Universidad Autónoma de Chiapas

Facultad de Contaduría y Administración, Campus I

Actividad 1.6 - Práctica 2 – "Escaneo de puertos"

Nombre: **Paola Culebro López.**

Matrícula: **A200176.**

Catedrático: **Dr. Luis Gutiérrez Alfaro.**

Asignatura: **Análisis de Vulnerabilidades.**

Grupo: **LIDTS 7º "M".**

Tuxtla Gutiérrez, Chiapas; 26/08/2023

Introducción

En esta práctica se explora el uso básico de Nmap, una herramienta poderosa de escaneo de red, desde la línea de comandos en sistemas Windows (en mi caso). A lo largo de la práctica se mostrará comandos esenciales y su funcionalidad. Desde escaneos básicos de puertos hasta detección de servicios, versiones y vulnerabilidades, cómo obtener información valiosa sobre hosts y redes. Además, se enfatiza la importancia de utilizar Nmap de manera ética y respetuosa, obteniendo permiso adecuado antes de realizar escaneos en redes o sistemas que no son de nuestra propiedad.

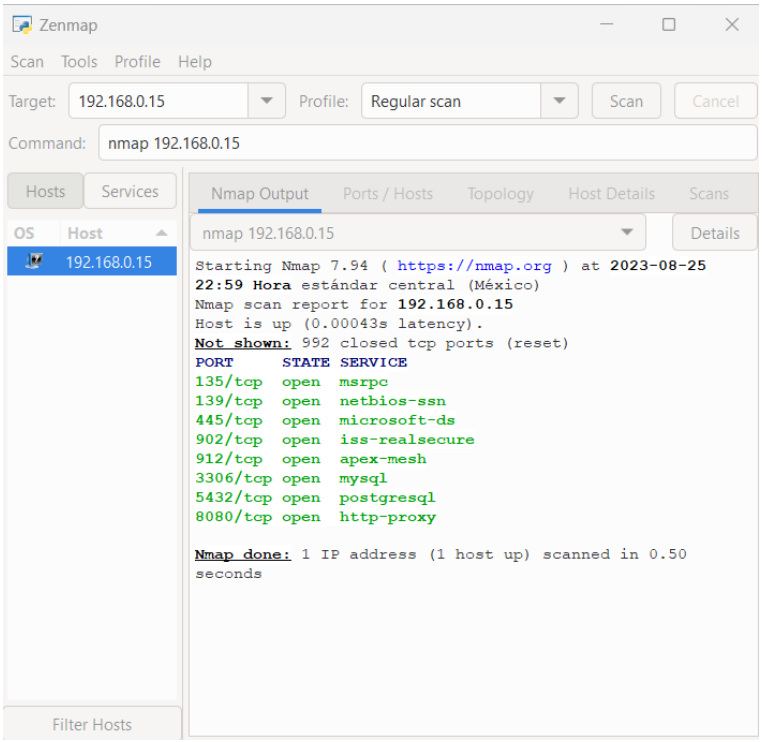
Escaneo de puertos y comandos (NMAP)

Para esta práctica, una vez instalado el programa Nmap en Windows, comencé por abrir el CMD en mi equipo para ejecutar '*ipconfig*' y obtener la IP de Windows. Pues con este, pude realizar los escaneos de los puertos desde la interfaz de Nmap.

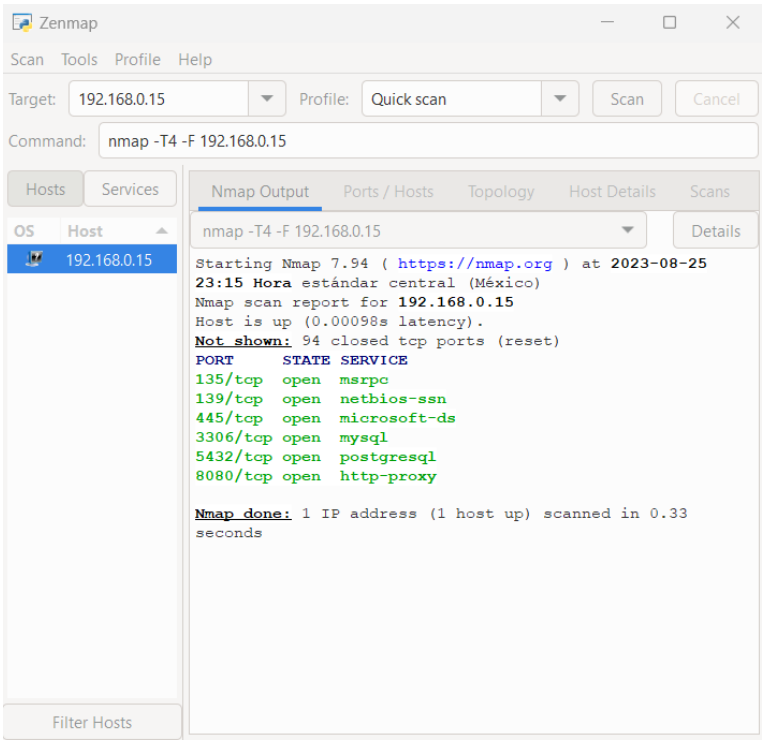
```
C:\Users\Paola>ipconfig

Configuración IP de Windows


Adaptador de Ethernet Ethernet 2:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::d2a8:d444:e32a:dabf%3
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.56.1
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . :

Adaptador de LAN inalámbrica Conexión de área local* 9:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Conexión de área local* 10:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :

Adaptador de Ethernet VMware Network Adapter VMnet1:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::df8:bb2e:9e6f:60d9%49
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.72.1
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . :

Adaptador de Ethernet VMware Network Adapter VMnet8:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::c8c5:8052:da01:e43e%50
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.174.1
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . :

Adaptador de LAN inalámbrica Wi-Fi:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::25cd:72:730d:e921%16
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.0.15
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.0.1
```

En Target (Objetivo) ingresé la IP de Windows; en Profile (Perfil) seleccioné el tipo de análisis a usar y di clic en Scan (Escaneo) para iniciar los procesos. Yo realicé tres procesos diferentes.

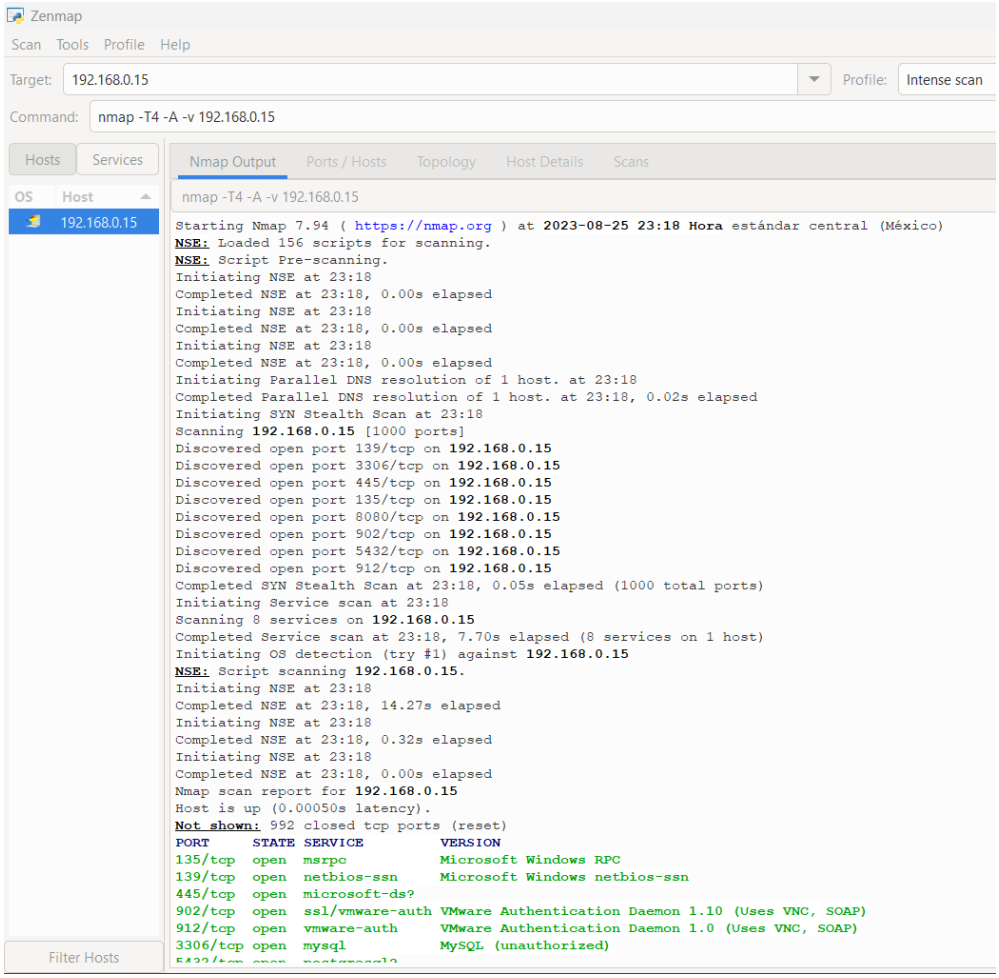
1. **Escaneo regular.**



2. **Escaneo rápido.**



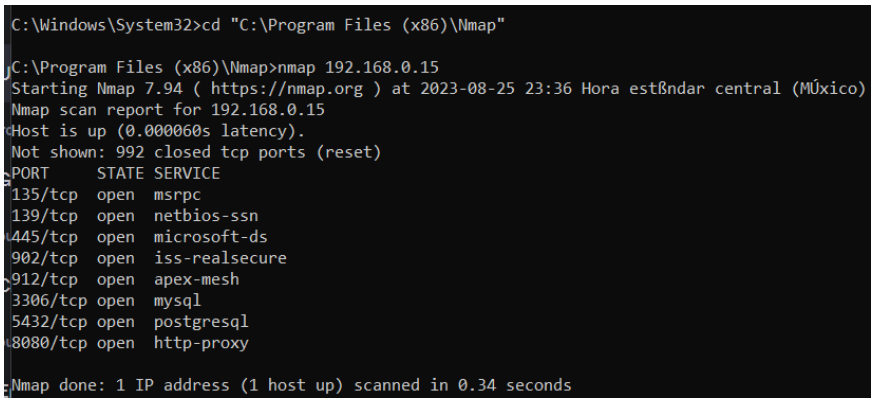
3. Escaneo intenso.



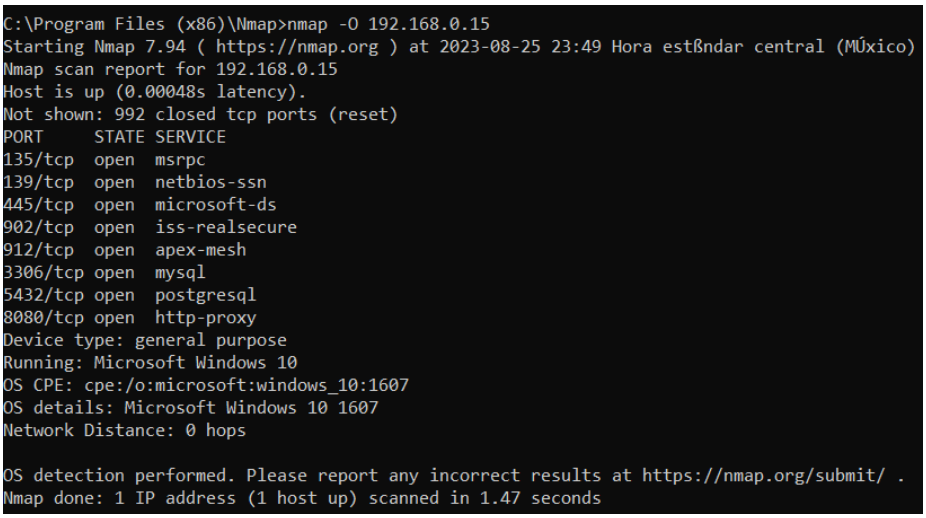

```
5432/tcp open  postgresql?
8080/tcp open  http            Apache httpd
|_http-title: Site doesn't have a title (text/html).
|_http-open-proxy: Proxy might be redirecting requests
| http-methods:
|   Supported Methods: POST OPTIONS HEAD GET TRACE
|_  Potentially risky methods: TRACE
|_http-server-header: Apache
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10:1607
OS details: Microsoft Windows 10 1607
Uptime guess: 14.276 days (since Fri Aug 11 16:41:24 2023)
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-08-26T05:18:36
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

NSE: Script Post-scanning.
Initiating NSE at 23:18
Completed NSE at 23:18, 0.00s elapsed
Initiating NSE at 23:18
Completed NSE at 23:18, 0.00s elapsed
Initiating NSE at 23:18
Completed NSE at 23:18, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
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 25.48 seconds
           Raw packets sent: 1016 (45.418KB) | Rcvd: 2046 (87.052KB)
```

Ahora bien, para ejecutar los comandos que el profesor nos proporcionó en el PDF, abrí el símbolo de sistema como administrador, pues Nmap requiere permisos especiales para realizar escaneos de red y acceder a ciertos recursos del sistema. Abrir la línea de comandos en modo administrador garantiza que Nmap tenga los permisos necesarios para funcionar correctamente… Una vez abierto de esta manera, me ubiqué al directorio de Nmap y empecé a ejecutar todos los comandos.

a) **nmap 192.168.0.15** (Ejecuta un escaneo básico en el host con mi dirección IP. El escaneo básico intenta identificar los puertos abiertos en este host y muestra la información sobre los servicios que se ejecutan en esos puertos).



b) **nmap -O 192.168.0.15** (Ejecuta un escaneo con detección de sistema operativo en el host. La opción -O indica a Nmap que realice una adivinanza sobre el sistema operativo que podría estar ejecutándose en el host objetivo, en función de las características de la red y las respuestas a las solicitudes enviadas durante el escaneo).



c) **nmap -sV 192.168.0.15** (Ejecuta un escaneo de servicios y versiones en el host. La opción -sV indica que realice un escaneo para detectar los servicios que se están ejecutando en los puertos abiertos del host y también intente determinar las versiones de esos servicios).

```
C:\Program Files (x86)\Nmap>nmap -sV 192.168.0.15
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-25 23:45 Hora estßndar central (MÚxico)
Nmap scan report for 192.168.0.15
Host is up (0.00012s latency).
Not shown: 992 closed tcp ports (reset)
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?
902/tcp  open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp  open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
3306/tcp open  mysql           MySQL (unauthorized)
5432/tcp open  postgresql?
8080/tcp open  http            Apache httpd
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 8.36 seconds
```

d) nmap -A 192.168.0.15 (DE TODO EL SEGMENTO… Ejecuta un escaneo avanzado. La opción -A indica que realice un escaneo con detección de sistema operativo, detección de versión de servicio, detección de script y trazado de ruta (traceroute) integrados).

```
C:\Program Files (x86)\Nmap>nmap -A 192.168.0.15
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-25 23:52 Hora estßndar central (MÚxico)
Nmap scan report for 192.168.0.15
Host is up (0.00068s latency).
Not shown: 992 closed tcp ports (reset)
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?
902/tcp  open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp  open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
3306/tcp open  mysql           MySQL (unauthorized)
5432/tcp open  postgresql?
8080/tcp open  http            Apache httpd
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|_  Potentially risky methods: TRACE
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10:1607
OS details: Microsoft Windows 10 1607
Network Distance: 0 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-08-26T05:52:47
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

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 23.93 seconds
```

e) **nmap -v -p139,445 --script=smb-vuln-*.nse --script-args=unsafe=1 192.168.0.15** (Ejecuta un escaneo enfocado en las vulnerabilidades de SMB (Server Message Block), un protocolo de red utilizado para compartir archivos e impresoras en redes locales).

```
C:\Program Files (x86)\Nmap>nmap -v -p139,445 --script=smb-vuln-*.nse --script-args=unsafe=1 192.168.0.15
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-25 23:54 Hora estßndar central (MÚxico)
NSE: Loaded 11 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 23:54
Completed NSE at 23:54, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 23:54
Completed Parallel DNS resolution of 1 host. at 23:54, 0.02s elapsed
Initiating SYN Stealth Scan at 23:54
Scanning 192.168.0.15 [2 ports]
Discovered open port 139/tcp on 192.168.0.15
Discovered open port 445/tcp on 192.168.0.15
Completed SYN Stealth Scan at 23:54, 0.01s elapsed (2 total ports)
NSE: Script scanning 192.168.0.15.
Initiating NSE at 23:54
Completed NSE at 23:55, 12.83s elapsed
Nmap scan report for 192.168.0.15
Host is up (0.0010s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_smb-vuln-ms10-054: ERROR: Script execution failed (use -d to debug)

NSE: Script Post-scanning.
Initiating NSE at 23:55
Completed NSE at 23:55, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 13.31 seconds
           Raw packets sent: 2 (88B) | Rcvd: 5 (216B)
```

f) **nmap -p445 --script smb-vuln-ms17-010 192.168.0.15** (Ejecuta un escaneo en el host con mi dirección IP 192.168.0.15, focalizado en la vulnerabilidad específica MS17-010 en el servicio SMB (Server Message Block) que utiliza el puerto 445.)

```
C:\Program Files (x86)\Nmap>nmap -p445 --script smb-vuln-ms17-010 192.168.0.15
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-26 00:16 Hora estßndar central (MÚxico)
Nmap scan report for 192.168.0.15
Host is up (0.00s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 1.54 seconds
```

Ahora bien, ejecuté 10 comandos más solicitados por el profesor:

1. **nmap -sn 192.168.0.0/24** (Escaneo de ping (sin barrido de puertos) en una red completa para detectar hosts activos).

```
C:\Program Files (x86)\Nmap>nmap -sn 192.168.0.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-26 00:39 Hora estßndar central (MÚxico)
Nmap scan report for 192.168.0.1
Host is up (0.012s latency).
MAC Address: 48:4B:D4:11:07:E6 (Technicolor CH USA)
Nmap scan report for 192.168.0.10
Host is up (0.0020s latency).
MAC Address: 48:4B:D4:11:07:E8 (Technicolor CH USA)
Nmap scan report for 192.168.0.16
Host is up (0.0050s latency).
MAC Address: 90:9A:4A:2B:1D:85 (TP-Link Technologies)
Nmap scan report for 192.168.0.28
Host is up (0.011s latency).
MAC Address: 12:C1:E1:D5:47:02 (Unknown)
Nmap scan report for 192.168.0.15
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 8.29 seconds
```

2. **nmap -p T:80,U:53 192.168.0.15** (Escaneo TCP en el puerto 80 y escaneo UDP en el puerto 53 en el host 192.168.0.15).

```
C:\Program Files (x86)\Nmap>nmap -p T:80,U:53 192.168.0.15
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-26 00:42 Hora estßndar central (MÚxico)
WARNING: Your ports include "U:" but you haven't specified UDP scan with -sU.
Nmap scan report for 192.168.0.15
Host is up (0.00s latency).

PORT   STATE  SERVICE
80/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

3. **nmap -O 192.168.0.15** (Detección del sistema operativo).

```
C:\Program Files (x86)\Nmap>nmap -O 192.168.0.15
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-26 00:43 Hora estßndar central (MÚxico)
Nmap scan report for 192.168.0.15
Host is up (0.00035s latency).
Not shown: 992 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
3306/tcp open  mysql
5432/tcp open  postgresql
8080/tcp open  http-proxy
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10:1607
OS details: Microsoft Windows 10 1607
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.47 seconds
```

4. **nmap -sU -p123 192.168.0.15** (Escaneo UDP en el puerto 123 (NTP)).

```
C:\Program Files (x86)\Nmap>nmap -sU -p123 192.168.0.15
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-26 00:44 Hora estßndar central (MÚxico)
Nmap scan report for 192.168.0.15
Host is up.

PORT    STATE         SERVICE
123/udp open|filtered ntp

Nmap done: 1 IP address (1 host up) scanned in 2.39 seconds
```

5. **nmap -p- -sV 192.168.0.15** (Escaneo de todos los puertos y detección de servicios y versiones).

```
C:\Program Files (x86)\Nmap>nmap -p- -sV 192.168.0.15
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-26 00:45 Hora estßndar central (MÚxico)
Nmap scan report for 192.168.0.15
Host is up (0.00079s latency).
Not shown: 65517 closed tcp ports (reset)
PORT      STATE    SERVICE         VERSION
135/tcp   open     msrpc           Microsoft Windows RPC
137/tcp   filtered netbios-ns
139/tcp   open     netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open     microsoft-ds?
902/tcp   open     ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp   open     vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
3306/tcp  open     mysql           MySQL (unauthorized)
5040/tcp  open     unknown
5432/tcp  open     postgresql?
7680/tcp  open     pando-pub?
8080/tcp  open     http            Apache httpd
33060/tcp open     mysqlx?
49664/tcp open     msrpc           Microsoft Windows RPC
49665/tcp open     msrpc           Microsoft Windows RPC
49666/tcp open     msrpc           Microsoft Windows RPC
49667/tcp open     msrpc           Microsoft Windows RPC
49668/tcp open     msrpc           Microsoft Windows RPC
49674/tcp open     msrpc           Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port33060-TCP:V=7.94%I=7%D=8/26%Time=64E99FAF%P=i686-pc-windows-windows
SF:%r(NULL,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(GenericLines,9,"\x05\0\0\0\
SF:x0b\x08\x05\x1a\0")%r(GetRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(HT
SF:TPOptions,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(RTSPRequest,9,"\x05\0\0\0
SF:\x0b\x08\x05\x1a\0")%r(RPCCheck,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(DNS
SF:VersionBindReqTCP,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(DNSStatusRequestT
SF:CP,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\
SF:x0fInvalid\x20message\"\x05HY000")%r(Help,9,"\x05\0\0\0\x0b\x08\x05\x1a
SF:\0")%r(SSLSessionReq,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08
SF:\x01\x10\x88'\x1a\x0fInvalid\x20message\"\x05HY000")%r(TerminalServerCo
SF:okie,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(TLSSessionReq,2B,"\x05\0\0\0\x
SF:0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20messa
SF:ge\"\x05HY000")%r(Kerberos,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(SMBProgN
SF:eg,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(X11Probe,2B,"\x05\0\0\0\x0b\x08\
SF:x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"\x0
SF:5HY000")%r(FourOhFourRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LPDStr
SF:ing,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LDAPSearchReq,2B,"\x05\0\0\0\x0
SF:b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20messag
SF:e\"\x05HY000")%r(LDAPBindReq,46,"\x05\0\0\0\x0b\x08\x05\x1a\x009\0\0\0\
SF:x01\x08\x01\x10\x88'\x1a\*Parse\x20error\x20unserializing\x20protobuf\x
SF:20message\"\x05HY000")%r(SIPOptions,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r
SF:(LANDesk-RC,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(TerminalServer,9,"\x05\
SF:0\0\0\x0b\x08\x05\x1a\0")%r(NCP,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(Not
SF:esRPC,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x
```

6. **nmap -v -A 192.168.0.15** (Escaneo completo que incluye detección de sistema operativo, detección de servicios y trazado de ruta en el host).

```
C:\Program Files (x86)\Nmap>nmap -v -A 192.168.0.15
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-26 00:59 Hora estßndar central (MÚxico)
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 01:13
Completed NSE at 01:13, 0.00s elapsed
Initiating NSE at 01:13
Completed NSE at 01:13, 0.00s elapsed
Initiating NSE at 01:13
Completed NSE at 01:13, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 01:13
Completed Parallel DNS resolution of 1 host. at 01:13, 0.02s elapsed
Initiating SYN Stealth Scan at 01:13
Scanning 192.168.0.15 [1000 ports]
Discovered open port 3306/tcp on 192.168.0.15
Discovered open port 135/tcp on 192.168.0.15
Discovered open port 8080/tcp on 192.168.0.15
Discovered open port 139/tcp on 192.168.0.15
Discovered open port 445/tcp on 192.168.0.15
Discovered open port 902/tcp on 192.168.0.15
Discovered open port 912/tcp on 192.168.0.15
Discovered open port 5432/tcp on 192.168.0.15
Completed SYN Stealth Scan at 01:13, 0.06s elapsed (1000 total ports)
Initiating Service scan at 01:13
Scanning 8 services on 192.168.0.15
Completed Service scan at 01:13, 7.22s elapsed (8 services on 1 host)
Initiating OS detection (try #1) against 192.168.0.15
NSE: Script scanning 192.168.0.15.
Initiating NSE at 01:13
Completed NSE at 01:13, 14.29s elapsed
Initiating NSE at 01:13
Completed NSE at 01:13, 0.31s elapsed
Initiating NSE at 01:13
Completed NSE at 01:13, 0.00s elapsed
Nmap scan report for 192.168.0.15
Host is up (0.00072s latency).
Not shown: 992 closed tcp ports (reset)
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?
902/tcp  open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp  open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
3306/tcp open  mysql           MySQL (unauthorized)
5432/tcp open  postgresql?
8080/tcp open  http            Apache httpd
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|   Supported Methods: POST OPTIONS HEAD GET TRACE
|_  Potentially risky methods: TRACE
|_http-open-proxy: Proxy might be redirecting requests
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10:1607
OS details: Microsoft Windows 10 1607
Uptime guess: 14.356 days (since Fri Aug 11 16:41:24 2023)
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

7. **nmap -sS -Pn 192.168.0.15** (Escaneo de tipo SYN (Stealth Scan) sin hacer ping para determinar los puertos abiertos).

```
C:\Program Files (x86)\Nmap>nmap -sS -Pn 192.168.0.15
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-26 01:14 Hora estßndar central (MÚxico)
Nmap scan report for 192.168.0.15
Host is up (0.00081s latency).
Not shown: 992 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
3306/tcp open  mysql
5432/tcp open  postgresql
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
```

8. **nmap -p80 --script http-enum 192.168.0.15** (Escaneo en el puerto 80 utilizando un script para enumerar directorios y archivos en un servidor web).

```
C:\Program Files (x86)\Nmap>nmap -p80 --script http-enum 192.168.0.15
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-26 01:16 Hora estßndar central (MÚxico)
Nmap scan report for 192.168.0.15
Host is up (0.00s latency).

PORT   STATE  SERVICE
80/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
```

9. **nmap -T4 -F 192.168.0.15** (Escaneo rápido en el host 192.168.0.15 usando una velocidad de escaneo más rápida y solo los puertos más comunes).

```
C:\Program Files (x86)\Nmap>nmap -T4 -F 192.168.0.15
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-26 01:17 Hora estßndar central (MÚxico)
Nmap scan report for 192.168.0.15
Host is up (0.00045s latency).
Not shown: 94 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
5432/tcp open  postgresql
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

10. **nmap -p445 --script smb-vuln-cve-2017-7494 192.168.0.15** (Escaneo en el puerto 445 para la vulnerabilidad CVE-2017-7494 en el servicio SMB).

```
C:\Program Files (x86)\Nmap>nmap -p445 --script smb-vuln-cve-2017-7494 192.168.0.15
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-26 01:17 Hora estßndar central (MÚxico)
Nmap scan report for 192.168.0.15
Host is up (0.00s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 1.40 seconds
```

Conclusión

La práctica me proporcionó una visión general sobre cómo utilizar Nmap para explorar redes y sistemas. Aprendí a ejecutar diferentes tipos de escaneos, desde descubrimiento de hosts hasta detección de vulnerabilidades. Sin embargo, hay que recordar que la seguridad y la ética son fundamentales al utilizar herramientas como Nmap. Siempre se debe asegurar de tener permisos y consentimiento antes de realizar escaneos y respetar las leyes y políticas aplicables. Nmap, como herramienta versátil, puede ayudarnos a identificar problemas de seguridad y configuración, pero es nuestra responsabilidad utilizarla de manera responsable para mejorar la seguridad y protección de sistemas y redes.