SEGURIDAD EN SISTEMAS OPERATIVOS

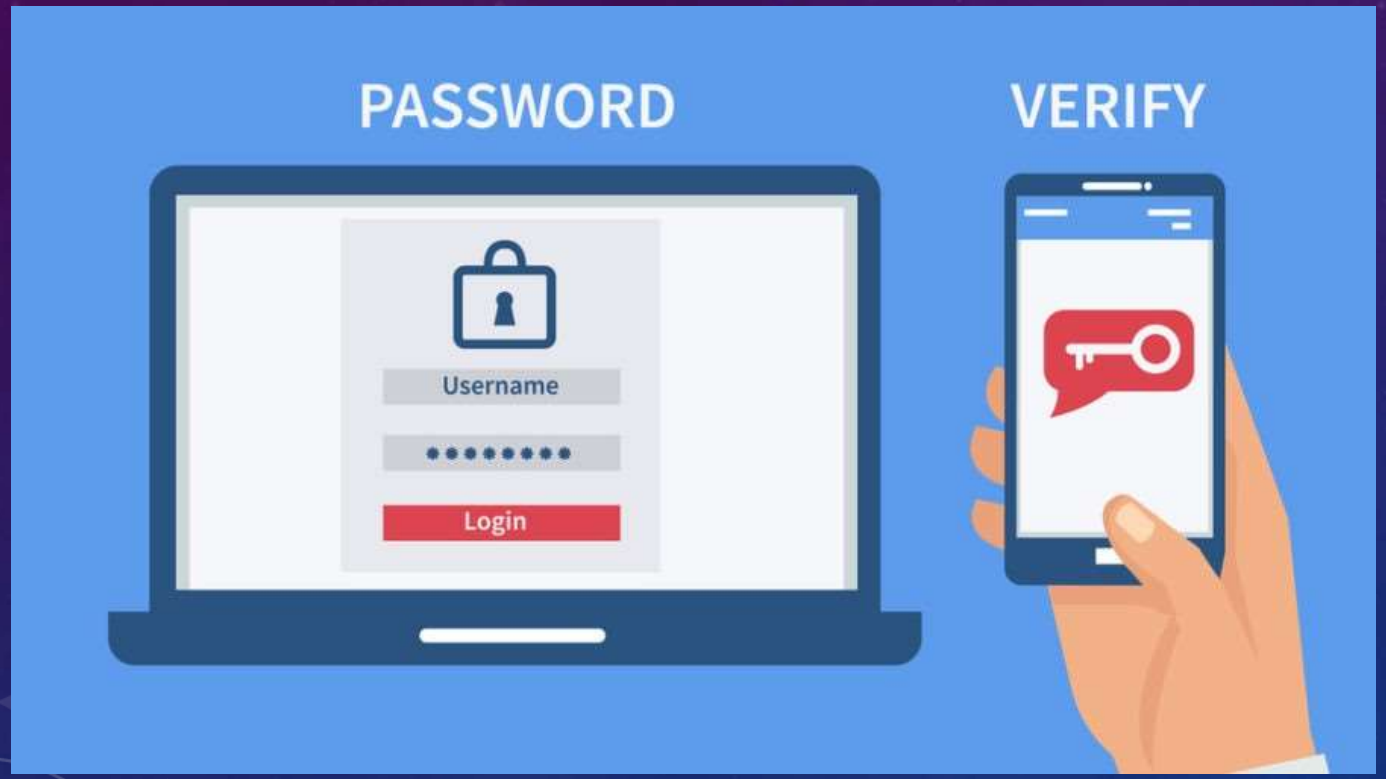
GESTIÓN DE LA SEGURIDAD DE PUERTOS EN SISTEMAS OPERATIVOS WINDOWS

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)**
- **Registrados (1024-49151)**
- **Dinámicos o privados (49152-65535)**

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.

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).

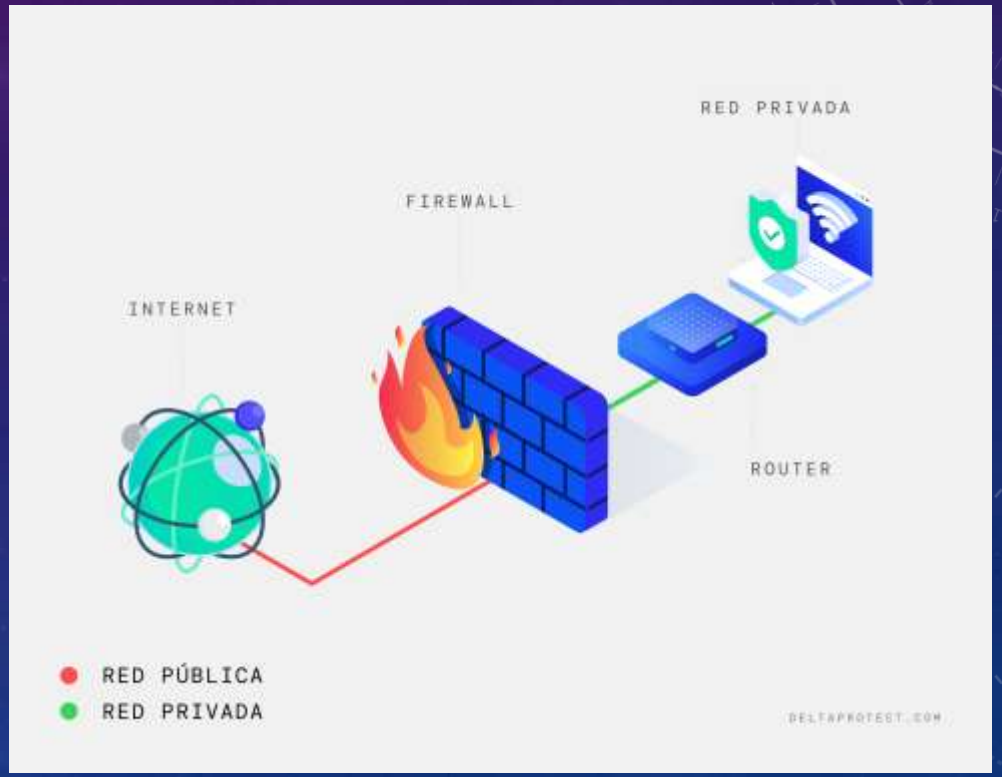
Una de las herramientas más comunes para este fin es **Nmap**, que permite identificar:

- 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:

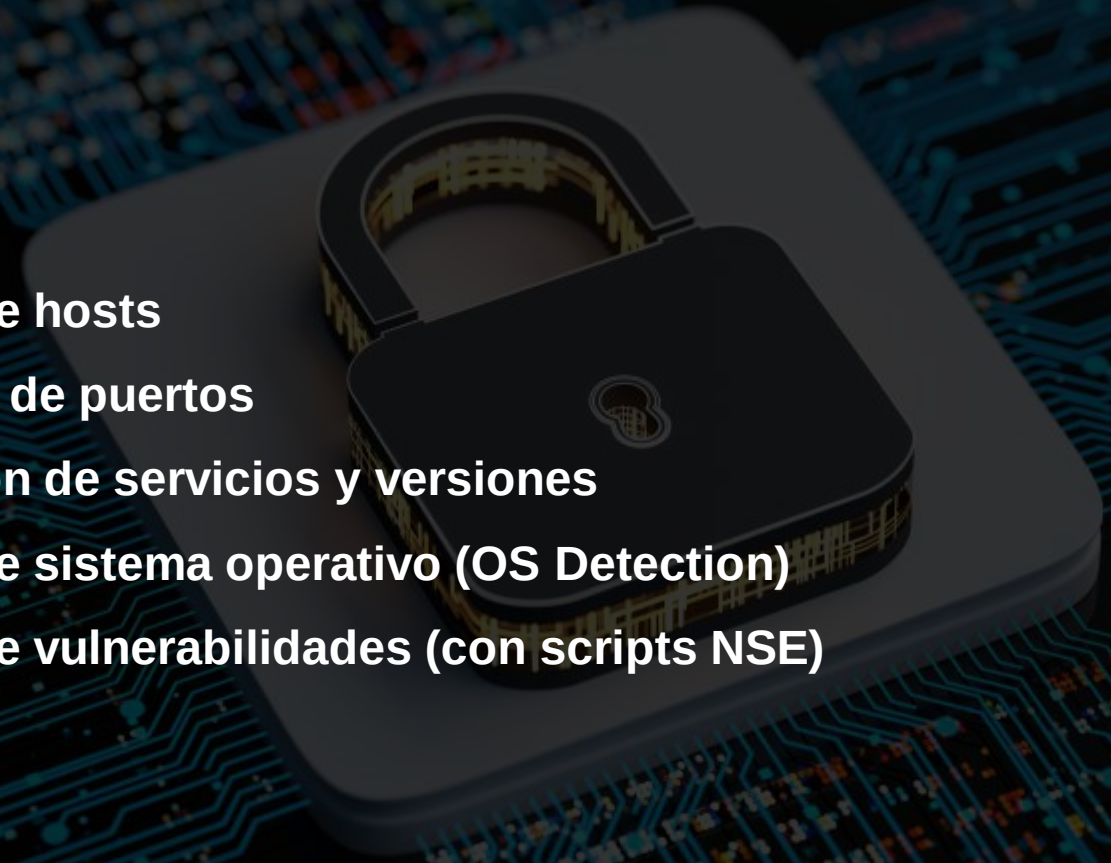
- Bloquear puertos innecesarios.
- Limitar accesos según direcciones IP, protocolos o servicios.
- Registrar intentos de conexión.
- Esencial para la seguridad de la red.
- Permite el filtrado de tráfico entrante y saliente.
- Reglas personalizables.
- Monitoreo en tiempo real.
- Integración con el Centro de Seguridad de Windows



AUDITORÍA DE PUERTOS Y SERVICIOS

- 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



- **Detección de hosts**
- **Exploración de puertos**
- **Identificación de servicios y versiones**
- **Detección de sistema operativo (OS Detection)**
- **Detección de vulnerabilidades (con scripts NSE)**

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.
-

CASO PRACTICO

- Gabriel debe realizar una auditoría de seguridad en una empresa de activos financieros.
- Se simulo un escaneo de puertos con Nmap.
  - Se encontró abierto el puerto 3389.
  - Se aplico una medida de seguridad mediante Firewall de Windows Defender.

RESULTADOS OBTENIDOS – CONCLUSIONES

- 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.
- 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 (de forma ética), el uso correcto del firewall, la restricción de privilegios y la activación de auditoría permiten reforzar la seguridad del sistema operativo de forma eficaz.