UNIVERSIDAD DEL ISTMO

UNISTMO TEHUANTEPEC

DOCENTE:

ING. CARLOS MIJANGOS JIMENEZ.

ASIGNATURA:

REDES DE COMPUTADORAS II.

TEMA:

WIRESHARK Y NMAP.

ALUMNOS:

PALACIOS TRINIDAD MARIANA.

CARRERA:

INGENIERÍA EN COMPUTACIÓN.

GRUPO:

704.

PARCIAL:

SEGUNDO PARCIAL.

SANTO DOMINGO TEHUANTEPEC, OAXACA; 17 DE NOVIEMBRE DE 2025.

Índice

Introducción

Nmap, al igual que Wireshark, es una herramienta de código abierto y es utilizada para el descubrimiento de redes y auditorías de seguridad. Se puede usar para escanear redes y encontrar hosts activos, detectar puertos abiertos, identificar servicios y sus versiones, y determinar el sistema operativo de los dispositivos.

Algunos de los escaneos más comunes son:

Ping Scan: identifica si un host está activo sin revisar puertos.

SYN Scan: rápido y difícil de detectar, envía paquetes SYN sin completar la conexión.

TCP Connect Scan: completa la conexión TCP, es más detectable pero útil sin permisos elevados.

UDP Scan: analiza puertos UDP para servicios como DNS o DHCP, aunque puede generar falsos positivos.

También ofrece **detección de versiones** y **detección de sistema operativo**, útil pero más fácil de registrar por los sistemas de seguridad.

Ambos tipos generan tráfico muy particular, por lo que son más fáciles de detectar.

Wireshark, por su parte, es un analizador de protocolos que captura y muestra el tráfico de red en detalle. Se usa principalmente en defensa, ya que permite detectar comportamientos anómalos, escaneos de puertos o intentos de intrusión mediante filtros que revelan patrones como SYN scans o conexiones sospechosas.

Para la realización de esta práctica se utilizaron dos equipos: un dispositivo atacante con sistema operativo Windows 11 y una máquina virtual con Linux Mint 22.2 como equipo objetivo. Fue necesario contar con una red local donde ambos dispositivos estuvieran conectados, así como tener instaladas las herramientas Nmap y Wireshark. También se requirió conocer las direcciones IP asignadas a cada equipo para realizar los escaneos y capturas de tráfico de forma correcta.

La ip del dispositivo Linux es: 192.168.56.101 con la configuración en solo host (en un principio era 192.168.56.101 pero se modificó a 0.22 debido a la configuración de la máquina virtual que la cambié a puente)

De igual forma, se abrió el puerto 5500. Y se ejecutaron los siguientes comandos:

sudo ufw allow 5500/tcp para abrir el puerto 5500

sudo ufw status para visualizar el estado del firewall.

```
mariana@mariana-VirtualBox:~$ ss -tulwn | grep 5500
tcp   LISTEN 0      511          0.0.0.0:5500       0.0.0.0:*
mariana@mariana-VirtualBox:~$ sudo ufw allow 5500/tcp
[sudo] contraseña para mariana:
Regla añadida
Regla añadida (v6)
mariana@mariana-VirtualBox:~$ sudo ufw status
Estado: activo

Hasta                      Acción      Desde
-----                      ------      -----
Anywhere                   ALLOW       192.168.0.0/24
22/tcp                     ALLOW       192.168.0.0/24
5500/tcp                   ALLOW       Anywhere
5500/tcp (v6)              ALLOW       Anywhere (v6)
```

Desarrollo

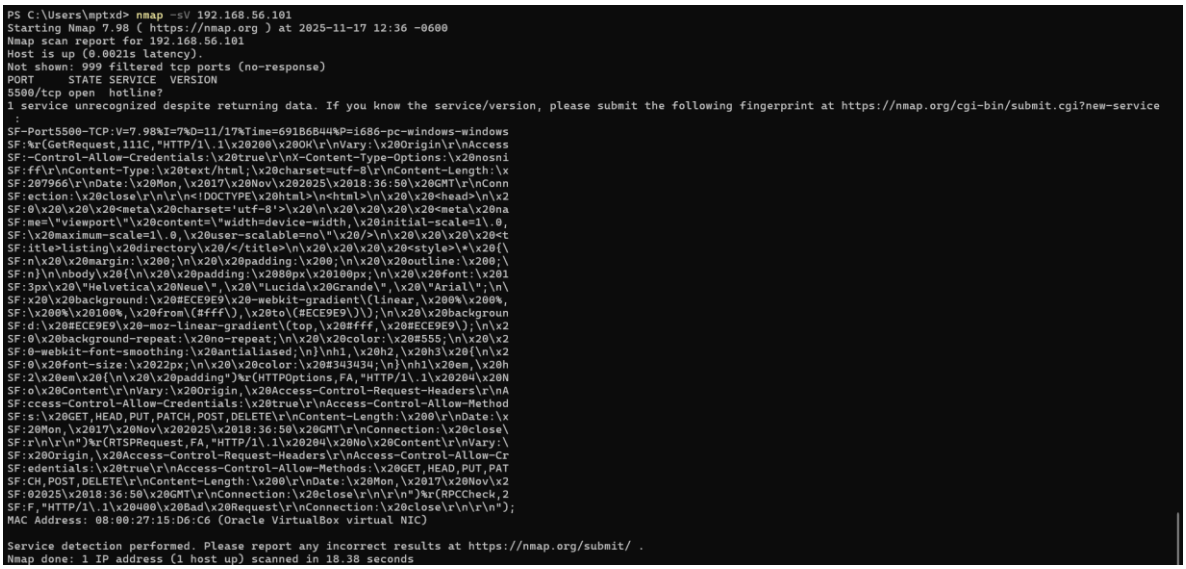
Escaneos con Nmap:

1. **Comando nmap -sV 192.168.56.101**

Descripción de funcionamiento:

Realiza un escaneo de servicios y versiones en el host especificado.

Es ideal para auditorias donde se quiere saber qué servicios se están ejecutando y qué versiones tiene.



2. **Comando nmap -sn 192.168.56.101**

Descripción de funcionamiento:

Realiza un escaneo sin puertos, únicamente para determinar si el host está activo.

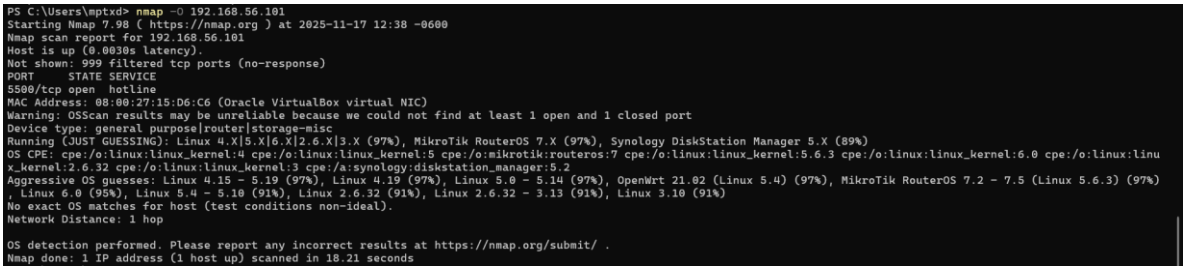
```
PS C:\Users\mptxd> nmap -sn 192.168.56.101
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-17 12:37 -0600
Nmap scan report for 192.168.56.101
Host is up (0.0020s latency).
MAC Address: 08:00:27:15:D6:C6 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.77 seconds
```

3. **Comando nmap -O 192.168.56.101**

Descripción de funcionamiento:

Realiza un escaneo de sistema operativo, intentando identificar la plataforma (Linux, Windows, etc.).

Se utiliza para identificar el SO del objetico, apoyar evaluaciones de seguridad y categorizar dispositivos dentro de una red.



4. **Comando nmap -sn -vv -packet-trace -Pn 192.168.56.101**

Descripción de funcionamiento:

Este comando realiza un **escaneo sin puertos**, con un nivel de detalle muy alto y mostrando *traza completa de paquetes*, ignorando el descubrimiento de host por ping.

Sirve principalmente para **diagnóstico**, depuración y análisis detallado de lo que Nmap está enviando y recibiendo.

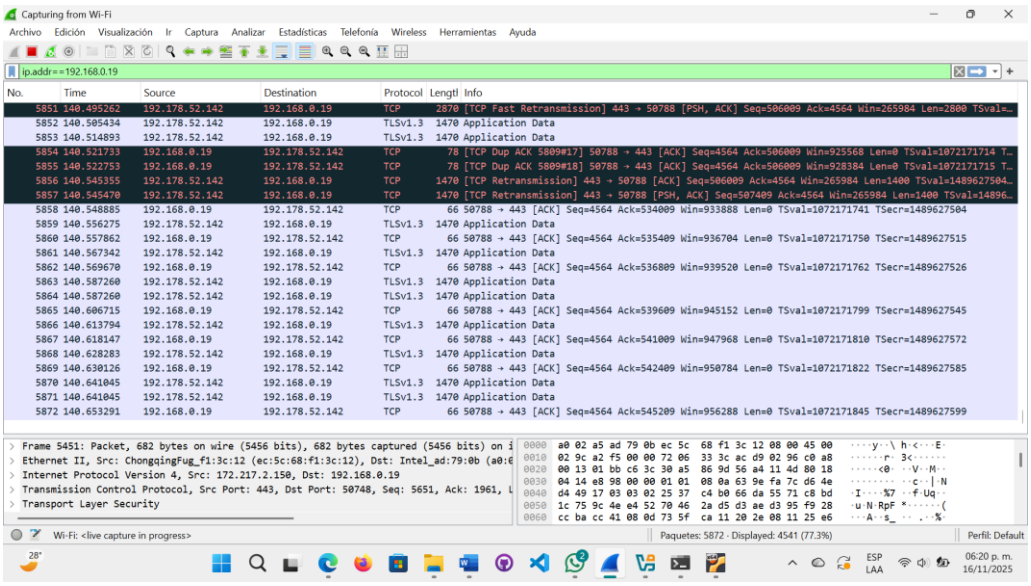
```
PS C:\Users\mptxd> nmap -sn -vv --packet-trace -Pn 192.168.56.101
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-17 12:27 -0600
NSOCK INFO [0.0290s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.0300s] nsock_connect_udp(): UDP connection requested to 200.52.173.50:53 (IOD #1) EID 8
NSOCK INFO [0.0300s] nsock_iod_new2(): nsock_iod_new (IOD #2)
NSOCK INFO [0.0310s] nsock_connect_udp(): UDP connection requested to 200.52.170.150:53 (IOD #2) EID 16
NSOCK INFO [0.0310s] nsock_iod_new2(): nsock_iod_new (IOD #3)
NSOCK INFO [0.0320s] nsock_connect_udp(): UDP connection requested to 189.197.62.74:53 (IOD #3) EID 24
NSOCK INFO [0.0320s] nsock_iod_new2(): nsock_iod_new (IOD #4)
NSOCK INFO [0.0330s] nsock_connect_udp(): UDP connection requested to 2806:260:1001:100:200:52:173:50:53 (IOD #4) EID 32
NSOCK INFO [0.0330s] nsock_trace_handler_callback(): Callback: CONNECT ERROR [Se ha intentado una operación de socket en una red no accesible.  (10051)] for EID 32 [2806:
260:1001:100:200:52:173:50:53]
NSOCK INFO [0.0330s] nsock_iod_new2(): nsock_iod_new (IOD #5)
NSOCK INFO [0.0370s] nsock_connect_udp(): UDP connection requested to 2806:260:1003:100:200:52:170:150:53 (IOD #5) EID 40
NSOCK INFO [0.0370s] nsock_trace_handler_callback(): Callback: CONNECT ERROR [Se ha intentado una operación de socket en una red no accesible.  (10051)] for EID 40 [2806:
260:1003:100:200:52:170:150:53]
Initiating Parallel DNS resolution of 1 host. at 12:27
NSOCK INFO [0.0380s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [200.52.173.50:53]
NSOCK INFO [0.0380s] nsock_read(): Read request from IOD #1 [200.52.173.50:53] (timeout: -1ms) EID 50
NSOCK INFO [0.0380s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 16 [200.52.170.150:53]
NSOCK INFO [0.0380s] nsock_read(): Read request from IOD #2 [200.52.170.150:53] (timeout: -1ms) EID 58
NSOCK INFO [0.0380s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 24 [189.197.62.74:53]
NSOCK INFO [0.0390s] nsock_read(): Read request from IOD #3 [189.197.62.74:53] (timeout: -1ms) EID 66
NSOCK INFO [0.0390s] nsock_write(): Write request for 45 bytes to IOD #1 EID 75 [200.52.173.50:53]
NSOCK INFO [0.0400s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 75 [200.52.173.50:53]
NSOCK INFO [0.0590s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 50 [200.52.173.50:53] (122 bytes)
NSOCK INFO [0.0590s] nsock_read(): Read request from IOD #1 [200.52.173.50:53] (timeout: -1ms) EID 82
Completed Parallel DNS resolution of 1 host. at 12:27, 0.50s elapsed
NSOCK INFO [0.5400s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [0.5400s] nevent_delete(): nevent_delete on event #82 (type READ)
NSOCK INFO [0.5400s] nsock_iod_delete(): nsock_iod_delete (IOD #2)
NSOCK INFO [0.5400s] nevent_delete(): nevent_delete on event #58 (type READ)
NSOCK INFO [0.5400s] nsock_iod_delete(): nsock_iod_delete (IOD #3)
NSOCK INFO [0.5400s] nevent_delete(): nevent_delete on event #66 (type READ)
NSOCK INFO [0.5400s] nsock_iod_delete(): nsock_iod_delete (IOD #4)
NSOCK INFO [0.5400s] nsock_iod_delete(): nsock_iod_delete (IOD #5)
Nmap scan report for 192.168.56.101
Host is up, received user-set.
Nmap done: 1 IP address (1 host up) scanned in 0.54 seconds
```

Monitoreo con Wireshark:

1. **ip.addr == 192.168.0.19**

Muestra todo el tráfico IP donde la dirección IP 192.168.0.19 aparece ya sea como origen o como destino.

Funciona para ver toda la actividad de un host de red e identificar conexiones entrantes y salientes.

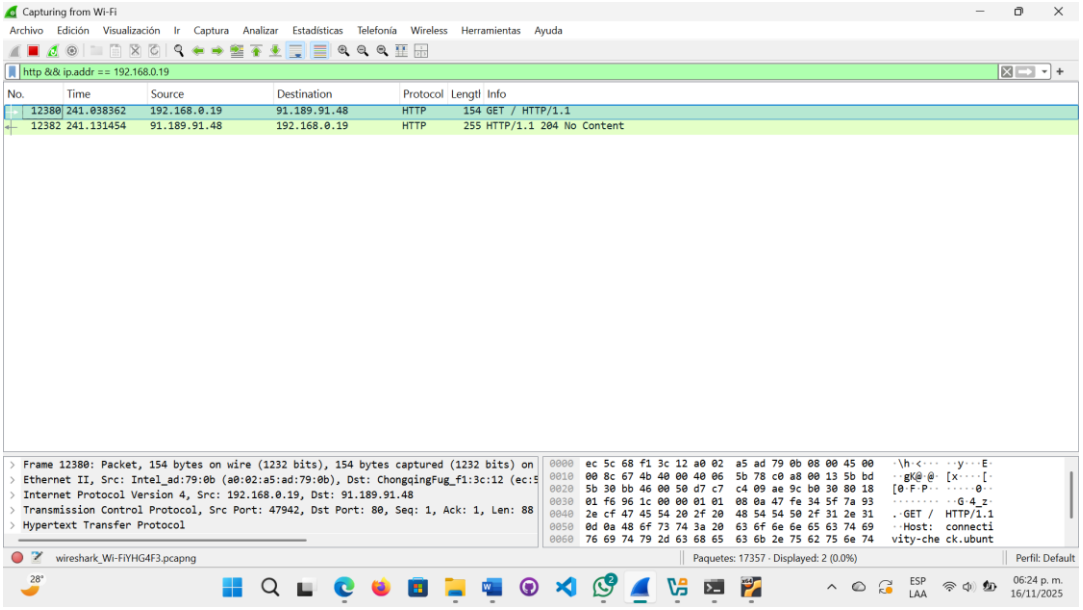


Se navega a una página HTTP y se observaron solicitudes de tipo **GET** y sus respuestas con contenido en texto claro.

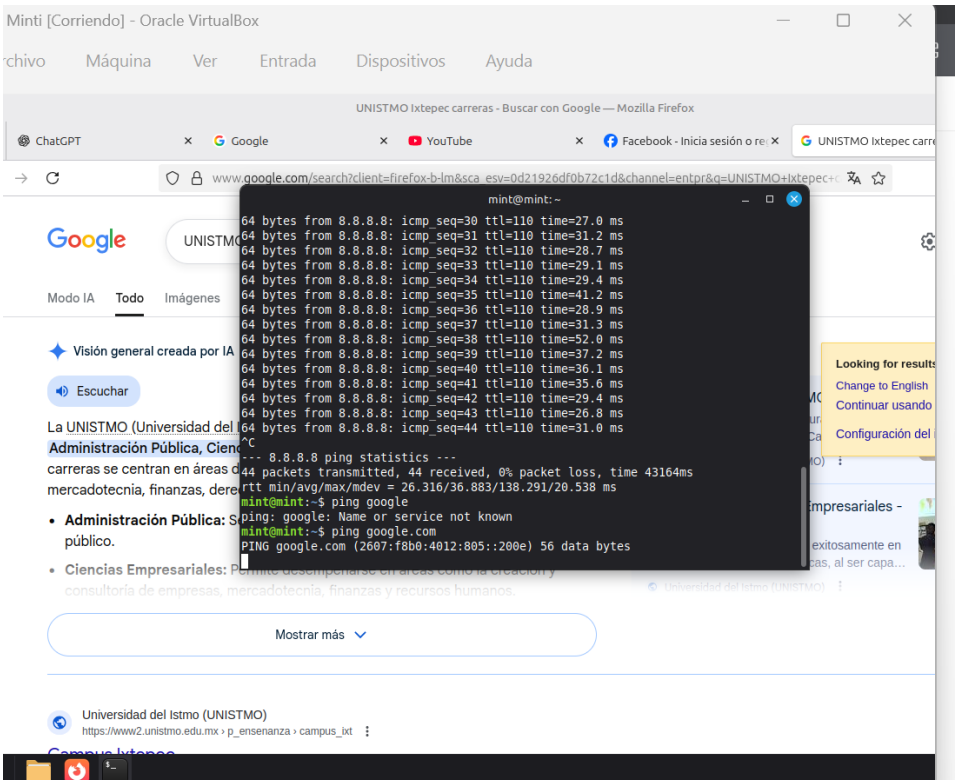
2. **http && ip.addr == 192.168.0.19**

Filtra únicamente **paquetes HTTP** que involucren a la dirección **192.168.0.19**, ya sea como origen o destino.

Se utiliza para ver solicitudes HTTP hechas por el host (GET, POST, etc.).



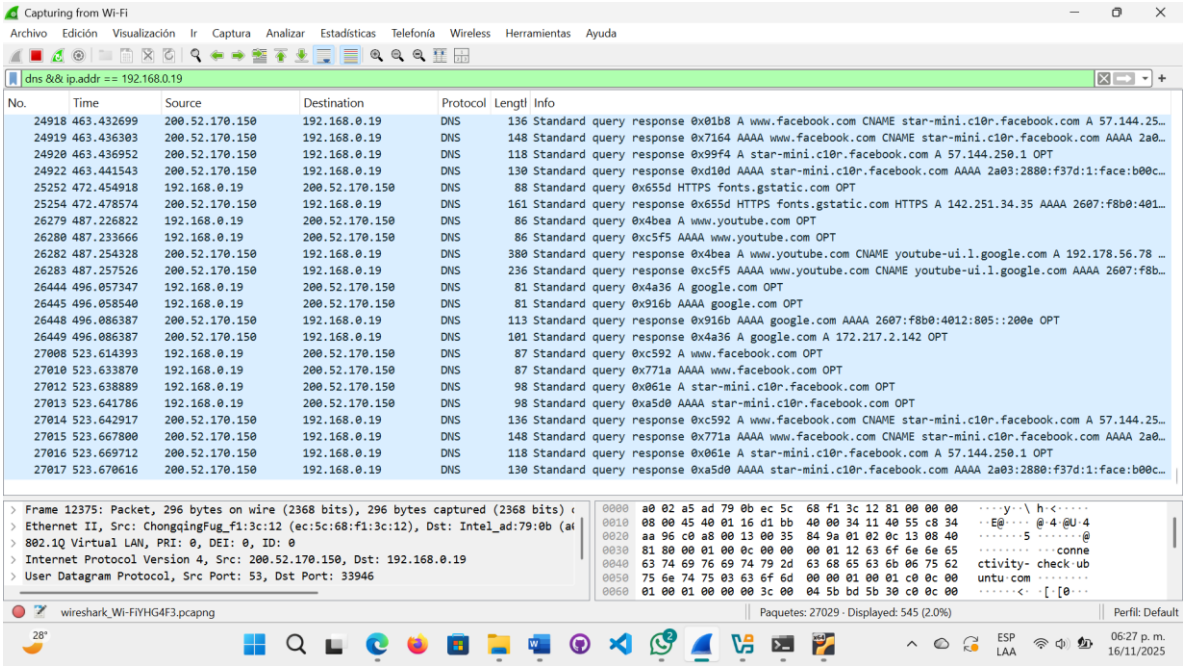
Se ejecutó el comando ping google.com y se visualizaron consultas y respuestas del protocolo **DNS**.



3. dns && ip.addr == 192.168.0.19

Muestra únicamente **tráfico DNS** en el que participa **192.168.0.19**.

Se utiliza para identificar dominios que consulta un equipo, revisar anomalías como demasiadas consultas, fallos de respuesta, etc.



Conclusiones

El uso combinado de Nmap y Wireshark permite comprender de manera práctica cómo funcionan las fases de reconocimiento y análisis dentro de una red. Con Nmap fue posible identificar hosts activos, detectar puertos abiertos, conocer servicios y versiones en ejecución, así como obtener información del sistema operativo del objetivo, lo que demuestra su utilidad tanto en auditorías de seguridad como en pruebas de penetración.

Por otro lado, Wireshark facilitó la observación detallada del tráfico generado durante los escaneos y otras actividades, permitiendo visualizar protocolos como HTTP y DNS, y entender cómo se intercambia la información dentro de la red.

En conjunto, ambas herramientas refuerzan la importancia del análisis de tráfico y del reconocimiento controlado para fortalecer la seguridad, detectar comportamientos anómalos y comprender mejor la estructura y el funcionamiento de una red informática.

Como recomendación, es importante realizar estos análisis únicamente en entornos controlados y autorizados para evitar riesgos legales o de seguridad. También se sugiere mantener las herramientas actualizadas, ya que sus bases de detección y funcionalidades mejoran constantemente. Además, se recomienda complementar este tipo de prácticas con

configuraciones de firewall y monitoreo continuo para identificar rápidamente actividades sospechosas dentro de una red real.

Referencias

- Lyon, G. F. (2009). *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. Insecure.Com LLC.
- Combs, G. (2023). *Wireshark User's Guide*. Wireshark Foundation.
- Stallings, W. (2021). *Network Security Essentials: Applications and Standards* (7th ed.). Pearson.