Trabajo Práctico – Seguridad en Sistemas Operativos

Alumnos:

Daiana Judith Velasquez Torrez

velasquezdaiana08@gmail.com

Gabriel Torres

gabicjs87@gmail.com

Materia:
Arquitectura y Sistemas Operativos

Profesor:
Osvaldo Falabella

Tutor: Adriel Ezequías Herrera

Fecha de Entrega: 22 de junio de 2025

Índice

1.Introducción

La seguridad en los sistemas operativos es un aspecto fundamental para proteger la información, garantizar el buen funcionamiento de los servicios y prevenir accesos no autorizados. Uno de los puntos clave en la protección de un sistema es el control de los **puertos de red**, ya que estos representan canales por los cuales los servicios del sistema se comunican con otros dispositivos.

Este trabajo se enfoca en la **gestión de la seguridad de puertos en sistemas operativos Windows**, y cómo esta se relaciona con otros mecanismos como los permisos de usuarios, el control de privilegios y la auditoría de eventos. Se eligió este tema porque los puertos abiertos sin control pueden permitir ataques remotos, como escaneos de estos, intrusiones o acceso a servicios críticos. A su vez, protegerlos requiere aplicar correctamente los conceptos de control de acceso, monitoreo y gestión de usuarios.

Este conocimiento es esencial en la formación técnica, ya que permite entender tanto el funcionamiento las aplicaciones como el entorno en que operan.

El objetivo del trabajo es analizar cómo se gestionan los puertos en Windows, qué riesgos implican, cómo se relacionan con permisos y usuarios, y cómo auditar y proteger los servicios que los utilizan. Para esto, se desarrollará un caso práctico basado en el escaneo de red en un entorno simulado.

2. Marco teórico

Los sistemas operativos modernos como Windows incorporan múltiples mecanismos de seguridad que permiten controlar quién accede a los servicios del sistema, cómo se ejecutan y cómo se comunican por red. Los **puertos** son una parte central de esta arquitectura, ya que permiten que los servicios escuchen y respondan a conexiones externas. A continuación, se explican los conceptos clave para la seguridad de puertos en Windows.

Puertos de red y su clasificación

Un puerto de red es un identificador lógico que permite a un dispositivo diferenciar entre diferentes servicios que se comunican por la red. Por ejemplo, un mismo equipo puede servir contenido web por el puerto 80 y recibir conexiones remotas por el 22.

Los puertos se dividen en tres grupos:

- **Bien conocidos (0–1023):** reservados para servicios estándar (HTTP (80), HTTPS (443), FTP (21), SSH (22), etc.).

- **Registrados (1024-49151):** usados por aplicaciones específicas que requieren registro.

- **Dinámicos o privados (49152-65535): s**e asignan temporalmente y no requieren registro. Se usan comúnmente en conexiones de cliente.

Servicios, usuarios y grupos

Cada servicio que utiliza un puerto opera bajo una cuenta de usuario del sistema, como LocalService o NetworkService. La seguridad de ese puerto depende directamente de los permisos asociados al usuario.

Windows organiza permisos mediante grupos. Por ejemplo, el grupo "Remote Desktop Users" determina quiénes pueden conectarse vía escritorio remoto.

Control de acceso y privilegios

Las **Listas de Control de Acceso (ACLs)** permiten definir qué usuarios o grupos pueden ejecutar servicios o modificar configuraciones relacionadas con puertos. Además, el firewall de Windows permite establecer estas reglas.

El **Control de Cuentas de Usuario (UAC)** regula las acciones críticas, como:

- Abrir puertos restringidos (<1024).
- Modificar reglas del firewall.
- Instalar servicios que utilizan la red.

- **Escaneo de puertos**

  El escaneo de puertos es una técnica utilizada para detectar qué puertos están abiertos en un sistema y qué servicios se encuentran disponibles. Esta práctica puede tener fines legítimos (como tareas de administración y monitoreo) o maliciosos (como la preparación de un ataque).
  Una de las herramientas más comunes para este fin es **Nmap**, que permite identificar:
  - Puertos abiertos.
  - Servicios activos.
  - Sistemas operativos aproximados.
  - Versiones de software expuesto.

- **Firewall y gestión de puertos**

  Los **firewalls** son herramientas clave para proteger el sistema.
  Permiten:

  ✓ **Bloquear puertos innecesarios.**
  ✓ **Limitar accesos según direcciones IP, protocolos o servicios.**
  ✓ **Registrar intentos de conexión.**

  En Windows, se utiliza Firewal de Windows Defender, accesible desde una interfaz gráfica o mediante comandos (netsh o PowerShell). Permite crear reglas de entrada y salida para programas, puertos y protocolos.

- **Auditoría de puertos y servicios**

  La **auditoría** es el proceso de registrar y revisar las actividades en el sistema para detectar comportamientos inusuales o no autorizados. En el caso de los puertos, puede incluir:

  - Registro de accesos a servicios.
  - Monitoreo de intentos fallidos de conexión.
  - Detección de apertura de puertos no autorizados.
  - Herramientas como auditd o los registros del firewall (ufw, iptables) pueden ser utilizadas para este fin.
  - **Nmap en Seguridad Informática**

Nmap (Network Mapper) es una herramienta de código abierto diseñada para explorar redes y realizar auditorías de seguridad. Su objetivo principal es descubrir hosts activos en una red, identificar puertos abiertos, detectar servicios en ejecución y determinar el sistema operativo de los dispositivos analizados.

Funcionalidades principales:

- **Detección de hosts**: Identifica qué dispositivos están activos en una red.
- **Exploración de puertos**: Determina qué puertos están abiertos y a la escucha.
- **Identificación de servicios y versiones**: Detecta servicios (por ejemplo, HTTP, SSH) y sus versiones.
- **Detección de sistema operativo (OS Detection)**: Estima qué sistema operativo usa un host.
- **Detección de vulnerabilidades (con scripts NSE)**: Mediante Nmap Scripting Engine, se pueden ejecutar scripts para detectar vulnerabilidades conocidas.

Importancia en seguridad:

Nmap es utilizado tanto por profesionales de ciberseguridad como por atacantes. Por eso, es vital conocerlo y saber cómo proteger la red contra escaneos y accesos no autorizados. Se usa en:

- Auditorías de seguridad
- Pruebas de penetración (pentesting)
- Reconocimiento en fases tempranas de ataques
- Monitoreo de infraestructura de red

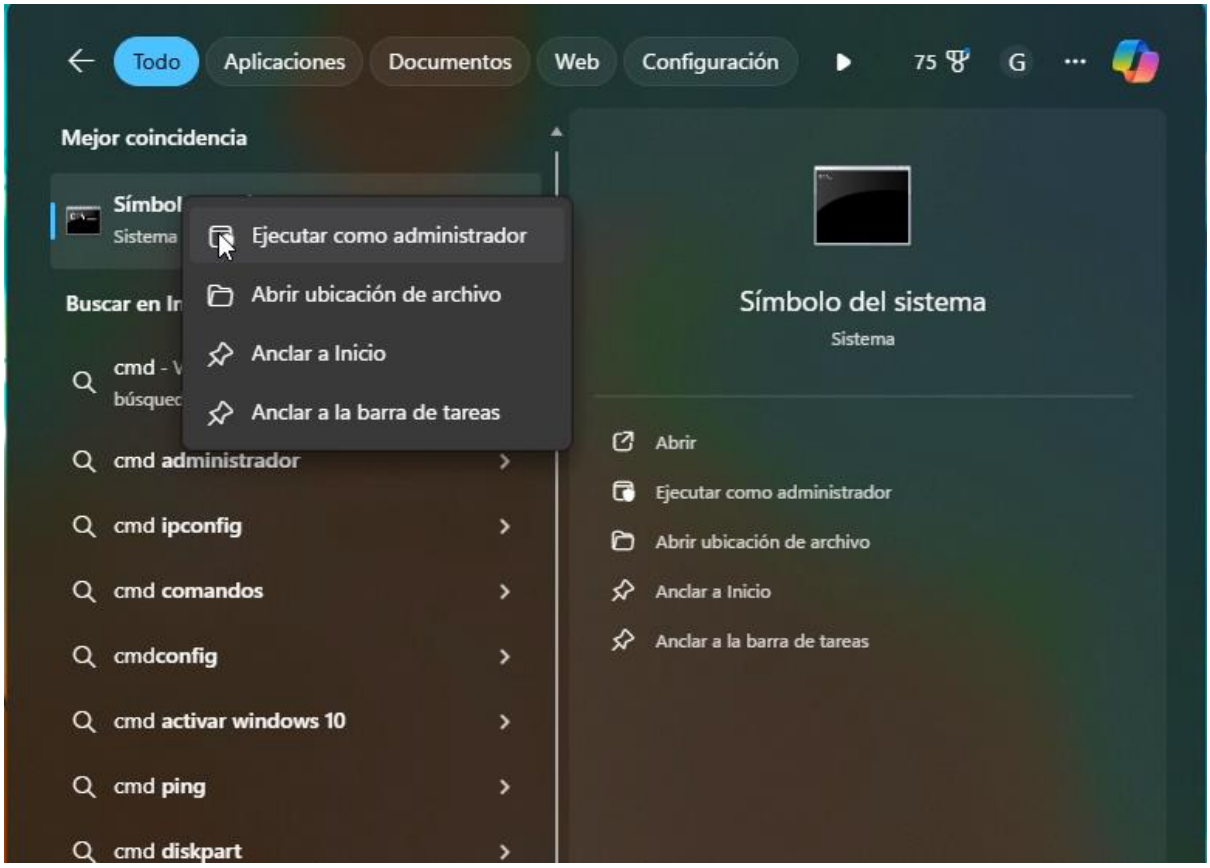
Consideraciones éticas y legales:

El uso de Nmap debe hacerse siempre dentro de un marco legal y con autorización. Escanear redes sin permiso puede considerarse una intrusión o un delito informático, por eso en el caso práctico vamos a mostrar solamente el comando a utilizar, pero no haremos un uso real de este.

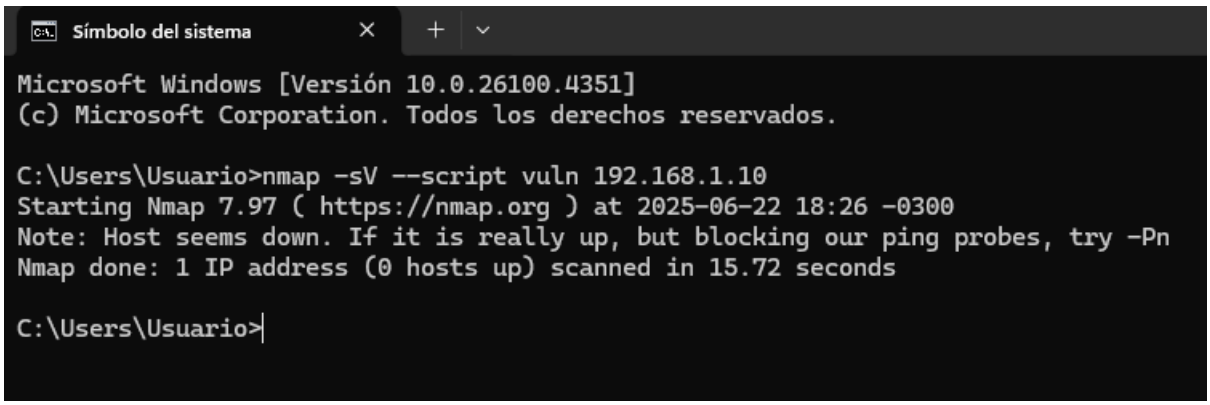
- **Buenas prácticas de seguridad en puertos**
  - ✓ Mantener **solo los puertos necesarios abiertos**.
  - ✓ Usar **firewalls** con reglas restrictivas.
  - ✓ **Actualizar los servicios** que escuchan en puertos abiertos.
  - ✓ Implementar **autenticación y cifrado** (ej: SSH con clave, HTTPS).
  - ✓ Ejecutar servicios con usuarios de bajo privilegio.
  - ✓ Auditar accesos y mantener el sistema actualizado.

3. Caso práctico

En este caso, Gabriel se encuentra trabajando en una empresa de activos financieros, donde le piden realizar una auditoría de seguridad, por lo cual procede a utilizar Nmap para “detectar” y luego bloquear los puertos abiertos, en este caso práctico, el puerto número 3389.

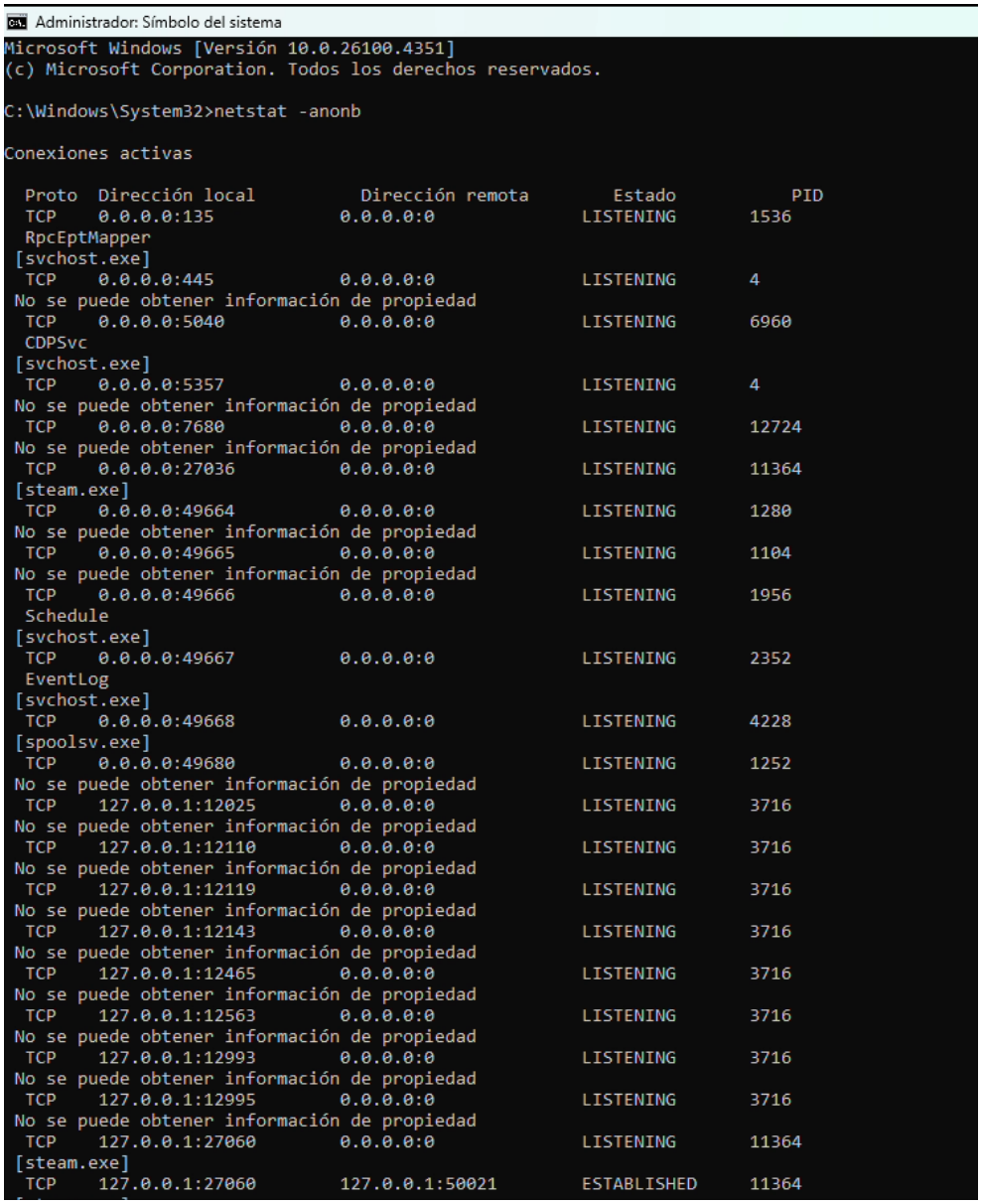


Además aplicamos un parche de seguridad en Windows. Primero a modo de muestra, les mostraremos la ejecución de nmap, hacia una ip (una ip no valida, pero ilustrativa) de modo ejemplo, ya que no sería ético usarlo en una ip real. El uso de esta imagen es pura y exclusivamente ilustrativo, para mostrar el comando utilizado a la hora de realizar este escaneo. Estos escaneos siempre deben realizarse de manera ética, sin fines maliciosos.

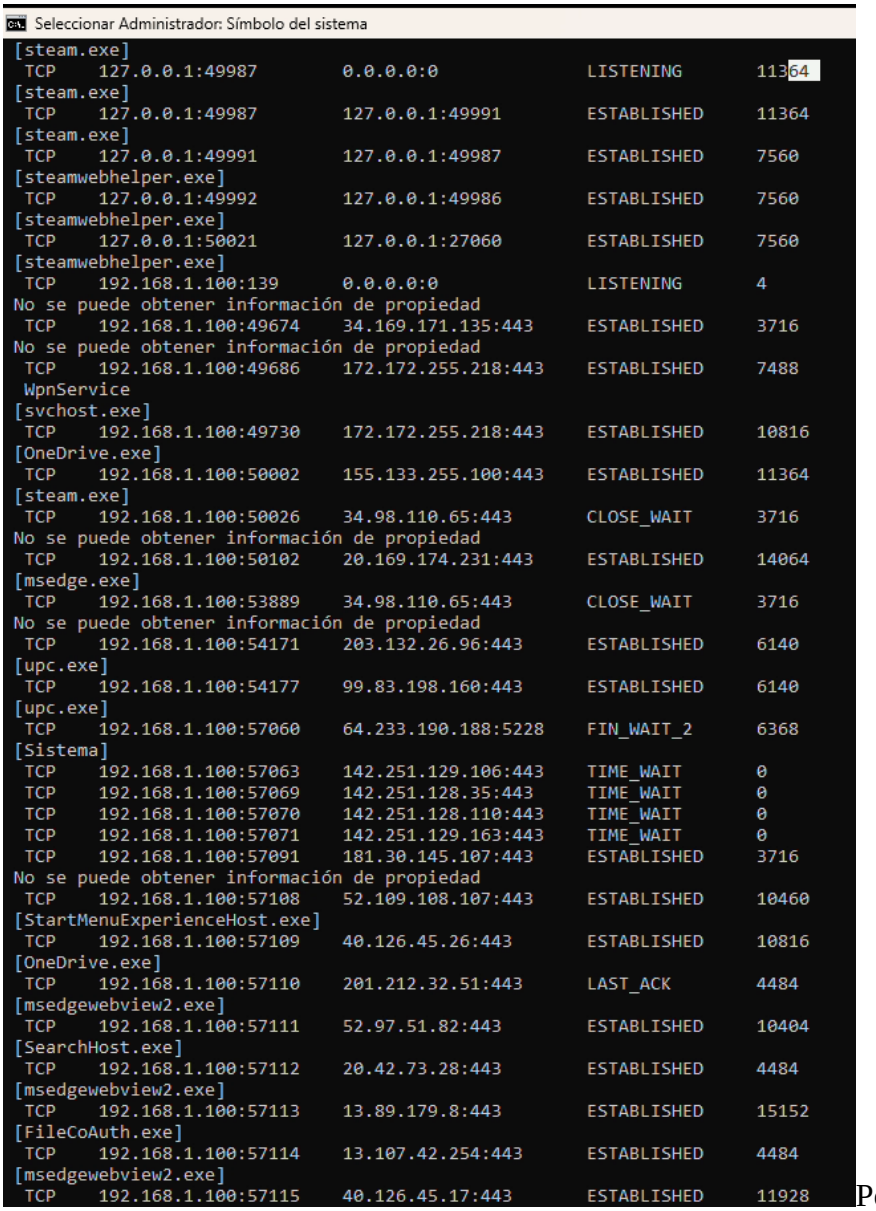


Luego ejecutamos la consola de comandos, el “cmd” o el llamado “símbolo del sistema” como administrador para poder ejecutar el siguiente comando, y ver los puertos y sus

respectivos estados, a modo ilustrativo.



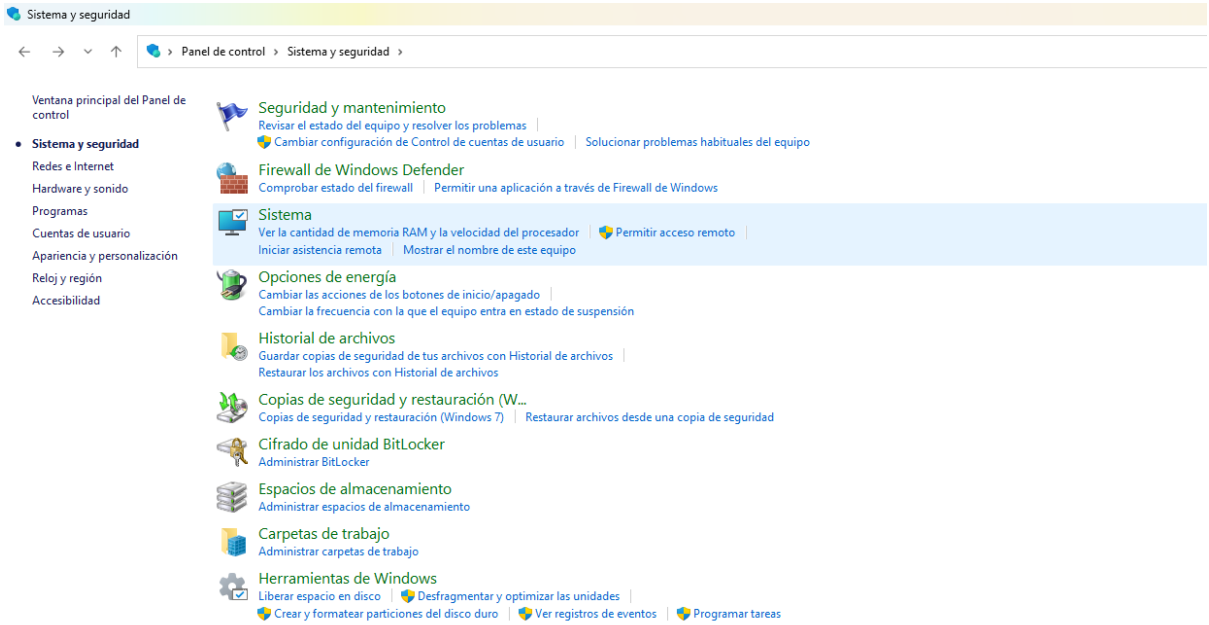
- En esta imagen podemos ver como al ejecutar el comando ”netstat -anob” la consola nos muestra todas las conexiones activas, las direcciones remotas, el estado de estas, y el número de identificación del puerto al cual pertenece esa conexión. Adjuntamos dos capturas de pantalla de los puertos a modo ilustrativo.



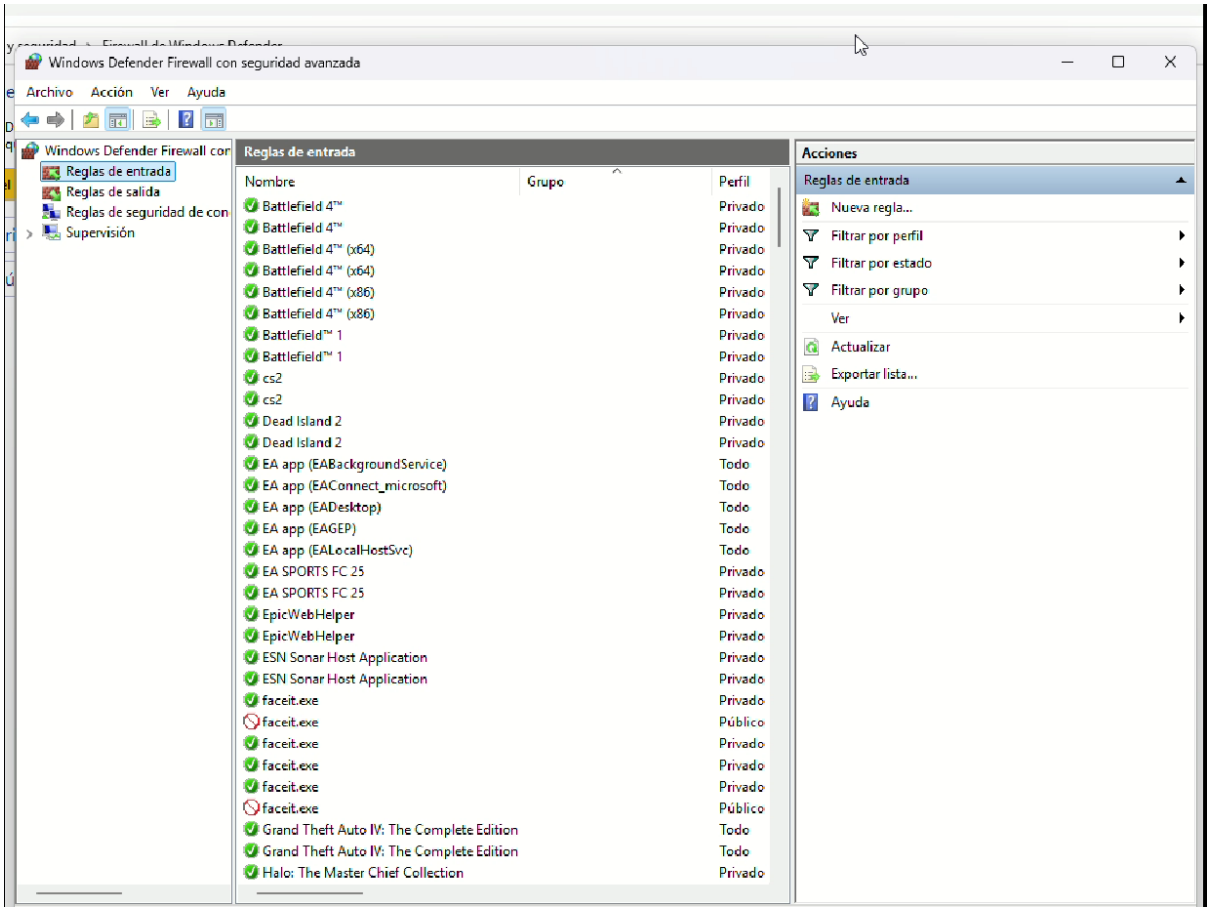
Podemos observar que hay muchísimos puertos, en varios de ellos la conexión esa establecida o “ESTABLISHED “, lo que **significa que hay una conexión activa entre dos equipos,** en este caso mi pc y un servidor. También puede aparecer” LISTENING “, lo cual **significa que un programa está esperando conexiones entrantes.**

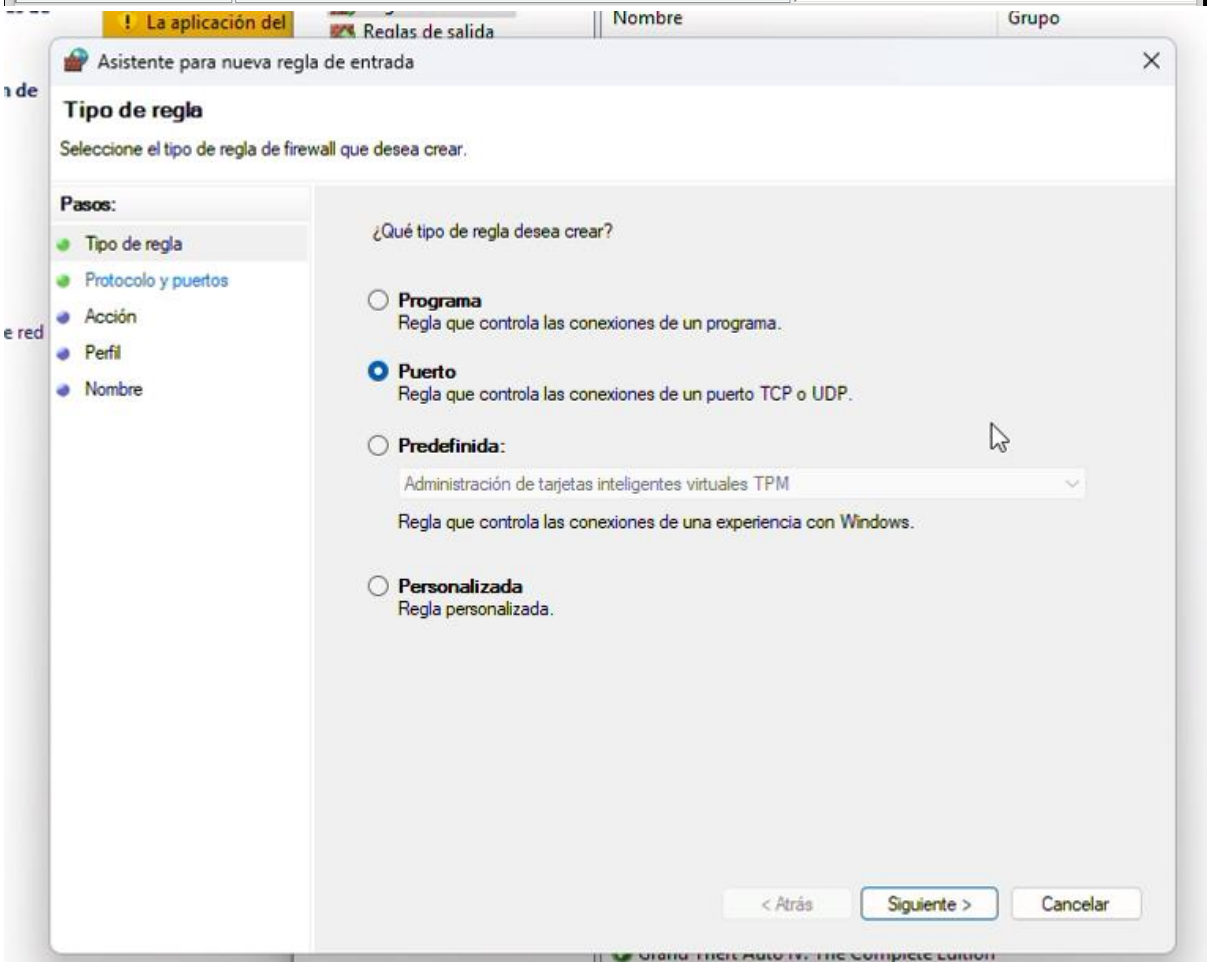
En este caso pudimos ver que el puerto 3389, que es el puerto predeterminado que se utiliza para las conexiones de Escritorio Remoto (RDP) en sistemas Windows, se encontraba esperando conexiones (Listening). Este puerto **permite a los usuarios acceder y controlar remotamente un ordenador desde otra ubicación** a través de una red, por lo cual podría ser muy peligroso si se expone este puerto a la red. Para parchar el problema, nos dirigimos al panel de control, accedemos a ”Sistema y Seguridad” y luego a ”Firewall de Windows Defender”. Por último, accedemos a la configuración avanzada y comenzamos con la configuración del parche. Primero vamos a crear una nueva regla, en la cual vamos a configurar el acceso al puerto

3389.

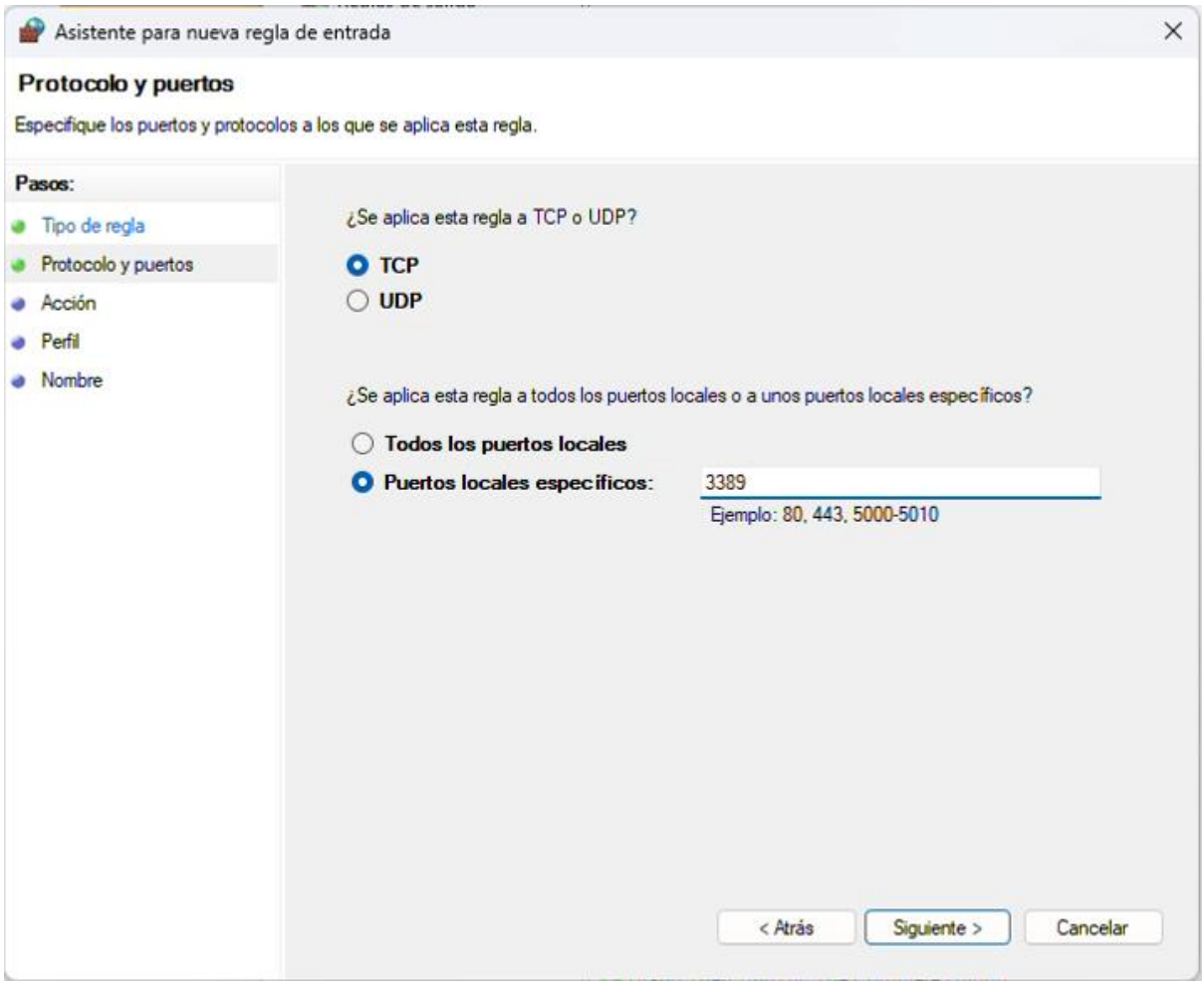


Primero vamos a seleccionar el tipo de regla que queremos crear, en este caso un puerto.

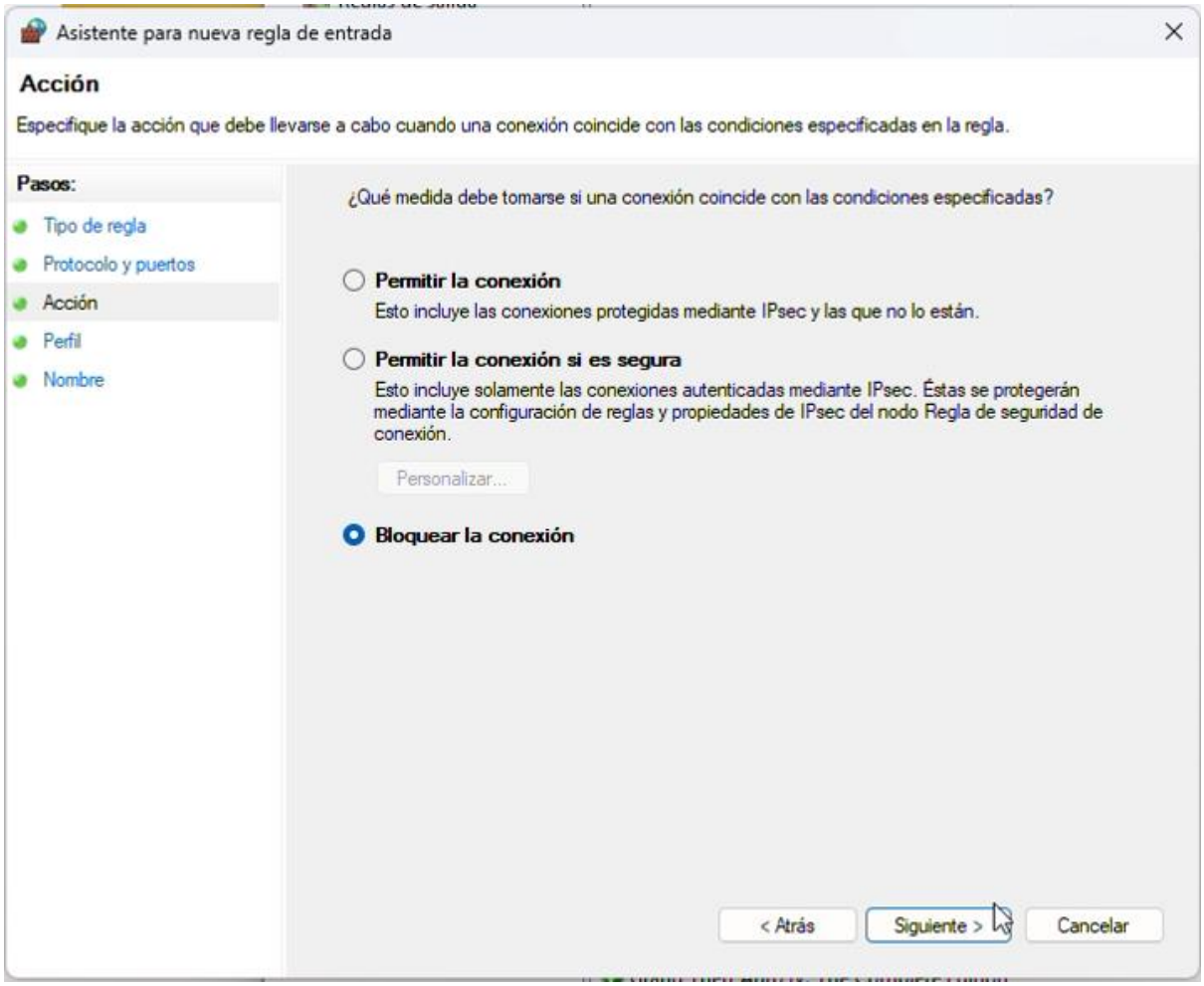

Windows Defender Firewall con seguridad avanzada
Archivo Acción Ver Ayuda
Windows Defender Firewall cor
Reglas de entrada
Reglas de salida
Reglas de seguridad de con
Supervisión
Reglas de entrada
Nombre Grupo Perfil
Battlefield 4™ Privado
Battlefield 4™ Privado
Battlefield 4™ (x64) Privado
Battlefield 4™ (x64) Privado
Battlefield 4™ (x86) Privado
Battlefield 4™ (x86) Privado
Battlefield™ 1 Privado
Battlefield™ 1 Privado
cs2 Privado
cs2 Privado
Dead Island 2 Privado
Dead Island 2 Privado
EA app (EABackgroundService) Todo
EA app (EAConnect_microsoft) Todo
EA app (EADesktop) Todo
EA app (EAGEP) Todo
EA app (EALocalHostSvc) Todo
EA SPORTS FC 25 Privado
EA SPORTS FC 25 Privado
EpicWebHelper Privado
EpicWebHelper Privado
ESN Sonar Host Application Privado
ESN Sonar Host Application Privado
faceit.exe Privado
faceit.exe Público
faceit.exe Privado
faceit.exe Privado
faceit.exe Privado
faceit.exe Público
Grand Theft Auto IV: The Complete Edition Todo
Grand Theft Auto IV: The Complete Edition Todo
Halo: The Master Chief Collection Privado
Acciones
Reglas de entrada
Nueva regla...
Filtrar por perfil
Filtrar por estado
Filtrar por grupo
Ver
Actualizar
Exportar lista...
Ayuda


La aplicación del
Reglas de salida
Nombre
Grupo
Asistente para nueva regla de entrada
Tipo de regla
Seleccione el tipo de regla de firewall que desea crear.
Pasos:
Tipo de regla
Protocolo y puertos
Acción
Perfil
Nombre
¿Qué tipo de regla desea crear?
Programa
Regla que controla las conexiones de un programa.
Puerto
Regla que controla las conexiones de un puerto TCP o UDP.
Predefinida:
Administración de tarjetas inteligentes virtuales TPM
Regla que controla las conexiones de una experiencia con Windows.
Personalizada
Regla personalizada.
< Atrás
Siguiente >
Cancelar

Lo segundo, en la sección de “protocolos y puertos” vamos a aplicar la regla al puerto TCP, y vamos a escribir el número de nuestro puerto especifico, el cual es 3389.

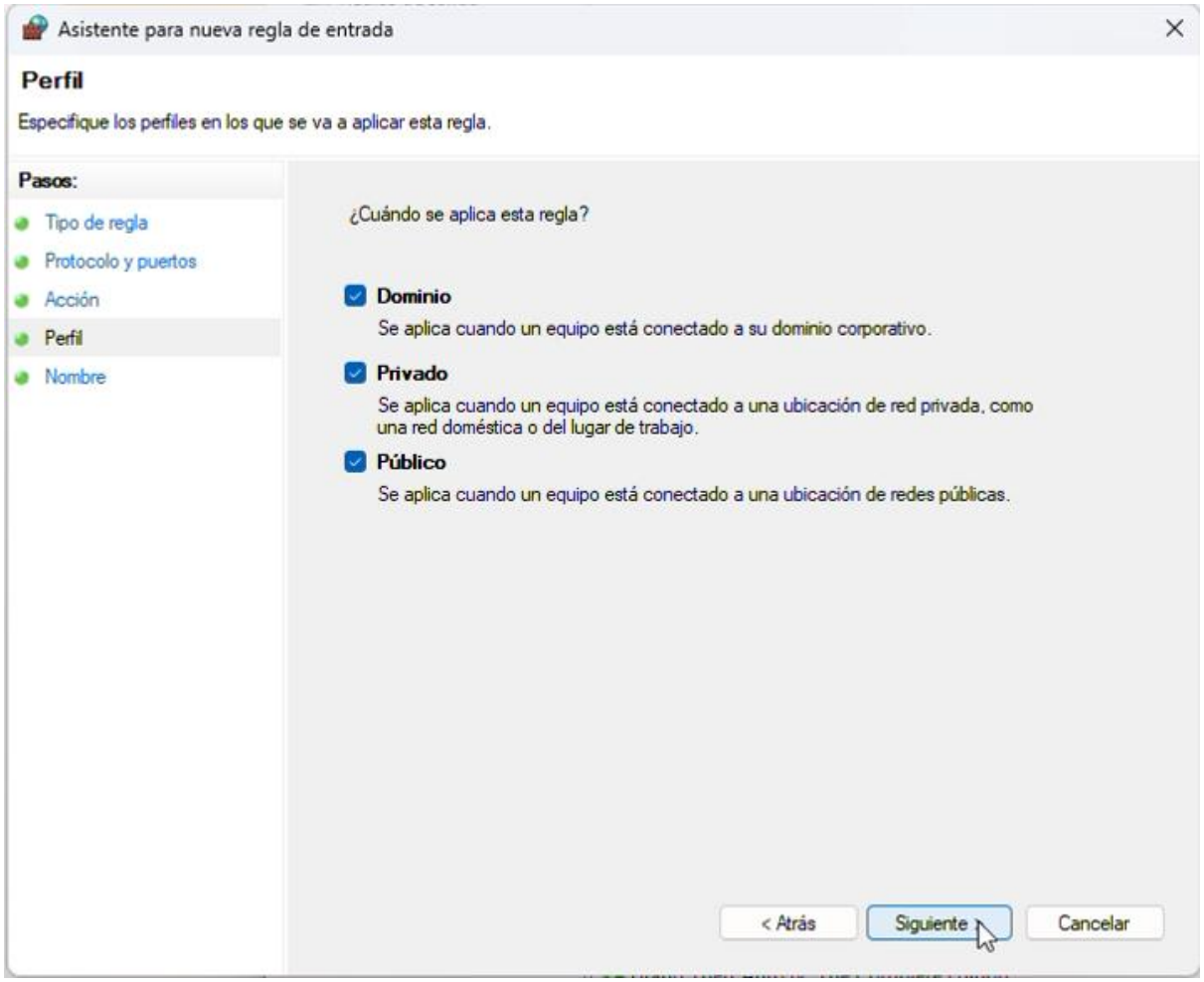


Luego en la sección “acción” procederemos a bloquear la conexión, para prohibir cualquier acceso no deseado de manera remota.

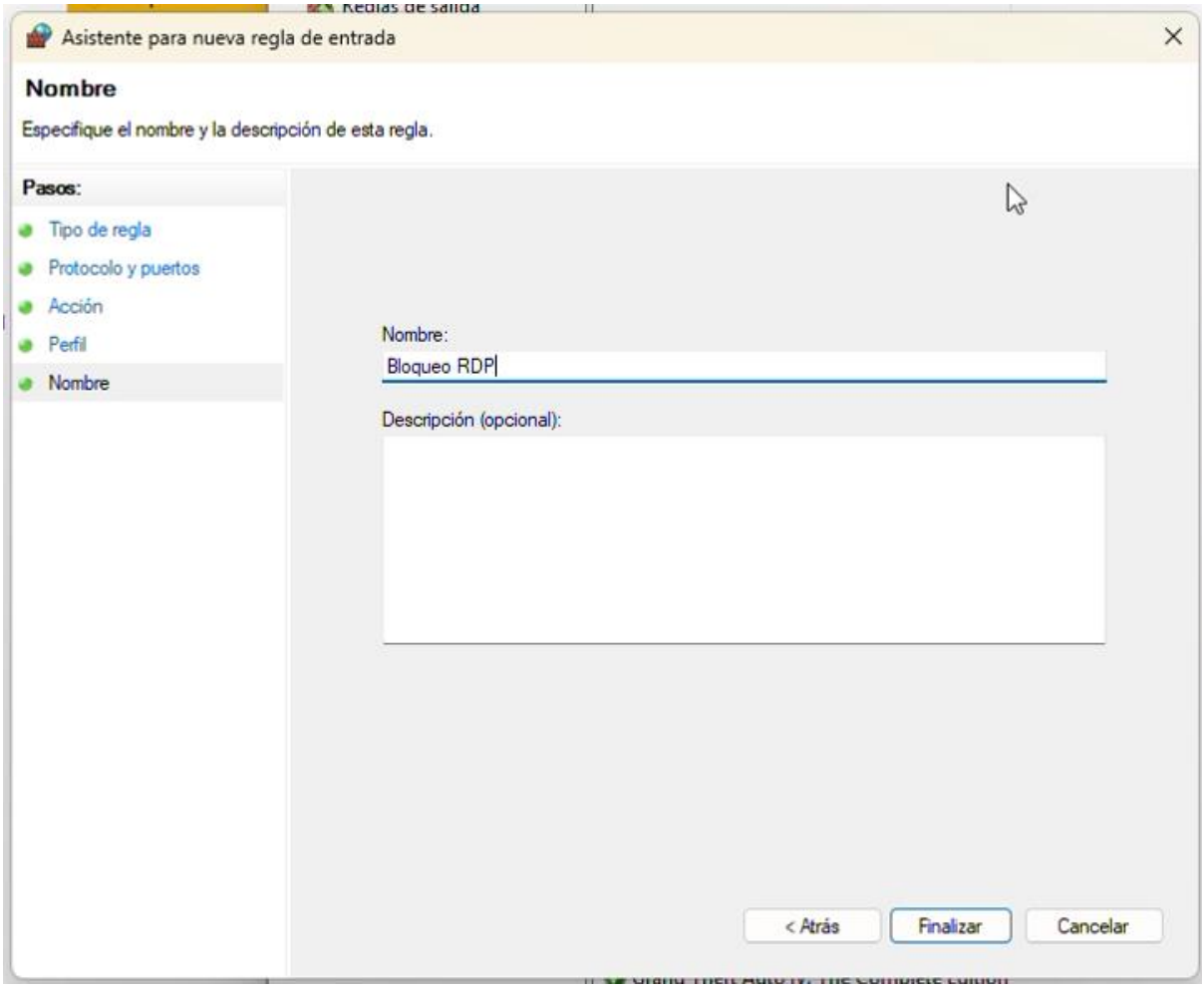


Luego en la sección ”perfil” marcaremos los tres casilleros disponibles, para aplicar

la regla siempre.



Luego en la parte de nombre, le daremos un nombre a nuestro parche, elegimos el nombre “Bloqueo RDP”. Luego procederemos a finalizar, y así quedo asegurado nuestro puerto.



4. Metodología utilizada

Para desarrollar el caso práctico sobre detección y protección de puertos en Windows, se siguieron los siguientes pasos:

1. Investigación técnica: Se consultaron guías oficiales de Microsoft y documentación técnica sobre la gestión de puertos, firewall, auditoría y servicios en Windows.
2. Simulación de entorno real: Se utilizó una PC con sistema operativo Windows 10/11 para simular un entorno empresarial.
3. Escaneo de red: Se empleó la herramienta Nmap para detectar puertos abiertos y servicios activos.
4. Evaluación de servicios y usuarios: Se identificaron los servicios asociados a los puertos abiertos y los usuarios que los ejecutaban.
5. Aplicación de medidas de seguridad: Se modificaron reglas del Firewall, se cerraron puertos innecesarios y se ajustaron configuraciones para limitar el acceso remoto.

6. Registro de resultados: Se documentaron los cambios, capturas de pantalla, medidas tomadas y pruebas realizadas antes y despúes.

5. Resultados obtenidos

A partir del análisis y pruebas realizadas, se obtuvieron los siguientes resultados:

- Se detectaron puertos abiertos (3389 y 445) utilizados por servicios críticos como Escritorio Remoto (RDP) y SMB.
- Se confirmó que dichos puertos estaban expuestos a conexiones desde cualquier dirección IP, sin restricciones de red ni autenticación fuerte.
- Se configuraron reglas de firewall para bloquear puerto 445 y restringir el 3389 a IP autorizadas.
- Se desactivó SMBv1 y se ajustaron servicios innecesarios para reducir la superficie de ataque.
- Se activó la auditoría de eventos de acceso remoto y cambios de configuración.
- Se mejoró la seguridad general del sistema mediante el cierre de puertos no utilizados y aplicación de buenas prácticas recomendadas por Microsoft.

7. Conclusiones

El presente trabajo permitió comprender de manera práctica cómo la gestión adecuada de los puertos de red en sistemas operativos Windows es clave para prevenir accesos no autorizados y proteger los servicios del sistema.

Se comprobó que muchos servicios se encuentran abiertos por defecto, y que su exposición sin restricciones representa un riesgo real en entornos empresariales. La aplicación de herramientas como Nmap, el uso correcto del firewall, la restricción de privilegios y la activación de auditoría permiten reforzar la seguridad del sistema operativo de forma eficaz.

Pequeñas configuraciones, como cerrar puertos no autorizados o restringir accesos po IP, pueden marcar una gran diferencia en la defensa contra amenazas externas. Además, el análisis evidenció la importancia de combinar controles técnicos con una buena administración de usuarios y monitoreo constante.

8. Bibliografía

Microsoft Docs. (2024). *Ver puertos abiertos con netstat*. Recuperado de: https://learn.microsoft.com/es-es/windows-server/administration/windows-commands/netstat

9. Microsoft Learn. (2024). *Configurar reglas del firewall de Windows Defender*. Recuperado de: https://learn.microsoft.com/es-es/windows/security/threat-protection/windows-firewall/create-an-inbound-port-rule
10. Nmap Project. (2024). *Nmap Network Scanning – Official Documentation*. Recuperado de: https://nmap.org/book/
11. Stallings, W. (2018). *Seguridad en Computadoras y Redes*. Pearson Educación.
12. Tanenbaum, A. S., & Wetherall, D. J. (2011). *Redes de computadoras* (5ª ed.). Pearson.
13. Instituto Nacional de Ciberseguridad (INCIBE). (2023). *Gestión de puertos y servicios expuestos*. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/puertos-red
14.