Práctica: Escaneo de redes con Nmap.

Introducción:

El escaneo de red se refiere a un conjunto de procedimientos utilizados para identificar el host, los puertos y los servicios en una red.

****Objetivos:****

-Descubrir equipos activos, direcciones IP y puertos abiertos.
-Descubrir el sistema operativo, su arquitectura y los servicios que ofrece.
-Descubrir vulnerabilidades en los equipos activos.

****Tipos de escaneos:****

****Escaneo de puertos:**** Tiene el objetivo de descubrir puerto abiertos. Además de verificar los servicios que corren dentro de un objetivo enviando una secuencia de mensajes para conectar y analizar los puertos TCP y UDP.
****Escaneo de red:**** Enumera las direcciones IP. Además, es un procedimiento para identificar un host activo en una red, ya sea para atacarlos o para evaluar la seguridad o la red.
****Escaneo de vulnerabilidades:**** Permite realizar un conjunto de pruebas sobre un sistema o red para encontrar debilidades y/o fallos de seguridad de estos.

Antes de iniciar la práctica es recomendable conocer un poco sobre los protocolos de red.

Familia de protocolos TCP/IP

Los protocolos de red normalmente se desarrollan en capas. Por lo cual TCP/IP es el resultado de combinar distintos protocolos en las diferentes capas. El cual consta de cuatro capas que son:

1. Capa física.
2. Capa de red.
3. Capa de transporte.
4. Capa de aplicación.

Protocolos relevantes en seguridad.

El protocolo TCP/IP posee unas características fundamentales que condicionan en gran medida las vulnerabilidades asociadas a su funcionamiento. En el aspecto de seguridad los siguientes protocolos permiten la realización de algunas conductas atípicas o diferentes al fin que fueron concebidos.

Protocolo ARP

Es un protocolo de capa física, que se encarga de encontrar la dirección física (MAC) que corresponde una determinada IP.

Protocolo IP

Es el principal protocolo de TCP/IP, el cual se encarga de transmitir y encaminar los paquetes de información del origen al destino. Se encuentra en la capa de red.

Características de IP:

-Protocolo no orientado a conexión
-No fiable.

Para avisar en los extremos de la comunicación de algún error se auxilia del protocolo ICMP (Internet Control Message Protocol).

****Protocolo TCP****

Es un protocolo orientado a conexión que requiere el establecimiento de una conexión entre los extremos que vayan a comunicarse antes de empezar el intercambio de mensajes. Definido en el RFC 793.

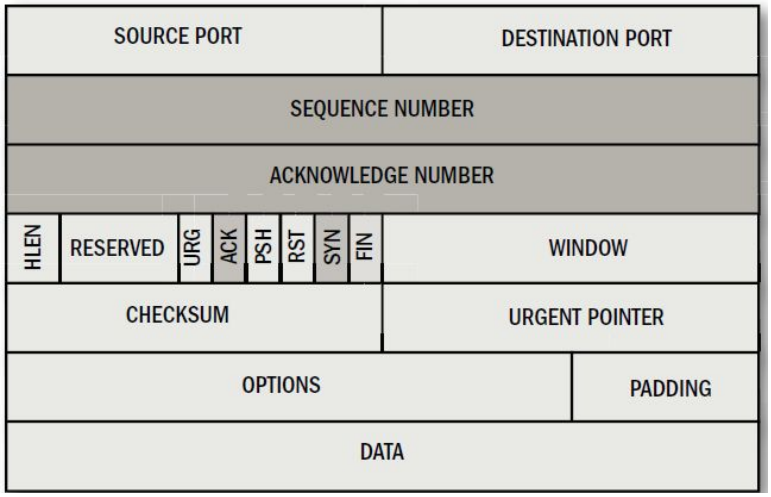
Características de TCP.

- Es un protocolo fiable.
- Se encarga tanto de asegurar la recepción de los paquetes, como de ensamblarlos en el orden correcto los paquetes que hayan sido fragmentados.
- Permite llevar un control de los paquetes recibidos por destinatario gracias a un ACK (confirmación de recepción).

****Banderas de comunicación TCP****

El encabezado TCP contiene varios indicadores que controlan la transmisión de datos a través de una conexión. Seis banderas de control TCP administra la conexión entre el host y dan instrucciones al sistema.

Cuatro de estas banderas son (SYN, ACK, FIN y RST) las cuales rigen el establecimiento, mantenimiento y terminación de una conexión. Las otras dos banderas (PSH y URG) proveen instrucciones al sistema.



****Protocolo UDP****

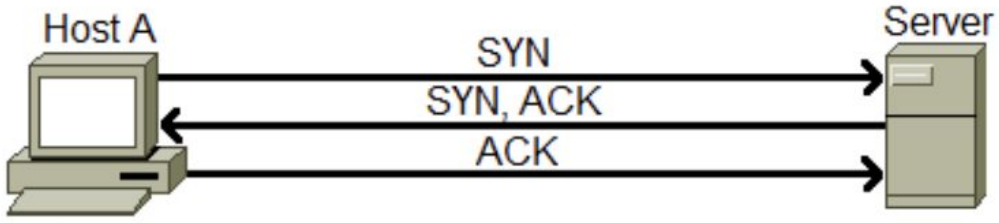
Es un protocolo más sencillo que TCP, no cuenta con mecanismos que permita corregir errores, retransmitir o detectar paquetes perdidos o duplicados.

Características de UDP.

- No está orientado a conexión.
- Es un protocolo no fiable.
- No necesita el establecimiento de una conexión, de manera que el número de paquetes que se tienen que enviar es menor.

****Establecimiento de conexión TCP.****

El procedimiento para establecer una conexión se conoce como Three-Way handshake, podemos hacer la análoga a una llamada telefónica donde en el primer paso SYN el emisor realiza la llamada y pregunta “Que tal puedo hablar contigo”, el receptor contesta con SYN, ACK algo como “Si, llámame” y por último el emisor contesta con un ACK similar a un “Gracias”. Con estos pasos se inicia la conversación.



****Metodología de escaneo.****

-ICMP Scanning

-TCP Scanning

-UDP Scanning

****Objetivos de la práctica:****

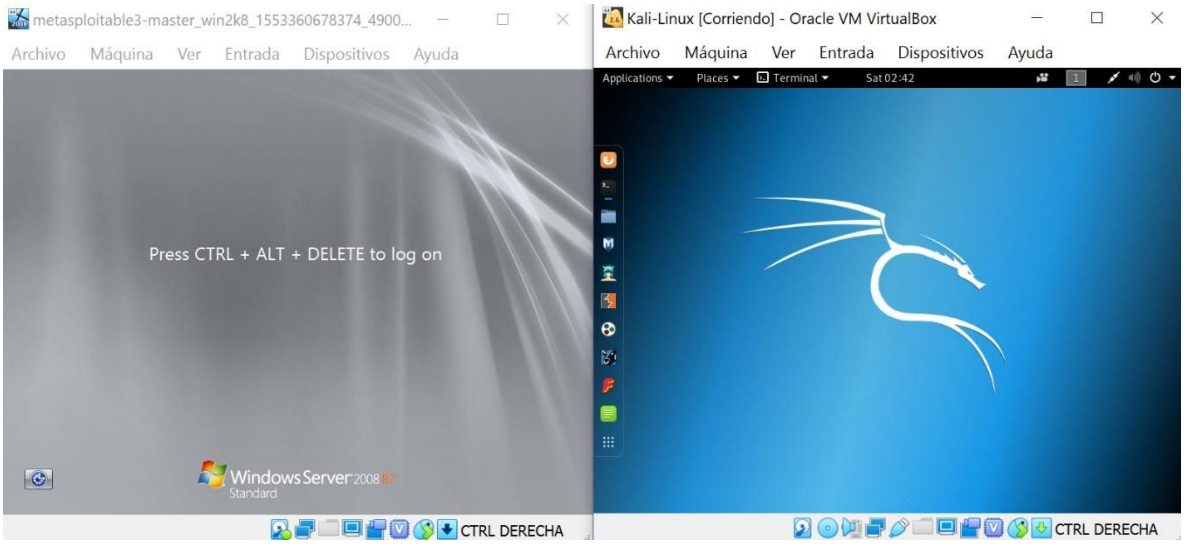
En esta práctica el alumno implementará un escaneo de red con la herramienta ****Nmap**,** con las técnicas vistas anteriormente. Además, se explicará de forma técnica lo que ocurre al enviar un comando con el objetivo de conocer el funcionamiento detrás de la misma.

****Herramientas necesarias:****

-VirtualBox 6.0.4.
https://www.virtualbox.org/wiki/Downloads
-Kali Linux 2019.1a.
https://www.kali.org/downloads/
-Metasploitable 3
https://github.com/dxa4481/truffleHog

****Puesta en marcha de Nmap en Kali Linux.****

1. Se inician las máquinas virtuales de Kali Linux y Metasploitable 3.



2. Verificar la red a la que pertenece el equipo de Kali con el comando ifconfig en la terminal.

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.2.5  netmask 255.255.255.0  broadcast 192.168.2.255
        inet6 fe80::de62:9e33:8ec3:89ed  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:c0:01:92  txqueuelen 1000  (Ethernet)
        RX packets 22565  bytes 32883190 (31.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 15420  bytes 943304 (921.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

3. ****ICMP Echo Scanning/ Ping Sweep**,** esta técnica se utiliza para detectar equipos activos dentro de la red. Su funcionamiento se basa en una petición ICMP 8 (echo request), si el equipo está conectado contesta con un ICMP 0 (echo reply) esto está definido en el RFC 792. Esto se representa con el comando

nmap -sP 192.168.2.0/24

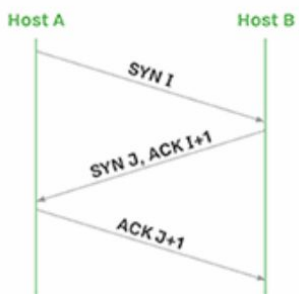
```
root@kali:~# nmap -sP 192.168.2.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-30 02:43 UTC
Nmap scan report for 192.168.2.1
Host is up (0.00011s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 192.168.2.2
Host is up (0.000051s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 192.168.2.3
Host is up (0.000051s latency).
MAC Address: 08:00:27:68:D9:86 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.2.7
Host is up (0.00012s latency).
MAC Address: 08:00:27:70:B4:99 (Oracle VirtualBox virtual NIC)
```

****TCP Connect/ Full Open Scan**:** Detecta que puerto se encuentran abiertos completando el three-way handshake.

Después de encontrar un equipo activo para este caso cuenta con la dirección IP "192.168.2.7" se prosigue a realizar el escaneo para conocer los puertos disponibles. Esto se representa con el comando:

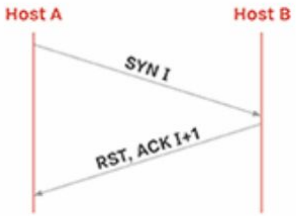
Nmap -sT "dirección IP"

Puerto abierto




```
root@kali:~# nmap -sT 192.168.2.7
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-30 02:44 UTC
Nmap scan report for 192.168.2.7
Host is up (0.00046s latency).
Not shown: 978 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-http
7676/tcp  open  imqbrokerd
8009/tcp  open  ajp13
8022/tcp  open  oa-system
8031/tcp  open  unknown
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8383/tcp  open  m2mservices
8443/tcp  open  https-alt
9200/tcp  open  wap-wsp
49152/tcp open  unknown
```

Puerto cerrado



4. ****Stealth Scan (Half-open Scan):**** Este escaneo corta el three-way handshake antes de establecer la conexión enviado un paquete tipo RST. Lo que permite saltar reglas establecidas por un firewall, mecanismos de registro ocultándose como lo hace el tráfico habitual de la red. Esto se representa con el comando:

Nmap -sS “dirección IP”

```
root@kali:~# nmap -sS 192.168.2.7
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-30 17:12 UTC
Nmap scan report for 192.168.2.7
Host is up (0.00021s latency).
Not shown: 978 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-http
7676/tcp  open  imqbrokerd
8009/tcp  open  ajp13
8022/tcp  open  oa-system
8031/tcp  open  unknown
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8383/tcp  open  m2mservices
8443/tcp  open  https-alt
9200/tcp  open  wap-wsp
49152/tcp open  unknown
```

5. ****Inverse TCP Flag Scanning**:** Los atacantes envían paquetes de probes TCP con un conjunto de indicadores TCP (FIN, URG, PSH) o sin indicadores (NULL). Esto escaneo se basa en una explotación del funcionamiento del protocolo TCP descrito RFC 793 donde se menciona que cualquier paquete que no contenga las

banderas SYN, RST, o ACK devolverá un RST si el puerto está **cerrado** y si se encuentra **abierto** no dará respuesta alguna.

Este tipo de escaneos resulta útil para saltar firewalls sin estado y filtrado de paquetes, un inconveniente es que la mayoría de los sistemas no siguen al pie de la letra este RFC y envían un RST aunque se encuentre cerrado o abierto, este escaneo funciona para sistemas UNIX.

Las configuraciones más utilizadas son:

1. **Escaneo NULL:** Donde no se fija ningún bit o bandera.

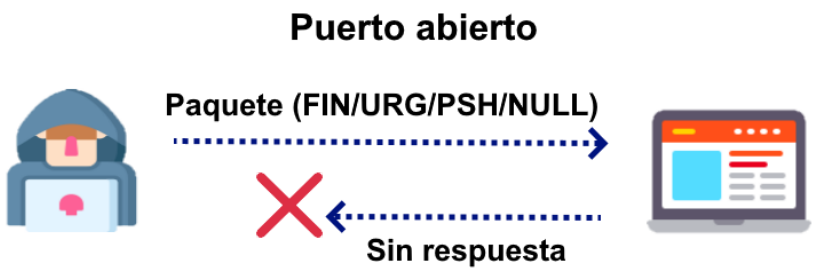
   nmap -sN “dirección IP”

2. **Escaneo FIN:** Que lleva consigo la bandera TCP FIN.

   nmap -sF “dirección IP”

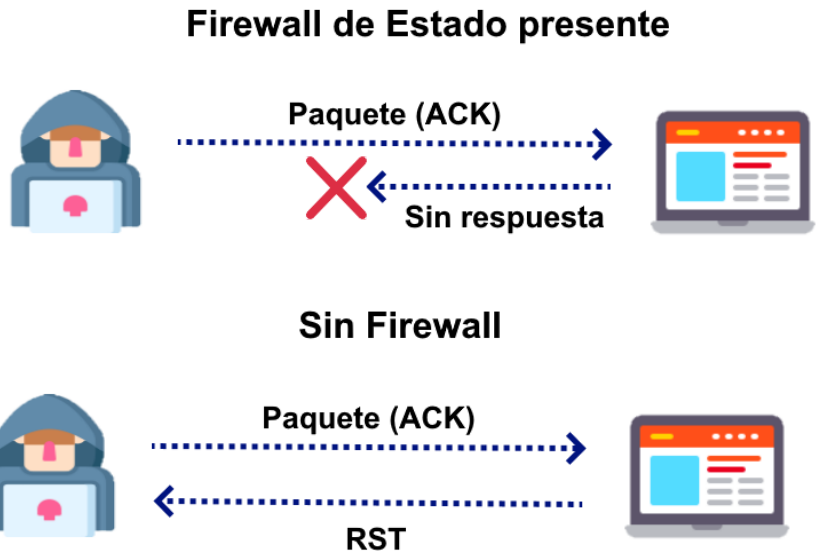
3. **Escaneo Xmas:** Donde se envían las banderas FIN, PSH y URG al mismo tiempo.

   nmap -sX “dirección IP”



6. ****ACK Flag Probe Scanning:**** Se puede utilizar para comprobar si el host destino cuenta con algún mecanismo de filtrado de paquetes.

   Por lo cual se envía un paquete de prueba ACK con un número de secuencia aleatorio, si el equipo destino no responde implica que el puerto está filtrado (Firewall de estado presente), caso contrario si la respuesta es un RST significa que el puerto no está filtrado.

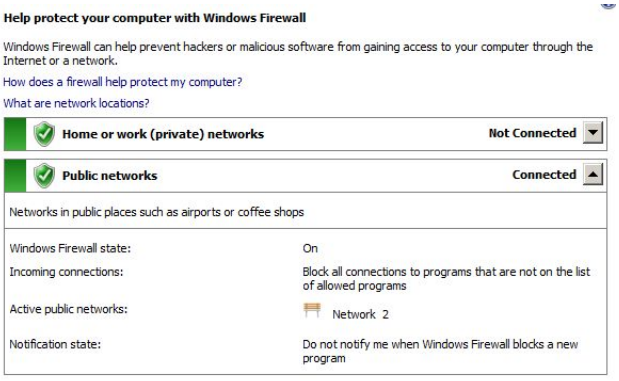


Para esta prueba de concepto en la máquina virtual de Metasploitable 3 por default se encuentra habilitado el firewall de Windows.

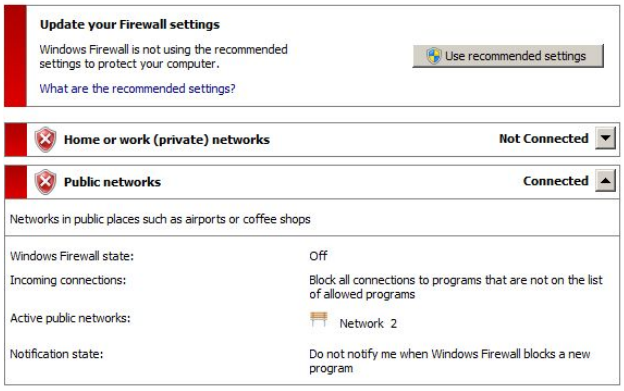
nmap -sA “dirección IP”

```
root@kali:~# nmap -sA 192.168.2.7
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-30 20:58 UTC
Nmap scan report for 192.168.2.7
Host is up (0.00025s latency).
All 1000 scanned ports on 192.168.2.7 are filtered
MAC Address: 08:00:27:70:B4:99 (Oracle VirtualBox virtual NIC)
```

Como se puede apreciar en la imagen anterior los puertos se encuentra filtrados.



Si se deshabilita el Firewalls de Windows, para iniciar sesión el usuario y password de la máquina virtual es vagrant ambos.



Se realiza nuevamente el escaneo y devuelve lo siguiente:

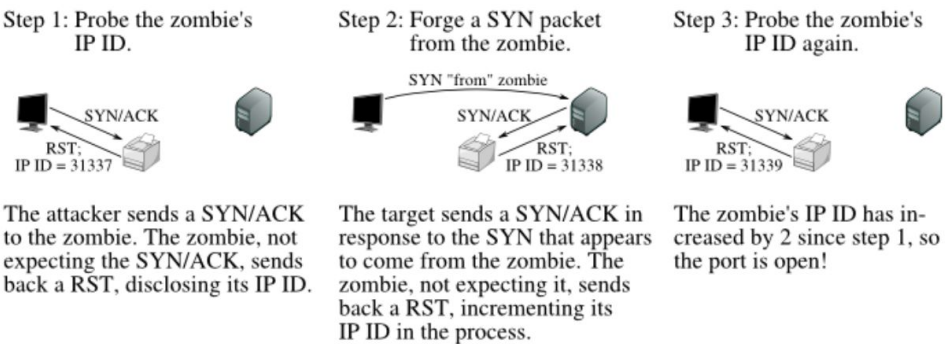
```
root@kali:~# nmap -sA 192.168.2.7
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-30 21:06 UTC
Nmap scan report for 192.168.2.7
Host is up (0.00020s latency).
All 1000 scanned ports on 192.168.2.7 are unfiltered
MAC Address: 08:00:27:70:B4:99 (Oracle VirtualBox virtual NIC)
```

Como se puede apreciar en la imagen ahora muestra que los puertos están sin filtrar, ya que se desactivo el Firewall.

7. ****IDLE/IPID Header Scan:**** Es un método de escaneo de puertos TCP que se utiliza para enviar una dirección de origen falsificada a una computadora para averiguar qué servicios están disponibles. Ofrece escaneo sigiloso de un host remoto.

Cada paquete IP en Internet tiene un número de identificación de fragmento (IPID); El sistema operativo aumenta el IPI para cada paquete enviado, por lo tanto, durante un escaneo del IPID le dan a un atacante el número de paquetes enviados después su ejecución.

Detección de puertos abiertos:



1. Primeramente, el atacante manda un paquete probe al equipo que utilizará como **zombie** y obtiene el IPID.
2. El atacante manda un paquete SYN al objetivo con la dirección IP del equipo **zombie**, el objetivo responde con un SYN/ACK al **zombie**, ya que supuestamente él lo envío, este último como no espera un paquete envía un RST e incrementa su IPID.
3. Nuevamente el atacante manda un paquete SYN/ACK al **zombie** para comprobar su IPID el cual incrementó en dos desde el primer paso. Se establece que el puerto está abierto ya que, entre la comunicación del objetivo y el zombi, este último envió un paquete.

Detección de puertos cerrados:

-Primeramente, el atacante manda un paquete probe al equipo que utilizará como zombie y obtiene el IPID.
-El atacante manda un paquete SYN al objetivo con la dirección IP del equipo zombie, el objetivo responde con un RST (ya que el puerto se encuentra cerrado) al zombie y este no responde y no incrementa su IPID.
-Nuevamer ra comprobar su IPID el cual incr puerto está cerrado ya que, en n paquete.

```
root@kali:~# nmap -Pn -p- -sI www.platzi.com 192.168.2.7
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-30 22:05 UTC
Idle scan using zombie www.platzi.com (104.20.18.218:80); Class: Incremental
Nmap scan report for 192.168.2.7
Host is up (0.051s latency).
Not shown: 65492 closed|filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
3700/tcp  open  lrs-paging
4848/tcp  open  appserv-http
5985/tcp  open  wsman
7676/tcp  open  imqbrokerd
8009/tcp  open  ajp13
8019/tcp  open  qbdb
8020/tcp  open  intu-ec-svcdisc
8022/tcp  open  oa-system
8027/tcp  open  unknown
8028/tcp  open  unknown
8031/tcp  open  unknown
```

Todo este o que nuestro zombie sera

8. **UDP Scanning:** Si el sistema no responde con un mensaje entonces el puerto se encuentra **abierto**. Por lo contrario, si responde con un *"ICMP port*

unreachable message" quiere decir que se está **cerrado**. La mayoría de los Spywares, troyanos y otras aplicaciones maliciosas usan estos puertos.

Para su funcionamiento con nmap se utiliza el comando:

Nmap -sU "dirección IP"

OTROS COMANDOS INTERESANTES:

ESPECIFICANDO PUERTOS

-p <rango>: Solo escanear puertos especificados.
Ejemplo: -p22; -p1-65535; -p U:53,111,137

--exclude-ports <rango>: Excluir puertos específicos.

-F: Fast mode: Menos puertos que el escaneo predeterminado.

DETECCIÓN DE SERVICIOS/VERSIÓN:

-sV: para determinar la información del servicio / versión

SCRIPT SCAN:

--script=<Lua scripts>: <Lua scripts> es una lista de script que utiliza nmap.
Ejemplo: nmap -p445 --script smb-vuln-ms17-010 <objetivo>

DETECCIÓN DEL SISTEMA OPERATIVO:

-O: Habilitar la detección del sistema operativo.
Páginas para encontrar puertos más representativos

- https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml
- https://support.apple.com/es-mx/HT202944
- http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/ch-ports.html