 192.168.1.103
Host is up (0.00050s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
554/tcp    open  rtsp
2869/tcp   open  iclslap
5357/tcp   open  wsddapi
10243/tcp   open  unknown
MAC Address: 08:00:27:CE:2E:32 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs: CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|       servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_
Nmap done: 1 IP address (1 host up) scanned in 4.79 seconds
root@root:~#
```

como se puede observar Nmap nos muestra que existe una vulnerabilidad como ya dije anteriormente es la misma que uso Wannacry siendo que este Ransomware aprovecho gracias al exploits 0Day de la NSA

Actualización de Scripts de Nmap

para tener actualizado los scripts que tiene Nmap podemos ejecutar en la terminal dela siguiente manera:

nmap -script-update-db

```
root@root:~# nmap --script-updatedb

Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-20 19:28 -04
NSE: Updating rule database.
NSE: Script Database updated successfully.
Nmap done: 0 IP addresses (0 hosts up) scanned in 1.10 seconds
root@root:~#
```

Es importante tener actualizado Nmap ya que asi tenemos la posibilidad de detectar las nuevas vulnerabilidades a la hora de hacer probar si un dispositivo es o no vulnerable.