P R Á C T I C A ONCE

NOMBRE: Escaneo de Redes Nmap.		**TEMA:** Cuatro.	número	11
SUBTEMA: 4.3 Políticas de Seguridad.	**VALOR:** 25%	**LUGAR:** Aula de clases		
ALUMNOS: Diana Paola Santiago Pelayo Clara Luz Milagro García Brenda Ciclali Ortiz Fonseca Ricardo Samuel Carranza Marcial	**GRUPO:** 803AB	**FECHA:** 12/05/2025		

1. Objetivo.

Instalar y configurar Nmap, para realizar el escaneo de la red.

2. Material a usar

Hardware:
- PC, Dispositivo móvil o tableta por alumno

Software:
- Procesador de texto mínimo.
- Oracle VM Virtual Box.
- Ubuntu Server.
- Windows Server.

De apoyo:
- Internet
- Apuntes de la clase

4. Marco Teórico

Seguridad.

Es el conjunto de políticas, tecnologías y prácticas diseñadas para proteger la infraestructura de red, los datos y los sistemas conectados contra accesos no autorizados, ataques cibernéticos, fugas de información y otros riesgos.

Nmap.

Es una herramienta gratuita y de código abierto utilizada para el descubrimiento de hosts y el escaneo de puertos en redes. Es ampliamente empleado en seguridad informática, auditorías de red y administración de sistemas debido a su versatilidad y potencia

Características principales:

- ✓ Descubrimiento de hosts: Detecta dispositivos activos en una red.
- ✓ Escaneo de puertos: Identifica puertos abiertos y servicios en ejecución.
- ✓ Detección de sistemas operativos.
- ✓ Evasión de Firewalls/IDS.
- ✓ Personalización y Rendimiento.
- ✓ Multiplataforma.
- ✓ Soporte para Redes Complejas.

Una de las herramientas básicas para el escaneo de la red es Nmap, también conocido como Network Mapper. Este programa escanea un objetivo e informa qué puertos están abiertos y cerrados, además de otras cosas. Los especialistas en seguridad usan este programa para probar la seguridad de una red.

4. Metodología

PASOS PARA REALIZAR LA PRACTICA:

Paso 1: Descargar Nmap.

Paso 2: Instalar y configurar Nmap en el sistema Operativo de su preferencia.

Paso 3: Ejecutar Nmap-zmap GNU.

Paso 4: Posteriormente establece un objetivo: un sitio web o una dirección, para la realización de la práctica introduce la **dirección de red de tu computadora.**

Paso 5: Realiza el **escaneo simple de red**, realiza la captura de pantallas.

REPORTE DE LA PRÁCTICA

6. Desarrollo

Contestas las siguientes preguntas:

1.- ¿Por qué elegiste instalar Nmap en el sistema operativo seleccionado?

Diana Paola Santiago Pelayo: Elegí instalar Nmap en Windows 11 porque es el sistema operativo que ya tengo instalado en mi computadora y con el que me siento más familiarizada. Además, Nmap cuenta con una versión compatible para Windows que incluye Zenmap, su interfaz gráfica, lo cual facilita mucho la ejecución de escaneos sin necesidad de usar únicamente la línea de comandos, como en el caso de Ubuntu Server. Al usar Windows 11, también pude comprobar que la herramienta funciona correctamente en sistemas actuales y me permitió analizar mi propia red de forma práctica.

2.- Describe mediante el uso de una tabla los comandos básicos al utilizar Nmap.

Ricardo Samuel Carranza Marcial:

COMANDO	EJEMPLO	DESCRIPCIÓN
nmap [objetivo]	nmap 192.168.0.1	Escanea un objetivo (IP, dominio o rango) para detectar hosts y puertos abiertos.
nmap [obj1] [obj2] ...	nmap 192.168.0.1 192.168.0.2	Escanea múltiples objetivos.
nmap -iL [archivo.txt]	nmap -iL lista.txt	Escanea una lista de objetivos desde un archivo.
nmap [rango IPs]	nmap 192.168.0.1-10	Escanea un rango de direcciones IP.
nmap [subred/cidr]	nmap 192.168.0.1/24	Escanea toda una subred.
nmap -iR [número]	nmap -iR 5	Escanea un número aleatorio de hosts.
nmap --exclude [objetivos]	nmap 192.168.0.1/24 --exclude 192.168.0.100	Excluye objetivos específicos del escaneo.
nmap --excludefile [archivo]	nmap 192.168.0.1/24 --excludefile no.txt	Excluye una lista de objetivos desde archivo.
nmap -A [objetivo]	nmap -A 192.168.0.1	Escaneo agresivo: detección de SO, servicios, scripts y traceroute.
nmap -6 [objetivo]	nmap -6 2607:f0d0:1002:51::4	Escaneo de objetivos IPv6.

nmap -sn [objetivo]	nmap -sn 192.168.0.1/24	Descubrimiento de hosts (ping scan, sin escaneo de puertos).
nmap -p [puerto(s)] [obj]	nmap -p 80,443 192.168.0.1	Escaneo de puertos específicos.
nmap -F [objetivo]	nmap -F 192.168.0.1	Escaneo rápido (solo los puertos más comunes).
nmap -sS [objetivo]	nmap -sS 192.168.0.1	Escaneo SYN (stealth scan).
nmap -sU [objetivo]	nmap -sU 192.168.0.1	Escaneo de puertos UDP.
nmap -v [objetivo]	nmap -v 192.168.0.1	Modo detallado (verbose), muestra más información.
nmap -h	nmap -h	Muestra la ayuda de Nmap

3.- Describe las razones por la que un administrador de red debe de usar Nmap.

Clara Luz Milagro García: Un administrador de red debe usar Nmap porque es una herramienta muy útil para tener control y visibilidad total de todo lo que está conectado a la red. Permite ver qué dispositivos hay, qué servicios están usando y qué puertos tienen abiertos, lo cual ayuda a detectar problemas de seguridad, configuraciones incorrectas o accesos no autorizados. Además, con Nmap se pueden encontrar vulnerabilidades antes de que alguien las aproveche, ya que permite hacer análisis de seguridad detallados y automatizar estas tareas con scripts. También es muy útil para hacer auditorías y asegurar que la red cumple con las políticas establecidas, así como para tener un inventario completo de los equipos y servicios. También Nmap es gratuito, funciona en muchos sistemas operativos y se puede integrar con otras herramientas de seguridad, lo que lo hace una opción eficiente, económica y muy completa para administrar redes.

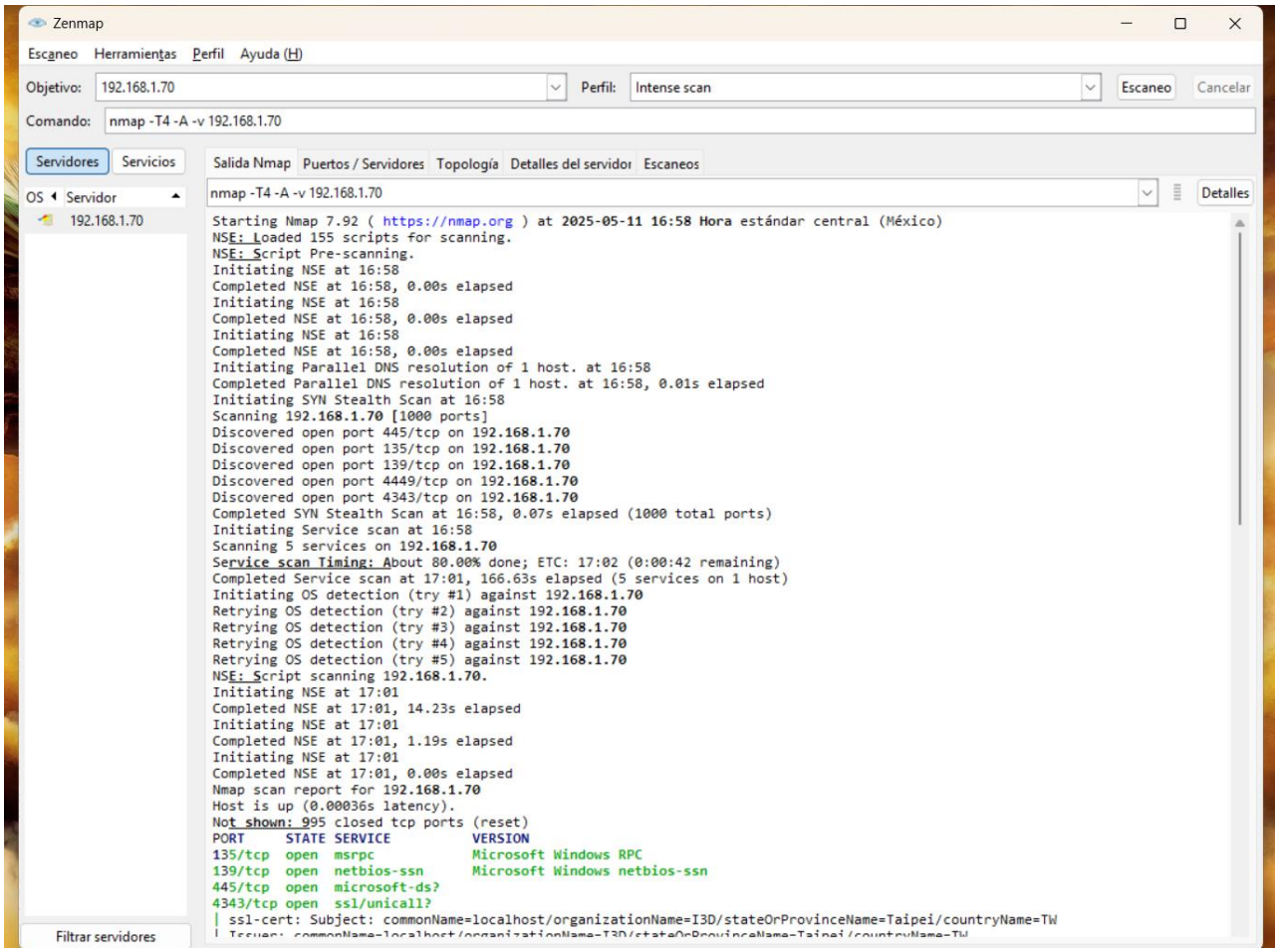
4.- ¿Por qué es importante obtener autorización antes de escanear una red con Nmap?

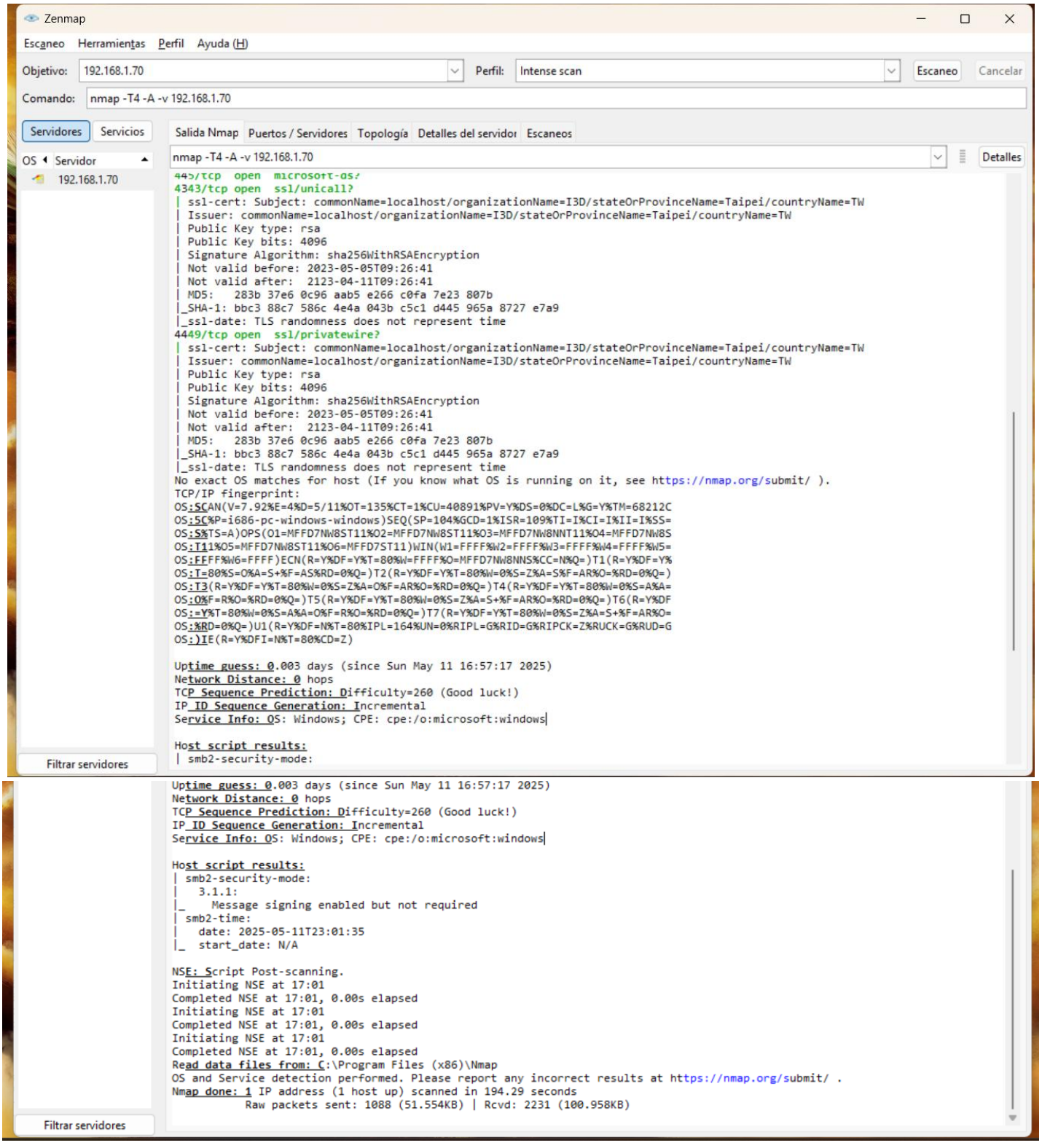
Brenda Ciclali Ortiz Fonseca: Es importante obtener autorización antes de escanear una red con Nmap porque realizar un escaneo no autorizado puede violar leyes de ciberseguridad y privacidad, lo que podría resultar en acciones legales, multas o incluso penas de cárcel. Además, muchos sistemas y redes monitorean actividades de escaneo no autorizadas, pudiendo interpretarlas como intentos de hacking o ataques cibernéticos, lo que puede llevar al bloqueo de la IP, denuncias o intervención de las autoridades. Siempre se debe contar con consentimiento explícito del propietario de la red para evitar riesgos legales y éticos.

7. Resultados

(Agregar capturas de pantalla del paso 5 y describe que es lo que muestra el escaneo simple de la red.

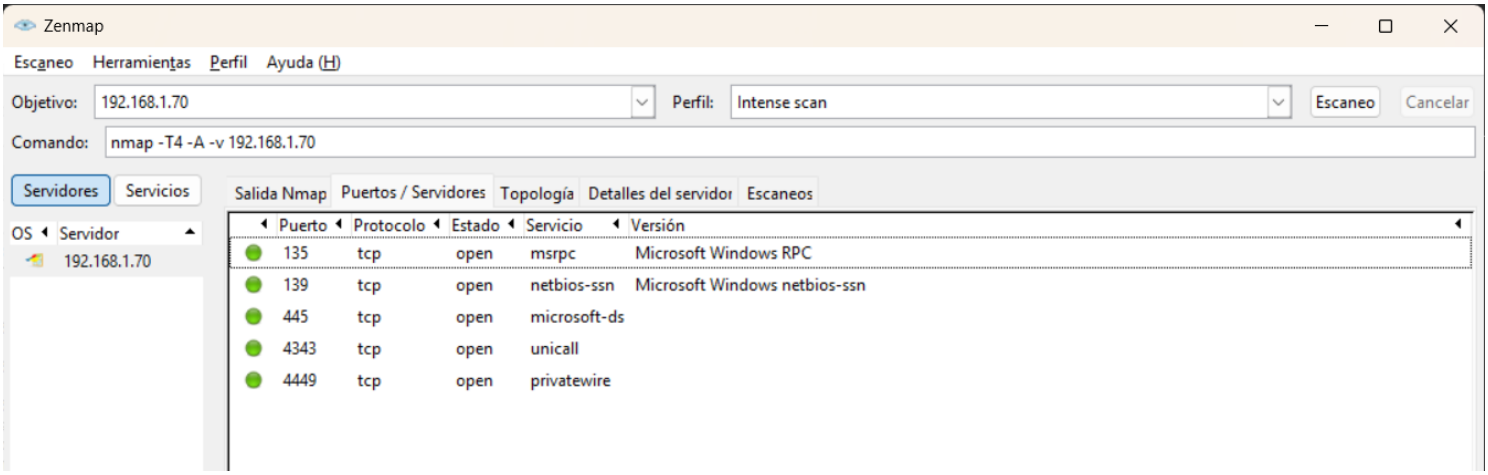
Abrimos Nmap y en objetivo ingresamos nuestra dirección IP y seleccionamos en perfil la opcion de Intense scan y le damos clic en Escaneo y esperamos a que realice el proceso correspondiente. Aquí realicé un escaneo con Nmap desde Zenmap directamente a mi computadora, que tiene la IP 192.168.1.70. El escaneo detectó que mi equipo está en línea y respondió casi de inmediato, lo que confirma que está conectado correctamente a la red local. Encontré cinco puertos TCP abiertos: el 135, 139 y 445, que son servicios típicos de Windows relacionados con la comunicación interna del sistema y la compartición de archivos. También aparecieron abiertos los puertos 4343 y 4449, que usan conexiones cifradas con SSL, aunque Nmap no logró identificar claramente qué servicios son. Ambos puertos tienen certificados autofirmados que están configurados para 'localhost' y fueron emitidos por una entidad llamada I3D, con sede en Taipei. Me parece que estos podrían estar relacionados con algún software específico que tengo instalado. Nmap no pudo identificar con precisión el sistema operativo, pero sí detectó características que coinciden con Windows, lo cual tiene sentido porque es el sistema que uso. Además, el escaneo indicó que mi equipo probablemente acababa de iniciar, lo cual también coincide porque lo encendí poco antes de hacer el análisis.



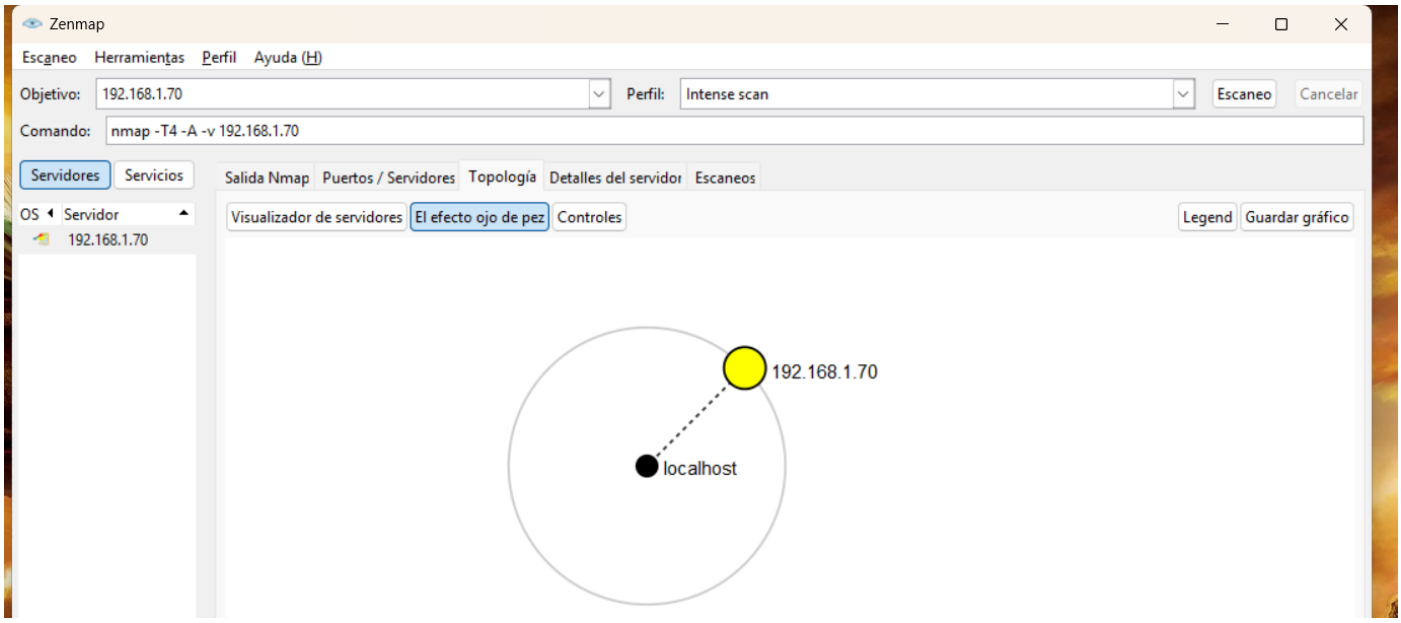

Zenmap
Escaneo Herramientas Perfil Ayuda (H)
Objetivo: 192.168.1.70
Perfil: Intense scan
Escaneo
Cancelar
Comando: nmap -T4 -A -v 192.168.1.70
Servidores
Servicios
Salida Nmap
Puertos / Servidores
Topología
Detalles del servidor
Escaneos
OS
Servidor
192.168.1.70
nmap -T4 -A -v 192.168.1.70
Detalles
4343/tcp open ssl/unicall?
| ssl-cert: Subject: commonName=localhost/organizationName=I3D/stateOrProvinceName=Taipei/countryName=TW
| Issuer: commonName=localhost/organizationName=I3D/stateOrProvinceName=Taipei/countryName=TW
| Public Key type: rsa
| Public Key bits: 4096
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-05-05T09:26:41
| Not valid after: 2123-04-11T09:26:41
| MD5: 283b 37e6 0c96 aab5 e266 c0fa 7e23 807b
|_SHA-1: bbc3 88c7 586c 4e4a 043b c5c1 d445 965a 8727 e7a9
|_ssl-date: TLS randomness does not represent time
4449/tcp open ssl/privatewire?
| ssl-cert: Subject: commonName=localhost/organizationName=I3D/stateOrProvinceName=Taipei/countryName=TW
| Issuer: commonName=localhost/organizationName=I3D/stateOrProvinceName=Taipei/countryName=TW
| Public Key type: rsa
| Public Key bits: 4096
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-05-05T09:26:41
| Not valid after: 2123-04-11T09:26:41
| MD5: 283b 37e6 0c96 aab5 e266 c0fa 7e23 807b
|_SHA-1: bbc3 88c7 586c 4e4a 043b c5c1 d445 965a 8727 e7a9
|_ssl-date: TLS randomness does not represent time
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=5/11%OT=135%CT=1%CU=40891%PV=Y%DS=0%DC=L%G=Y%TM=68212C
OS:5C%P=i686-pc-windows-windows)SEQ(SP=104%GCD=1%ISR=109%TI=I%CI=I%II=I%SS=
OS:S%TS=A)OPS(O1=MFFD7NW8ST11%O2=MFFD7NW8ST11%O3=MFFD7NW8NNT11%O4=MFFD7NW8S
OS:T11%O5=MFFD7NW8ST11%O6=MFFD7ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=
OS:FFFF%W6=FFFF)ECN(R=Y%DF=Y%T=80%W=FFFF%O=MFFD7NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%
OS:T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)
OS:T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=
OS:O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF
OS:=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=
OS:%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G%RUD=G
OS:)IE(R=Y%DFI=N%T=80%CD=Z)
Uptime guess: 0.003 days (since Sun May 11 16:57:17 2025)
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
Host script results:
| smb2-security-mode:
Filtrar servidores

Uptime guess: 0.003 days (since Sun May 11 16:57:17 2025)
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
Host script results:
| smb2-security-mode:
| 3.1.1:
|_ Message signing enabled but not required
| smb2-time:
| date: 2025-05-11T23:01:35
|_ start_date: N/A
NSE: Script Post-scanning.
Initiating NSE at 17:01
Completed NSE at 17:01, 0.00s elapsed
Initiating NSE at 17:01
Completed NSE at 17:01, 0.00s elapsed
Initiating NSE at 17:01
Completed NSE at 17:01, 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 194.29 seconds
Raw packets sent: 1088 (51.554KB) | Rcvd: 2231 (100.958KB)
Filtrar servidores

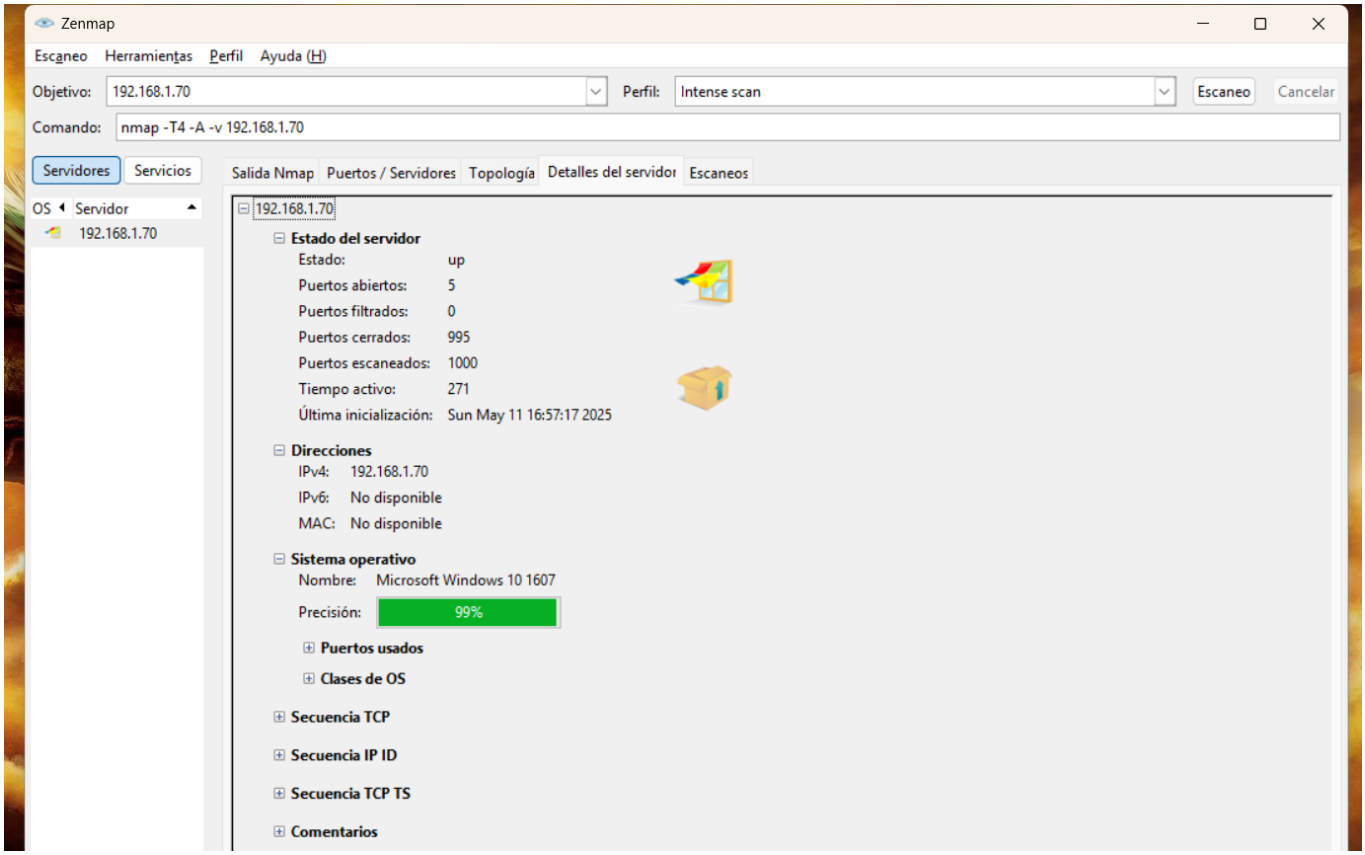
Aquí podemos observar los puertos que maneja mi computadora, que en este caso son tcp y todos están activos y nos muestra el nombre del servicio y su versión.



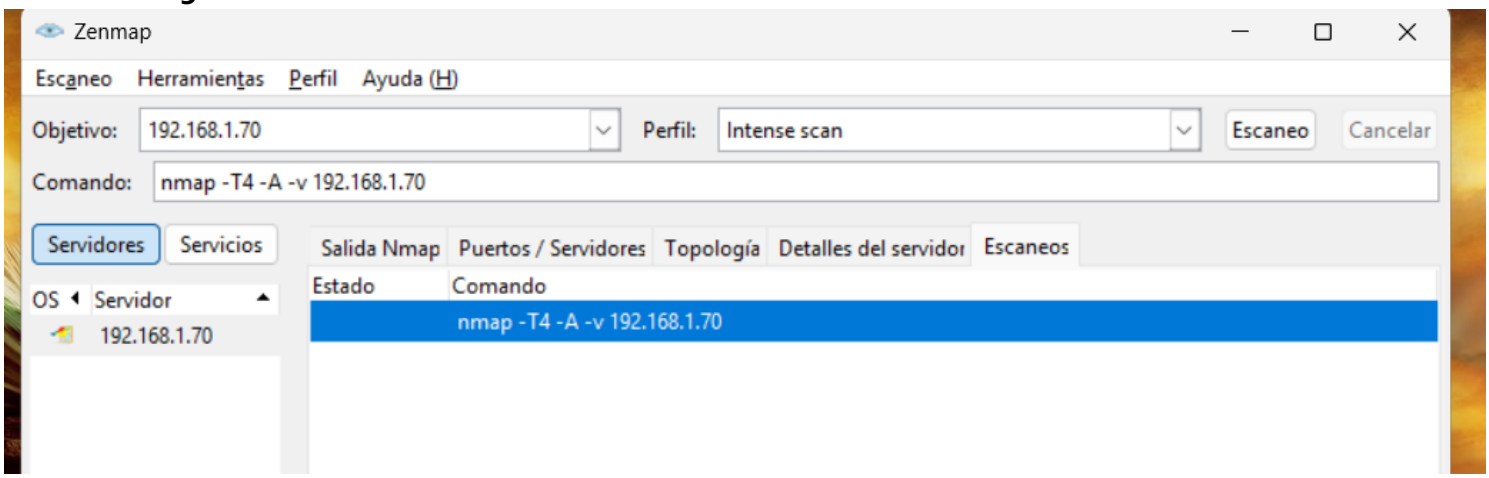
En la pestaña de topología dentro de Zenmap, se muestra una vista en forma de ojo de pez que representa la relación entre mi máquina (localhost) y el objetivo del escaneo, que en este caso es la IP 192.168.1.70, que también es mi computadora. La línea punteada indica que el escaneo se hizo desde el mismo equipo hacia sí mismo. El nodo amarillo indica el objetivo activo y en línea, esta visualización me sirve para confirmar que mi equipo fue correctamente identificado como parte de la red y que el escaneo se completó con éxito.



Después de hacer el escaneo a mi computadora con Zenmap, puedo ver que el estado del servidor es 'up', lo que significa que está encendido y respondiendo. Detectó que tengo 5 puertos abiertos, 0 filtrados y 995 cerrados, de un total de 1000 puertos escaneados. El equipo lleva encendido aproximadamente 271 segundos (unos 4 minutos y medio), y su última inicialización fue el domingo 11 de mayo de 2025 a las 16:57:17. Mi dirección IP local es 192.168.1.70 y aunque no muestra la dirección MAC ni IPv6, eso es normal en algunos casos dependiendo del escaneo. También identificó el sistema operativo como Microsoft Windows 10 versión 1607 con una precisión del 99%, lo cual indica que el análisis fue bastante certero en detectar qué sistema estoy usando.



Y aquí solo nos muestra el historial de los escaneos realizados y su estado, ya bien sea fallido, sin guardar o en este caso guardado.



8. Conclusiones

NOTA: La conclusión deberá estar formada de al menos 6 líneas, de lo contrario el valor de la conclusión será de 0 puntos.

Diana Paola Santiago Pelayo: En esta práctica realizamos la instalación de Nmap en donde primero instale la versión más reciente en Windows 11, más sin embargo al momento de realizar el escaneo de mi red me mandaba error, diciendo que algunas librerías no eran compatibles y que había que levantar un reporte, así que lo que hice fue desinstalar la versión que había instalado e instalar una versión anterior, al momento de ejecutarla y de realizar el escaneo, ahora si lo pudo realizar sin ningún problema, pude comprobar que esta herramienta es muy útil para analizar los puertos y servicios activos en un equipo dentro de la red y me ayudó a entender mejor cómo está configurada mi red local y me dio una idea más clara sobre posibles puntos que podrían requerir atención en términos de seguridad. Además de que comprendí la gravedad de realizar un escaneo no autorizado a un equipo.

Clara Luz Milagro García: Realizar esta práctica me permitió comprender mejor cómo funciona Nmap y su importancia dentro de la seguridad de redes. Al instalar y utilizar la herramienta, pude ver en tiempo real los dispositivos conectados a mi red, los puertos abiertos y los servicios activos, lo cual me ayudó a entender cómo se puede detectar una posible vulnerabilidad. También aprendí que el escaneo debe hacerse con responsabilidad y siempre con autorización, ya que puede ser malinterpretado como un intento de ataque. En general, considero que Nmap es una herramienta esencial para cualquier administrador de red, ya que permite tener control y conocimiento detallado de la infraestructura, facilitando la prevención de riesgos.

Brenda Ciclali Ortiz Fonseca: En esta práctica permitió comprender la importancia de Nmap como herramienta fundamental en seguridad informática para el análisis de redes, detección de vulnerabilidades y gestión de sistemas. A través de la instalación, se confirmó su capacidad para identificar hosts activos, puertos abiertos y servicios en ejecución, lo que ayuda a evaluar posibles riesgos en nuestra red. Yo realicé una prueba, pero no tenía la versión estable y en mi laptop me denegó el acceso, así que no pude realizarlo y la practica se realizará en otra maquina con otra red.

Ricardo Samuel Carranza Marcial: Durante esta práctica pude darme cuenta de lo valiosa que es la herramienta Nmap para el análisis de redes y la detección de posibles vulnerabilidades. Aunque al principio tuve algunos problemas con la instalación, especialmente por cuestiones de compatibilidad con ciertas versiones, logré encontrar una alternativa funcional que me permitió realizar los escaneos correctamente. Al usar Nmap, entendí mejor cómo están configurados los dispositivos dentro de mi red, qué puertos están abiertos y qué servicios están activos, lo cual me dio una visión más clara sobre los puntos que podrían representar un riesgo en términos de seguridad. También aprendí que es fundamental usar este tipo de herramientas con responsabilidad y siempre con autorización, ya que su uso indebido puede ser malinterpretado como una amenaza. En general, esta experiencia me ayudó a comprender mejor cómo mantener una red más segura y el papel que juega Nmap en ese proceso.

9. Referencias Bibliográficas.

Solvetic.com. (2021, diciembre 14). Cómo usar Nmap para escanear puertos [Tutorial 2021] [Video]. YouTube. https://www.youtube.com/watch?v=DHs_udHi7Cg&ab_channel=solvetic.com

Recorded Future. (n.d.). Nmap commands: A guide for threat intelligence professionals. Recorded Future. https://www.recordedfuture.com/threat-intelligence-101/tools-and-techniques/nmap-commands

Nmap - Descargar. (n.d.). Softonic.com. Retrieved May 11, 2025, from https://nmap.softonic.com/