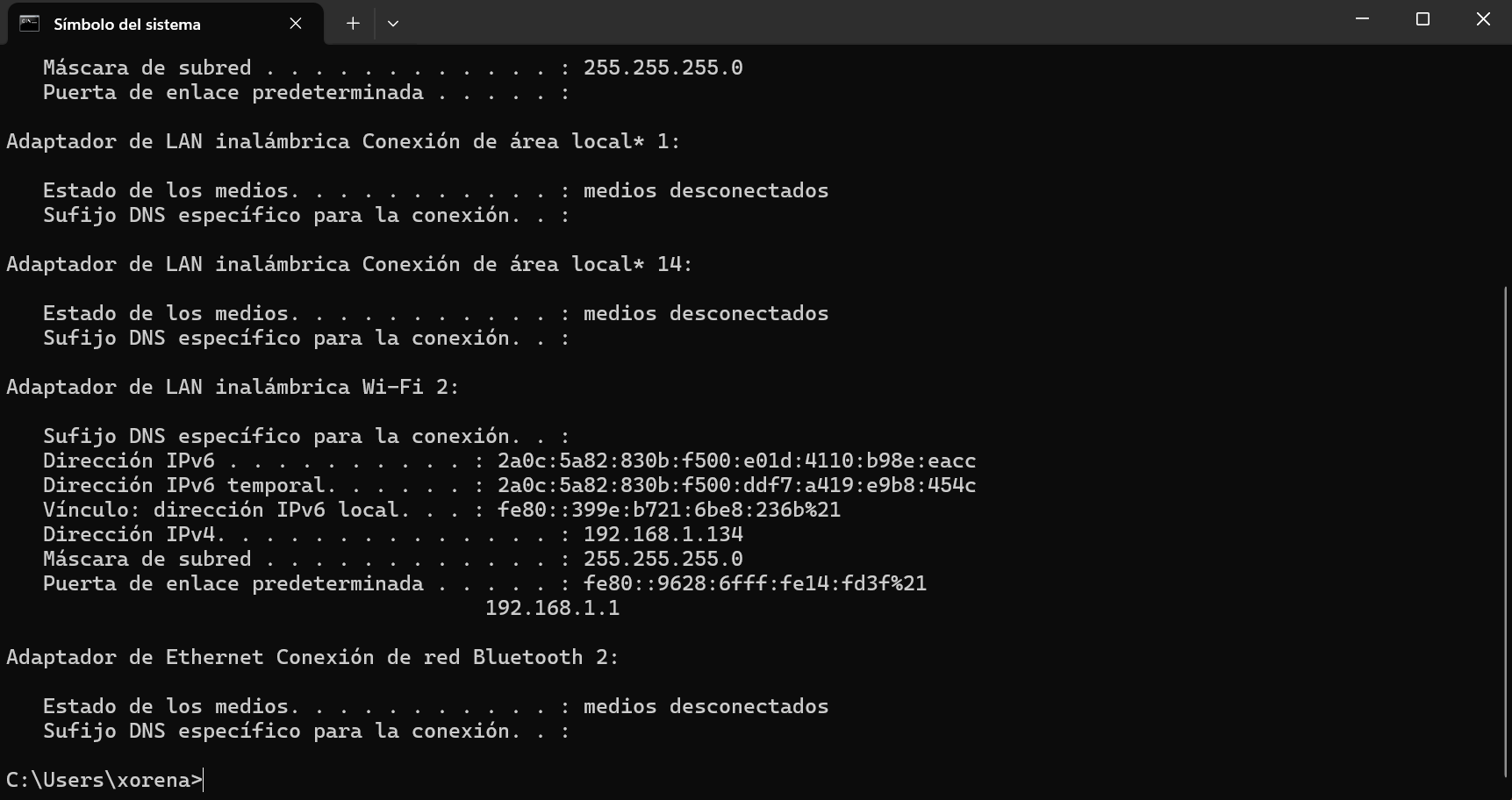
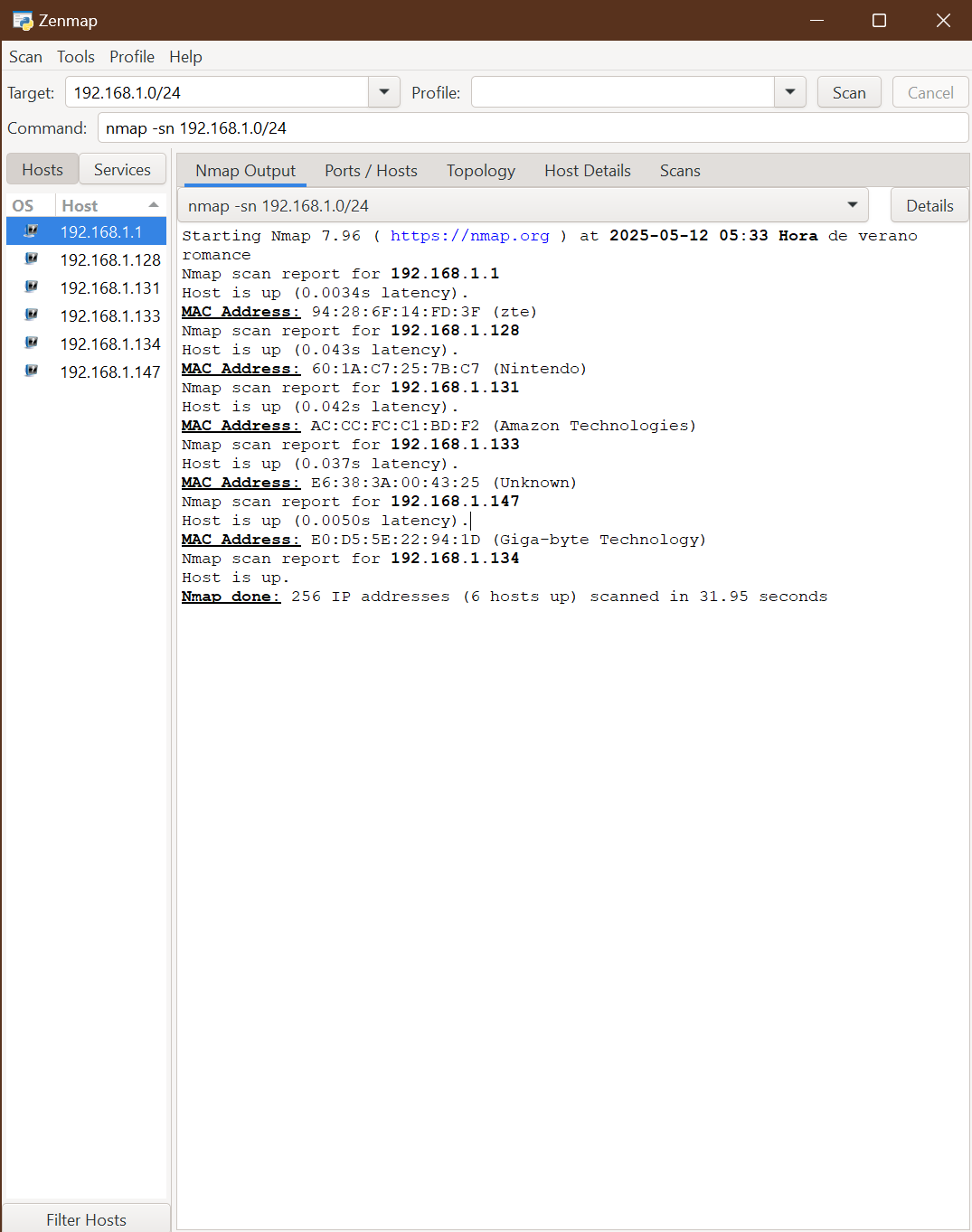
**Escenario 1:**

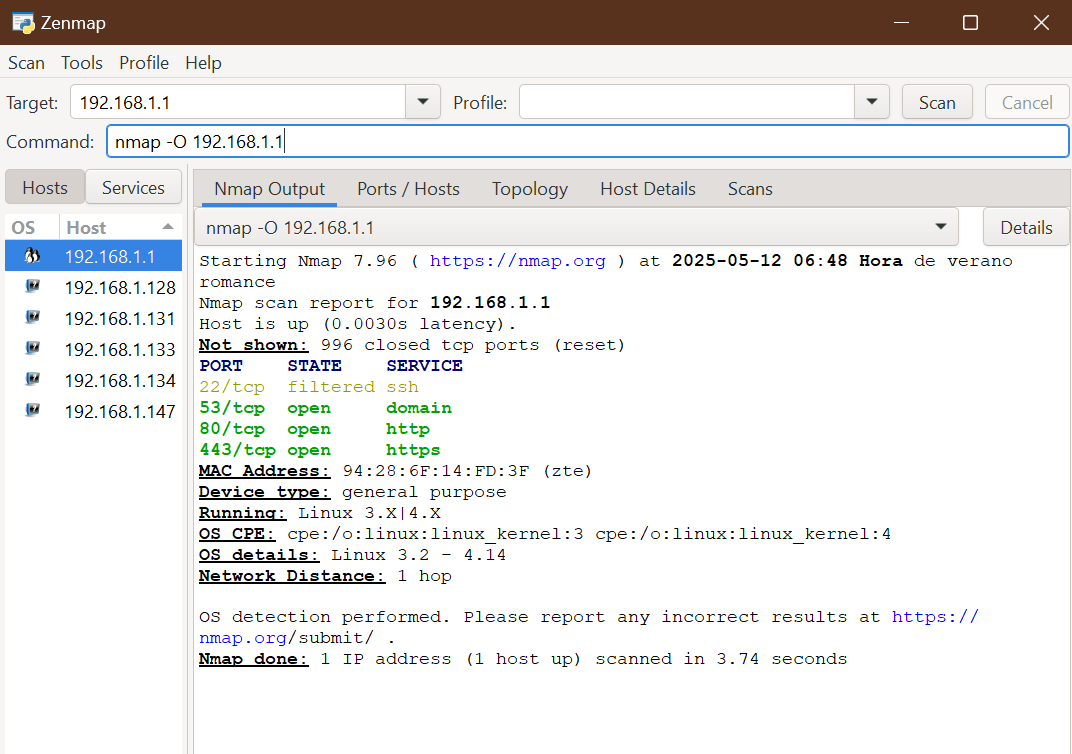
* Se Ejecuta ipconfig (Windows) para ver la IP del equipo y su máscara de red. 
* Nuestra IP es 192.168.1.134  y la máscara es 255.255.255.0, entonces el rango será 192.168.1.0/24.

1. Escanea el rango de IPs con **Nmap**:
2. **nmap -sn 192.168.1.0/24** (Este comando hace un ping scan)
   * Esto genera una lista de IPs activas en la red.
   * Observa las direcciones IP o MAC detectadas y busca una que corresponda al switch. El nombre del fabricante puede aparecer en la salida de **Nmap**, dependiendo de si el switch responde al escaneo.



1. Escaneo más detallado:

**nmap -O 192.168.1.1**



Esto intenta identificar el sistema operativo del dispositivo en una IP específica.

Comprende el propósito de **ARP**:

* ARP (Address Resolution Protocol) es un protocolo de capa 2 que relaciona direcciones IP con direcciones MAC. Permite identificar qué dispositivos están activos en la red y vincular su IP con su dirección MAC.

1. Usa el comando **ARP** para ver los dispositivos conectados:
   * En Windows:
   * **arp –a**



Esto mostrará una tabla con las IPs y las direcciones MAC asociadas de los dispositivos conectados.

1. Busca la dirección MAC que corresponde al switch:
   * Los primeros 6 dígitos de la dirección MAC (OUI) indican el fabricante del dispositivo.



* + Usa una herramienta en línea como [MAC Address Lookup](https://maclookup.app/) para verificar el fabricante y confirmar si corresponde al switch.

1. **¿Qué función tiene el comando nmap -sn 192.168.1.0/24?**

Este comando se usa para **descubrir qué dispositivos están conectados a una red local**.

* nmap: es una herramienta para explorar redes.
* -sn: significa "ping scan", que **no escanea puertos**, solo verifica si los dispositivos están encendidos (activos).
* 192.168.1.0/24: es el rango de direcciones IP que quieres escanear (de la 192.168.1.1 a la 192.168.1.254).

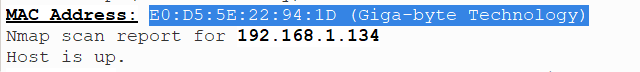
🔍 **¿Qué hace en la práctica?**

Envía una señal (ping o ARP) a cada dirección IP del rango, y te dice:

* Qué IPs están ocupadas por un dispositivo.
* En algunos casos, también te dice el nombre del dispositivo o el fabricante (usando la MAC).

📌 **Ejemplo de salida con nuestra IP 192.168.1.134 con MAC 255.255.255.0**

Host: 192.168.1.1 Status: Up MAC: E0:D5:5E:22:94:1D (Giga-byte Technology)



1. **¿Por qué el switch no aparece como un salto en tracert, pero sí es visible con Nmap o ARP?**

**tracert (en Windows) o traceroute (en Linux/macOS)** muestra los "saltos" que siguen los paquetes para llegar a un destino en otra red.

**¿Por qué no aparece el switch?**

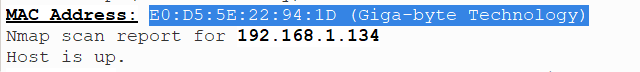
* Porque un **switch trabaja en la capa 2 del modelo OSI** (enlace de datos).
* tracert solo muestra **routers**, que están en la **capa 3** (red), y se encargan de mover datos entre diferentes redes.

**Pero... ¿por qué sí aparece en Nmap o ARP?**

* Nmap puede detectar dispositivos que **responden a solicitudes ARP** en la red local.
* ARP (Address Resolution Protocol) trabaja en la capa 2 y puede ver al switch si este responde o si su MAC es visible.

1. **¿Qué papel juega la dirección MAC en la identificación del switch?**

Te permite saber qué dispositivos están conectados y, mediante el OUI (los primeros 6 dígitos), **identificar el fabricante**. Cada dispositivo de red tiene una dirección MAC única (como una matrícula), por ejemplo, nuestra MAC ES:



Los **primeros 6 dígitos** (llamados **OUI**, Organizationally Unique Identifier) indican que el **fabricante** del dispositivo es GIGA-BYTE TECNOLOGÍA CO.,LTD.

A través del OUI también es posible identificar si una dirección IP pertenece a un switch, revisando si la MAC coincide con un fabricante de switches.

Herramientas como <https://macvendors.com/> te permiten pegar la MAC y ver quién la fábrica.

1. **¿Por qué ARP funciona únicamente para dispositivos en la misma subred?**

**ARP (Address Resolution Protocol)** funciona en la capa de enlace de datos (capa 2) del modelo OSI. Este protocolo es crucial para la comunicación en redes, ya que mapea direcciones IP (capa de red, OSI capa 3) a direcciones MAC (capa de enlace de datos, OSI capa 2).

¿**Por qué solo funciona en la misma subred?**

Porque ARP trabaja a nivel de **enlace de datos** (capa 2), y esta capa solo es relevante dentro de una misma red física o lógica. Veamos los puntos clave:

1. **Las tramas Ethernet (que usan MAC addresses) no se enrutan.**
   * Cuando un equipo quiere enviar datos, necesita la MAC de destino.
   * Si la IP destino está **en la misma subred**, hace un **broadcast ARP**: “¿Quién tiene la IP X.X.X.X?”.
   * Solo los dispositivos **en la misma subred** reciben el broadcast y responden.
2. **Los routers no reenvían broadcasts.**
   * Un paquete ARP es un **broadcast**, y los routers están diseñados para **no reenviar broadcasts** por otras interfaces.
   * Así se aísla el tráfico local del tráfico entre redes.
3. **Para IPs fuera de la subred, el gateway es el destino inmediato.**
   * Si tu PC quiere hablar con, por ejemplo, 8.8.8.8, verifica primero si esa IP está en su subred.
   * Como no lo está, busca la MAC del **router (gateway)** usando ARP.
   * Luego, **envía el paquete al router**, y el router se encarga de entregarlo en la red de destino.

**En resumen:**

* Dentro de la subred: Usamos ARP para encontrar la MAC del destino.
* Fuera de la subred: Usamos ARP para encontrar la MAC del **router** (no del destino final).

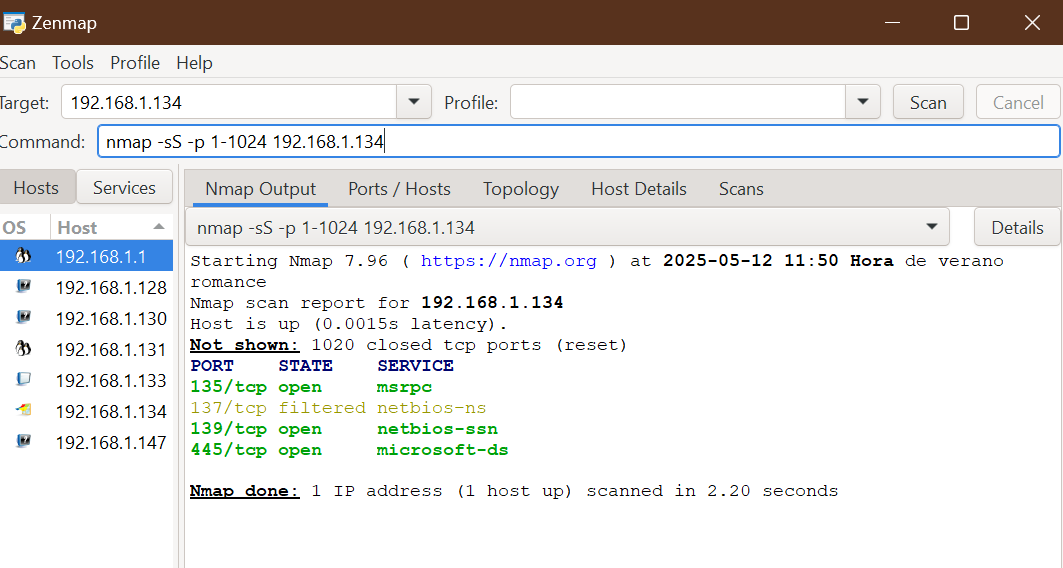
**Escenario 2: Identificación de dispositivos vulnerables mediante escaneo de puertos**

**1. Identificar el rango de IPs**

Con la IP 192.168.1.134 y la máscara 255.255.255.0, el **rango de IPs** de mi red local es:  
 192.168.1.1 a 192.168.1.254 (**192.168.1.0/24)**

**2. Escaneo de puertos con:**

nmap -sS -p 1-1024 192.168.1.134



**¿Qué hace este comando?**

* nmap: herramienta de escaneo de red.
* -sS: escaneo SYN (también llamado "half-open"), más sigiloso.
* -p 1-1024: escanea **los primeros 1024 puertos**, que son los **puertos bien conocidos**.
* 192.168.1.134: es mi IP

➡️ **No se están escaneando todos los puertos**, solo los del 1 al 1024. Para todos sería -p-.

**3. Detección de versiones:**

nmap -sV 192.168.1.134

**¿Qué hace esto?**

* -sV: intenta identificar las **versiones de los servicios** corriendo en los puertos abiertos.
  + Por ejemplo, si tienes el puerto 22 abierto, puede decirte si es "OpenSSH 8.2p1".

Esto te ayuda a saber si un servicio es antiguo o vulnerable.

**1. ¿Qué función tiene el comando nmap -sS -p 1-1024 192.168.1.134? ¿Estamos escaneando todos los puertos de nuestro equipo?**

Veamos detalladamente las partes de este comando nmap -sS -p 1-1024 192.168.1.134

**¿Qué hace cada parte?**

1. **nmap**  
   Es una herramienta de escaneo de red, se usa para descubrir hosts y servicios en una red.
2. **-sS**  
   Especifica el **tipo de escaneo**: un **escaneo SYN** (también llamado "half-open scan" o "escaneo sigiloso").
   * En lugar de completar una conexión TCP (como haría un escaneo normal con -sT), este tipo de escaneo envía solo el primer paquete de la conexión (el paquete SYN).
   * Si el puerto está **abierto**, el host responde con un SYN-ACK.
   * Si está **cerrado**, responderá con un RST (reset).
   * Como no completa la conexión, este método es **más rápido y más difícil de detectar** en los registros del sistema de destino (logs).
3. **-p 1-1024**  
   Le dice a nmap que escanee solo los **puertos del 1 al 1024**.
   * Estos se conocen como **puertos bien conocidos** o **puertos comunes**.
   * Muchos servicios estándar (como HTTP, FTP, SSH, DNS, etc.) usan puertos en este rango.
   * Hay **65,535** puertos TCP posibles, pero aquí estás escaneando solo los más utilizados.
4. **192.168.1.134**  
   Es la **dirección IP del objetivo**. La "X" debe ser reemplazada por un número (por ejemplo, 192.168.1.5) que identifique un dispositivo específico en la red local.

**¿Qué utilidad tiene este comando?**

* Saber **qué servicios están activos** en un host (por ejemplo, si tiene un servidor web en el puerto 80).
* Identificar **potenciales vulnerabilidades** (puertos abiertos que no deberían estarlo).
* Es útil tanto para **administradores de red** como para **auditores de seguridad** o **hackers éticos**.

**Resumen final**

El comando:

nmap -sS -p 1-1024 192.168.1.X

Este comando realiza un escaneo rápido y sigiloso los **puertos del 1 al 1024** de una dirección IP objetivo, para ver qué servicios están escuchando o abiertos.  
📌 **No se están escaneando todos los puertos**, solo los del 1 al 1024. Para escanear todos sería con -p-.

**2. ¿Qué puertos representan un riesgo si están accesibles sin restricciones y por qué?**

| **Puerto** | **Servicio** | **Función / Uso común** | **Riesgo potencial** |
| --- | --- | --- | --- |
| **135** | msrpc (Microsoft RPC) | Usado por Windows para servicios de red como DCOM. | Puede ser explotado para ejecutar código remotamente. |
| **137** | netbios-ns (NetBIOS Name Service) | Para resolución de nombres en redes Windows. | Filtrado (no abierto), pero si se abre, puede usarse para recolectar info del sistema. |
| **139** | netbios-ssn (NetBIOS Session Service) | Compartición de archivos/imágenes en Windows (antiguo). | Muy vulnerable si no está restringido a red local. Ataques tipo "null session". |
| **445** | microsoft-ds (SMB) | Usado para compartir archivos e impresoras. | Muy crítico: fue el vector de entrada del ransomware **WannaCry** y **EternalBlue**. |

➡️ **Riesgo mayor si están accesibles desde Internet o sin autenticación segura.**

**⚠️ ¿Qué tan expuesto estás?**

* Si **estás en una red doméstica protegida por NAT y firewall**, el riesgo es bajo.
* Pero si **expones tu equipo a Internet** o una red pública sin restricciones:
  + **Puerto 445** debe cerrarse o protegerse con firewall.
  + **135 y 139** también deberían estar bloqueados a equipos no confiables.

**🛡️ ¿Qué puedes hacer?**

1. **Desactivar compartición de archivos/impr. si no lo usas** (Panel de control > Red).
2. **Usar firewall de Windows** o uno externo para bloquear estos puertos fuera de tu LAN.
3. **Mantener Windows actualizado** (parches de seguridad).
4. **Desactivar NetBIOS** si no lo necesitas:
   * En las propiedades de la tarjeta de red > TCP/IPv4 > Avanzado > WINS.

**3. ¿Por qué es importante restringir los puertos abiertos en una red?**

* **Reduce la superficie de ataque**: menos servicios disponibles = menos oportunidades para atacantes.
* **Evita escaneos automáticos**: bots escanean puertos buscando servicios vulnerables.
* **Minimiza errores humanos**: algunos servicios se dejan activos sin configurarse bien.
* **Ayuda en el cumplimiento** de políticas de seguridad y normativas (ISO, GDPR, etc.).

**Escenario 3: Detección de dispositivos con ping desactivado**

## **Objetivo del ejercicio**

El objetivo es **detectar todos los dispositivos activos en una red**, incluso aquellos que **no responden al ping (ICMP)**. Algunos equipos lo tienen desactivado por seguridad, por lo tanto, necesitamos usar **métodos alternativos de detección**.

## **PASO A PASO**

### ****Primer comando (en CMD de Windows):**** for /L %i in (1,1,254) do @ping -n 1 192.168.1.%i >nul

### Este comando intenta **hacer ping** a todas las IPs del rango 192.168.1.1 hasta 192.168.1.254.

🔍 **¿Qué hace cada parte?**

* for /L %i in (1,1,254) → Bucle que va del 1 al 254.
* ping -n 1 → Envía **1 solo paquete de ping** a cada IP.
* 192.168.1.%i → Es la IP que cambia en cada iteración.
* @ → Evita mostrar el comando en la consola (limpia la salida).
* >nul → Oculta el resultado del ping (nada se muestra en pantalla).

❗ Limitación: Solo detecta **los dispositivos que responden al ping**. Si el ping está bloqueado, no se ven.

### ****Segundo comando (usando Nmap):**** nmap -sn 192.168.1.0/24

### 

Este comando **escanea toda la red** (de .1 a .254) y muestra qué hosts están activos.

* -sn → "Ping scan", busca qué IPs están vivas **sin escanear puertos**.

### ****Ventaja****: Nmap no depende solo del ping. Usa otras técnicas como:

* **ARP scan** (si es red local)
* **TCP SYN scan** (envía solicitudes a puertos comunes)
* **Reverse DNS**

### ****En Linux (como Kali):**** sudo nmap -sn 192.168.1.0/24

### 

Cuando se usa con sudo, Nmap puede hacer **escaneo ARP**, que es:

* Mucho más confiable en redes locales.
* Detecta dispositivos **incluso si el ICMP está bloqueado**.
* Basado en la forma en que los dispositivos se anuncian en la red local.

## **Comparación de resultados**

Después de correr ambos comandos:

* Si **hay más dispositivos detectados con Nmap que con ping**, es porque algunos **no responden a ICMP** pero sí se pueden detectar por ARP u otros métodos.

**Respuestas a las preguntas**

1. **¿Por qué algunos dispositivos no responden a ping?**

* El **firewall** lo bloquea.
* Está desactivado por **política de seguridad**.
* Dispositivos como cámaras, impresoras, o IoT lo traen **desactivado por defecto**.

1. **¿Cómo ayuda Nmap a descubrirlos de todos modos?**

Nmap **no depende solo del ping (ICMP)**. Usa:

* **ARP** → Identifica dispositivos en la red local sin necesidad de ping.
* **SYN packets** → Comprueba si los dispositivos responden a conexiones.
* **Otras técnicas de escaneo** para descubrir equipos "ocultos".

1. **¿Qué implicaciones de seguridad tiene permitir o bloquear ICMP?**

✅ **Permitir ICMP:**

* Útil para diagnosticar problemas (ping, traceroute).
* Necesario para herramientas de monitoreo.

❌ **Bloquear ICMP:**

* Mejora la seguridad: los atacantes no pueden detectar fácilmente el dispositivo.
* Pero puede dificultar el diagnóstico de red.

Lo ideal es **controlar quién puede hacer ping**, no bloquearlo totalmente.

1. **¿Cuándo ejecutas sudo nmap -sn 192.168.1.0/24 en Kali, aparecen las direcciones IP?**

* **Sí aparecen:** Tienes buena conectividad de red. (NUESTRO CASO)
* **No aparecen:** Tu Kali está **aislado de la red** (por ejemplo, por configuración de la red virtual o adaptador de red).

**¿Parece que el sistema está aislado? ¿Podrías resolverlo?**

Sí, si **no ves ninguna IP activa**, puede que:

* Kali esté en modo "solo anfitrión" o "red NAT mal configurada".
* El adaptador de red esté deshabilitado.

🛠 **Solución:**

1. Ejecuta ip a o ifconfig para ver si Kali tiene una IP.
2. Verifica la configuración del adaptador en VirtualBox/VMware (modo puente o NAT).
3. Intenta hacer ping a tu router (ping 192.168.1.1).

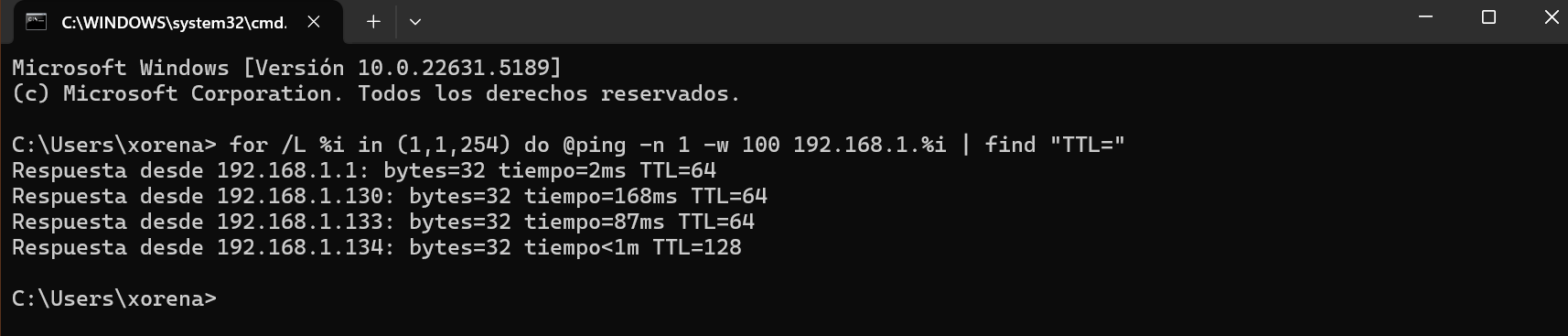
**5. ¿En el comando for /L %i in (1,1,254) do @ping -n 1 192.168.1.%i >nul, qué hace @ y >nul?**

* @ → **Evita mostrar** el comando que se está ejecutando en pantalla.
* >nul → **Descarta la salida** del ping. Es decir, no muestra nada, aunque funcione. Si eliminamos el >nul del comando permitiría la salida de ping a todas las IPs del rango 192.168.1.1 hasta 192.168.1.254 y se vería así:



🔁 Si quieres ver qué IPs responden al ping, usa esta versión:

for /L %i in (1,1,254) do @ping -n 1 192.168.1.%i | find "TTL="



Esto **filtra y muestra solo las IPs que sí respondieron**.

**Escenario 4: Detección de spoofing ARP en la red local**

**¿Qué es ARP Spoofing?**

ARP (Address Resolution Protocol) es un protocolo que permite a los dispositivos de una red local obtener la dirección MAC correspondiente a una dirección IP. El ataque de ARP Spoofing ocurre cuando un atacante envía respuestas ARP falsas para asociar su dirección MAC con la dirección IP de otro dispositivo, como un router o una computadora legítima. Esto permite al atacante interceptar, modificar o redirigir el tráfico de red entre dos dispositivos.

**Pasos para detectar un ataque ARP Spoofing**

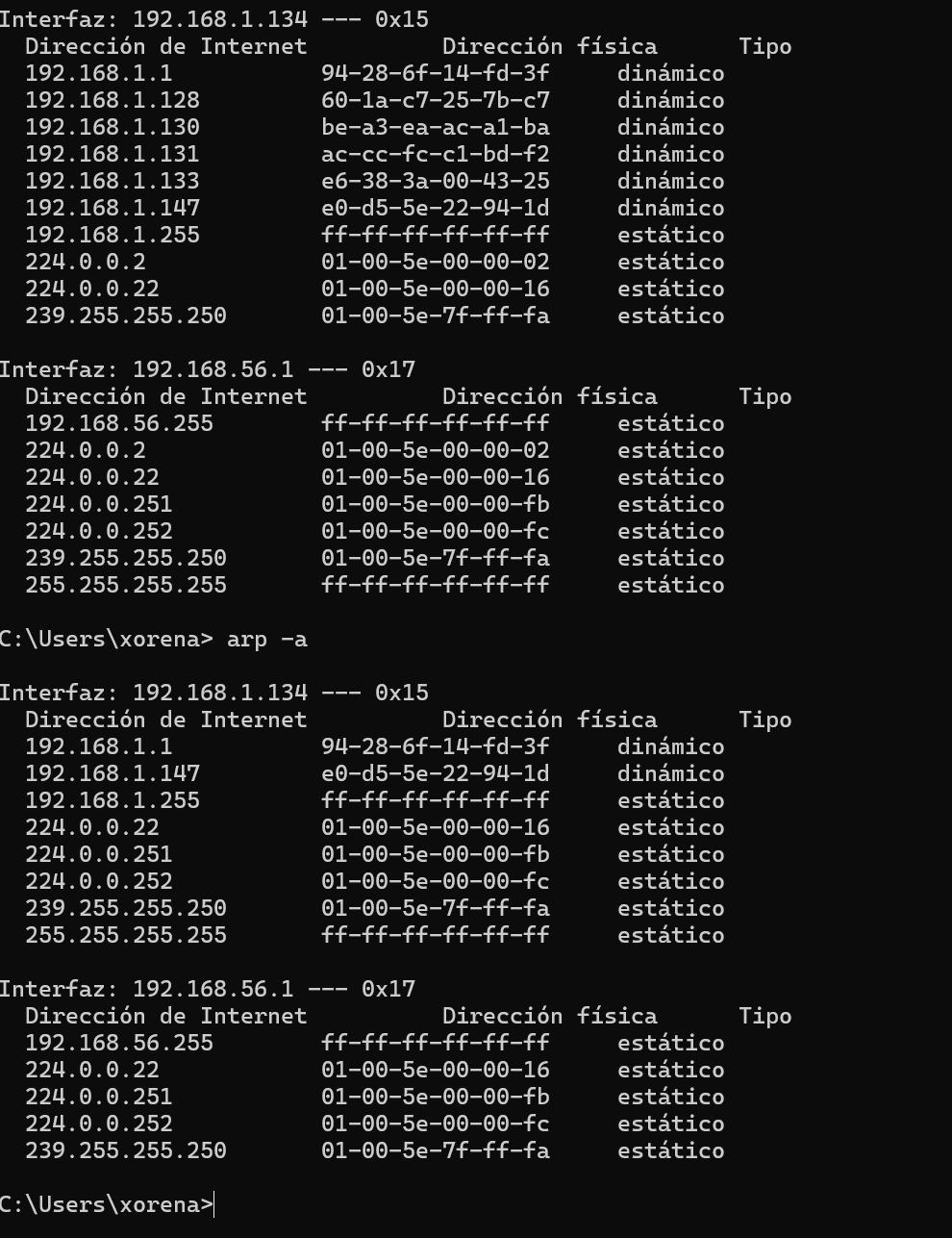
**1. Ejecutar el comando arp**

Debes verificar la tabla ARP en la máquina que estás utilizando. Dependiendo de tu sistema operativo, utiliza:

* **En Windows**  : arp -a
* **En Linux:** arp –n

Esto te mostrará las IPs de la red local y las direcciones MAC asociadas.

**Ejemplo de salida** (puede variar según tu red):



Se realiza esta verificación varias veces, en intervalos de tiempo lo que permitirá observar si hay cambios en las direcciones MAC asociadas a las IPs.

Al tener una lista de las IPs y las MACs de los dispositivos en la red local, se puede verificar si alguna dirección IP está asociada a diferentes direcciones MAC en momentos distintos, como lo vemos en el ejemplo.

**Respuestas a las preguntas**

**¿Qué señales indican un ataque de ARP Spoofing?**

**1. Direcciones IP asociadas a diferentes direcciones MAC**

* Si ves que una **misma IP** está asociada a **distintas direcciones MAC** en diferentes momentos, es una señal de que podría haber un ataque de ARP Spoofing.
* Esto sucede porque el atacante envía respuestas ARP falsas para asociar su dirección MAC con una IP que no le corresponde.

**2. Inestabilidad en la tabla ARP**

* Si las direcciones MAC de dispositivos legítimos están cambiando constantemente o se mezclan con direcciones desconocidas, puede ser un indicio de un ataque.

**3. Comportamiento extraño en la red**

* Si experimentas una **lentitud inesperada** en la red o **perdida de paquetes**, podría ser un efecto secundario del ARP Spoofing, ya que el atacante está interceptando el tráfico.

**¿Cómo mitigar un ataque de ARP Spoofing?**

**1. Usar ARP Static Binding**

* Configura **entradas estáticas ARP** en los dispositivos, lo que significa que cada dispositivo tiene una IP asociada permanentemente a una MAC en su tabla ARP. Esto previene que el dispositivo acepte respuestas ARP falsas.
* **En Linux**, puedes hacer algo como esto:

sudo ip neighbor add 192.168.1.1 lladdr 00:14:22:01:23:45 nud permanent

**2. Habilitar seguridad en switches (Port Security)**

* **Port Security** en switches puede ayudar a mitigar el ARP Spoofing al **limitar las direcciones MAC** que pueden asociarse con un puerto de switch. Si un puerto recibe una dirección MAC desconocida, el switch puede bloquear ese puerto o generar una alerta.

**3. Detectores y herramientas de monitoreo**

* **Herramientas como arpwatch** en Linux o **Wireshark** en todos los sistemas operativos pueden ayudar a identificar cambios en la tabla ARP.
* Estas herramientas pueden generar alertas si detectan respuestas ARP inusuales.

**4. Uso de VPNs**

* Una VPN puede cifrar el tráfico, lo que dificulta que un atacante pueda interceptarlo, incluso si realiza un ARP Spoofing.

**🔄 El papel del switch en la propagación de respuestas ARP falsas**

Los **switches** operan principalmente en la **capa 2** (enlace de datos) del modelo OSI, y su función principal es enviar datos entre dispositivos utilizando direcciones MAC. Aquí está su relación con el ARP Spoofing:

**1. Aprendizaje de direcciones MAC en el switch**

* Los switches **aprenden** las direcciones MAC de los dispositivos que se conectan a sus puertos. Cuando un dispositivo envía un paquete, el switch lo **mapea a su puerto correspondiente**.
* Sin embargo, si un atacante envía respuestas ARP falsas, el switch **asocia la IP legítima de otro dispositivo** con la **dirección MAC del atacante**. Así, el switch comienza a enviar el tráfico destinado a la IP legítima al dispositivo atacante.

**2. Impacto del switch en el ataque**

* Si el **switch no tiene mecanismos de seguridad (como Port Security)**, puede permitir que el atacante propague ARP Spoofing sin restricciones.
* Sin embargo, si el switch tiene características avanzadas, como **port security** o **mac address filtering**, puede ayudar a prevenir la propagación de respuestas ARP falsas.

**Conclusión**

Para detectar y mitigar ataques de ARP Spoofing, necesitas monitorear las tablas ARP de la red local, observar cambios inusuales y aplicar medidas preventivas como ARP estático, seguridad en los switches y herramientas de detección. A medida que avanzamos, herramientas como **Wireshark** y **arpwatch** te ayudarán a detectar este tipo de ataques en tiempo real.

**Escenario 5, Detección y bloqueo de puertos con Nmap y firewall**

**FASE 1: Escaneo con Nmap**

El primer paso es identificar qué puertos están abiertos en tu equipo usando Nmap, que es una herramienta de escaneo de redes muy popular. Vamos a ver cómo hacerlo.

**Paso 1: Identificar tu IP local**

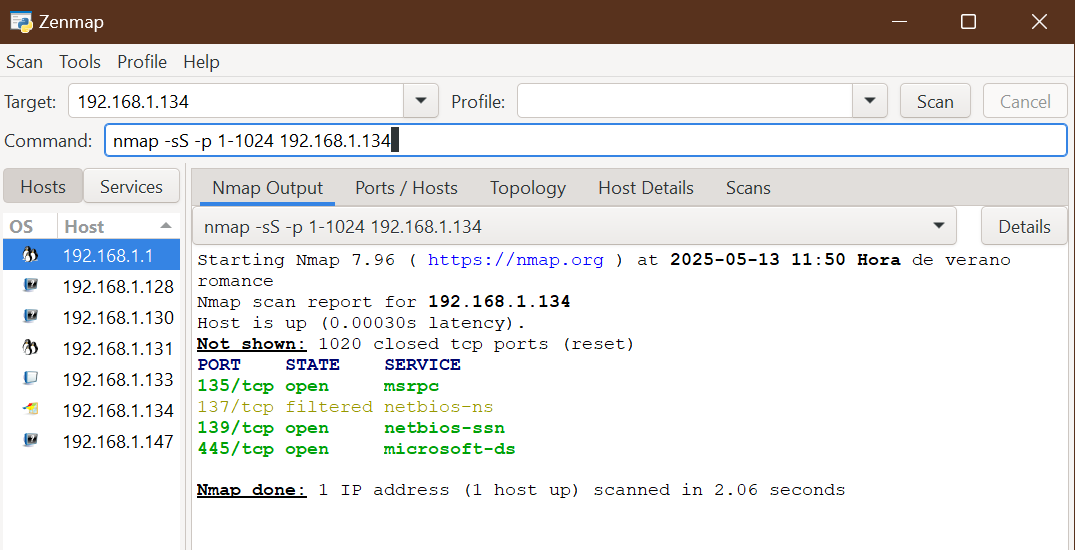
* En Windows: Abre el símbolo del sistema y escribe ipconfig. Busca la sección que diga "Dirección IPv4" para encontrar tu IP local, en nuestro caso: 192.168.1.134.

**Paso 2: Escanear tu propio equipo**

Para hacer un escaneo con Nmap, se usa el siguiente comando: nmap -sS -p 1-1024 192.168.1.134.

* -sS: Esto realiza un escaneo de tipo SYN, que es rápido y eficiente.
* -p 1-1024: Especifica que Nmap debe escanear los puertos del 1 al 1024 (puertos comunes de servicios).
* 192.168.1.134: Es la IP del equipo .

Este comando te mostrará qué puertos están abiertos en tu equipo y qué servicios están asociados a esos puertos (por ejemplo, el puerto 80 es común para HTTP, el 22 para SSH[[1]](#footnote-1)).



Puertos abiertos en mi equipo 135 RPC Microsoft DCOM, 137-139 NetBIOS, 445 Microsoft-DS (SMB)

**En Windows (con PowerShell)**

1. **Abrir PowerShell como Administrador** (clic derecho en el icono de PowerShell y "Ejecutar como administrador").
2. **Bloquear el puerto 139 (NetBIOS):**

New-NetFirewallRule -DisplayName "Bloqueo puerto 139" -Direction Inbound -Protocol TCP -LocalPort 139 -Action Block

* + DisplayName: El nombre de la regla (puedes cambiarlo a algo más descriptivo si lo prefieres).
  + Direction: Especifica si la regla aplica a conexiones de entrada (Inbound) o salida (Outbound).
  + Protocol: El tipo de protocolo (en este caso, TCP).
  + LocalPort: El puerto que deseas bloquear (en este caso, el 139).
  + Action: La acción que se tomará (en este caso, bloquear)

1. **Verificar las reglas existentes:**

powershell: Get-NetFirewallRule

1. **Eliminar la regla (si decides revertir el cambio):**

powershell: Remove-NetFirewallRule -DisplayName "Bloqueo puerto 139"

**Con netsh (otra forma en Windows)**

1. **Abrir el símbolo del sistema como Administrador**.
2. **Bloquear el puerto 139 con netsh:**

netsh advfirewall firewall add rule name="Bloqueo puerto 139" protocol=TCP dir=in localport=139 action=block

1. **Verificar que la regla ha sido aplicada:**

netsh advfirewall firewall show rule name="Bloqueo puerto 139"

1. **Eliminar la regla:**

netsh advfirewall firewall delete rule name="Bloqueo puerto 139"

**Desde el Firewall de Windows Defender (GUI)**

1. Ve a **Panel de control > Sistema y seguridad > Firewall de Windows Defender > Configuración avanzada**.
2. En **Reglas de entrada**, haz clic en **Nueva regla**.
3. Elige **Puerto** y luego selecciona **TCP** o **UDP**, dependiendo del puerto que estás bloqueando (por ejemplo, TCP para el puerto 139).
4. Especifica el puerto (139) y selecciona **Bloquear la conexión**.
5. Aplica la regla a todos los perfiles (dominio, privado, público).
6. Nombra la regla como "Bloqueo puerto 139" y haz clic en **Finalizar**.

### ****FASE 3: Verificación****

Una vez que hayas bloqueado el puerto, es hora de verificar si efectivamente está cerrado.

Ejecuta nuevamente el escaneo con Nmap:

nmap -sS -p 139 192.168.1.134

* Si el puerto está correctamente bloqueado, deberías ver algo como esto:

80/tcp filtered

* O también puede ser:

80/tcp closed

Esto indica que el puerto está cerrado o filtrado, lo que significa que el firewall está bloqueando las conexiones.

**Respuestas a las preguntas**

1. **¿Qué riesgos implica dejar puertos abiertos innecesarios?**  
   Dejar puertos abiertos innecesarios aumenta la superficie de ataque de tu sistema. Los atacantes pueden aprovechar vulnerabilidades en los servicios que están escuchando en esos puertos, permitiendo la explotación de estos servicios o el acceso no autorizado.
2. **¿Qué diferencia hay entre "puerto cerrado" y "puerto filtrado" en Nmap?**
   * **Puerto cerrado**: El puerto está cerrado, pero hay una respuesta del sistema indicando que no hay servicio en ese puerto.
   * **Puerto filtrado**: El puerto está bloqueado por un firewall u otro dispositivo de red que está interceptando la comunicación, por lo que no hay respuesta.
3. **¿Qué ventajas tiene un firewall sobre simplemente desactivar un servicio?**  
   Un firewall permite controlar el acceso a los puertos y servicios sin tener que desactivar completamente los servicios. Esto es útil porque puedes mantener un servicio activo para ciertos usuarios o en ciertos casos, pero bloquearlo para otros.
4. **¿Hay diferencias en Windows para cerrar los puertos desde NetFirewallRule, netsh, o desde el propio GUI de Windows?**  
   No hay diferencias funcionales importantes entre estos métodos. Todos realizan lo mismo: crear una regla de firewall. La diferencia radica en la forma en que interactúas con ellos (línea de comandos vs interfaz gráfica) y en que PowerShell y netsh permiten automatización (scripts), mientras que la GUI no.
5. **¿Hay alguna forma de verificar que los puertos están cerrados? ¿Y verificarlo desde otros equipos de la misma red?**  
   Puedes verificarlo usando Nmap desde otro equipo de la misma red, ejecutando el mismo escaneo en la IP del dispositivo que tiene el puerto bloqueado. Esto te permitirá comprobar si el puerto está accesible desde otro dispositivo.

1. | **Puerto** | **Servicio/Protocolo** | **Riesgo de seguridad** | **Recomendación** |
   | --- | --- | --- | --- |
   | **20, 21** | FTP (File Transfer Protocol) | FTP transmite datos sin cifrado, lo que permite el robo de credenciales y datos. | Usar SFTP (puerto 22) o FTP sobre TLS (FTPS). |
   | **23** | Telnet | Transmite datos sin cifrado (como contraseñas). | Deshabilitar Telnet, usar SSH (puerto 22). |
   | **25** | SMTP (Simple Mail Transfer Protocol) | Puede ser utilizado para enviar correos spam, o ataques de "mail relay". | Usar SMTPS (puerto 465) o iniciar autenticación. |
   | **80** | HTTP | Sin cifrado, puede ser atacado con vulnerabilidades conocidas. | Usar HTTPS (puerto 443). |
   | **443** | HTTPS | Asegúrate de tener un certificado SSL/TLS adecuado. | - |
   | **110** | POP3 | Transmite contraseñas y datos sin cifrado. | Usar POP3S (puerto 995) |
   | **143** | IMAP | Similar a POP3, sin cifrado. | Usar IMAPS (puerto 993) |
   | **445** | Microsoft-DS (SMB) | Vulnerable a ataques como **EternalBlue** y otros exploits de SMB. | Deshabilitar SMBv1, usar firewall y VPN. |
   | **137-139** | NetBIOS | Puede permitir acceso a información compartida en una red local. | Bloquear estos puertos si no usas NetBIOS. |
   | **55 3389** | RDP (Remote Desktop Protocol) | Puede ser explotado por atacantes si se deja abierto a Internet. | Usar VPN para acceder a RDP o deshabilitarlo si no es necesario. |
   | **1080** | SOCKS Proxy | Puede ser utilizado para evadir la detección de tráfico. | Cerrar si no es necesario. |
   | **3127** | MS Exchange RPC | Es un puerto asociado con Microsoft Exchange, vulnerable a exploits. | Cerrar si no se utiliza el servicio. |
   | **6660-6669** | IRC (Internet Relay Chat) | Utilizado para bots y otras actividades maliciosas. | Bloquear si no se usa IRC. |

   [↑](#footnote-ref-1)