

PUERTOS EN REDES



@saulruizplaza

¿QUÉ ES UN PUERTO?



Canal lógico que permite la **comunicación** entre dispositivos mediante una dirección IP

Cada servicio en una máquina emplea un puerto único que le **asigna a su tráfico**, razón por la cual varias aplicaciones pueden ejecutarse al mismo tiempo. La correcta configuración de un puerto es importante para el correcto funcionamiento de la red así como para su seguridad.

TIP

Documenta y **controla los puertos activos** para bien identificar accesos no autorizados.

@saulruizplaza

The background is black with a pattern of small, dark brown dots. There are three thick, orange brushstrokes: one in the top left corner, one in the top middle, and one in the bottom right corner.

TIPOS DE PUERTOS

PUERTOS BIEN CONOCIDOS (0-1023)



Destinados para aquellos **servicios y protocolos imprescindibles** que hacen posible la comunicación fundamental en las redes privadas y en internet.

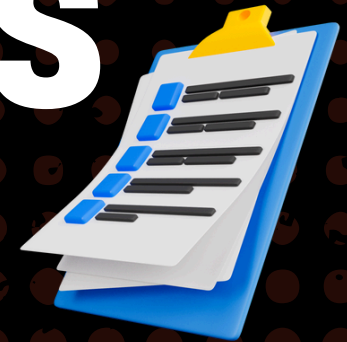
Estos puertos están **estandarizados**, lo que implica que los servicios se configurarán exactamente igual en cualquier dispositivo de esa red o de la red de internet.

TIP

Asegúrate de que estén tan solo **activos los servicios imprescindibles**, ya que cualquier vulnerabilidad presente en ellos podría comprometer a toda la red.

@saulruizplaza

PUERTOS REGISTRADOS (1024-49151)



Asignan a **aplicaciones y servicios específicos** (por ejemplo, bases de datos o herramientas comerciales). Aunque no son tan universales como los puertos bien conocidos, su incorrecta configuración puede dar lugar a vulnerabilidades.

CONSEJO

De forma regular, **verifica la configuración** de todos aquellos servicios que hacen uso de puertos registrados. Impone también **restricciones de acceso** basadas en roles y seguridad mediante sistemas de autenticación saneados para minimizar riesgos.

@saulruizplaza

PUERTOS DINÁMICOS

(49152-65535)



Asignan de forma **temporal** a conexiones salientes y solicitudes efímeras, como las que pueden derivar de videoconferencias o juegos en línea. Su uso es necesaria y útil, aunque es importante controlar el acceso a su rango de puertos para evitar accesos no deseados.

CONSEJO

Revisa la configuración del firewall para restringir el rango de puertos dinámicos sólo a los que sean necesarios.

@saulruizplaza



**PUERTOS MÁS
EXPLOTADOS**

FTP (21)



Es un puerto muy atacado debido a su configuración de la que la cuál puede permitir accesos anónimos en ocasiones y **transferencias** de datos sin cifrar. Los atacantes pueden beneficiarse de las configuraciones inseguras interceptando o modificando archivos sensibles en cuestión.

¿CÓMO PROTEGERSE?

- Deshabilitar o **restringir** el **acceso** anónimo.
- Implementar protocolos seguros como **SFTP** o **FTPS** en vez del tradicional FTP.
- Habilitar regularmente las **actualizaciones** y parches de seguridad.
- Establecer un Firewall para **limitar el acceso** a las direcciones IP autorizadas.

@saulruizplaza

SSH (22)



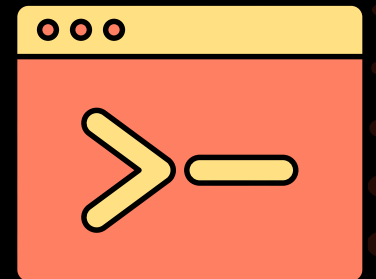
Blanco habitual para los ataques de fuerza bruta, de los que los atacantes tratan de adivinar credenciales de acceso mediante **fuerza bruta**, siendo una falla en la implementación y el uso de contraseñas poco complejas el punto de acceso a sistemas críticos.

¿CÓMO PROTEGERSE?

- Usar la **autenticación** basada en claves en lugar de contraseñas poco complejas.
- **Reemplazar el puerto por defecto** para dificultar la detección automatizada.
- Utilizar la política de **bloquear el acceso** después de fallar en múltiples situados.
- **Restringir el acceso** mediante listas blancas de IPs.

@saulruizplaza

TELNET (23)



Tiene un alto riesgo de seguridad pues transporta la información decodificándola en texto plano, lo que permiten a los atacantes **interceptar las credenciales** y otra información mediante el monitoreo de redes inseguras.

¿CÓMO PROTEGERSE?

- Tomar como alternativas seguras como el **servicio SSH** que requiere usuario y contraseña.
- Si se requiere el uso de Telnet, entonces úsalo a través de una **VPN** para poder cifrar la conexión.

@saulruizplaza

SMB (445)



SMB (Server Message Block) es un protocolo de comunicación de red empleado para la **compartición de archivos e impresoras** en entornos de Windows.

Este puerto se vio gravemente explotado en grandes ataques como el **WannaCry**. Las vulnerabilidades que presenta este servicio pueden llegar a permitir la propagación de ransomware y el acceso no autorizado a todos los recursos compartidos de la red.

¿CÓMO PROTEGERSE?

- **Cerrar el puerto** si el servicio SMB no es indispensable
- Aplicar de manera inmediata todos los **parches** y actualizaciones de seguridad
- **Segmentar la red** para limitar la exposición de los equipos que utilizan SMB

@saulruizplaza

RDP (3389)



El puerto 3389 utilizado para el protocolo RDP en **conexiones remotos** de sistemas Windows en ataques de fuerza bruta y explotación de vulnerabilidades. La exposición del protocolo RDP sin las medidas adecuadas puede permitir a un atacante tomar control remoto de un sistema.

¿CÓMO PROTEGERSE?

- Reemplazar el puerto por defecto o utilizar una VPN para acceder al protocolo RDP de forma segura.
- Usar la **autenticación multifactor (MFA)** para incrementar la seguridad del protocolo.
- Limitar el acceso a direcciones IP concretas mediante reglas de firewall.
- Controlar los intentos de acceso y aplicar bloqueos automáticos ante un comportamiento anómalo.

@saulruizplaza

The background is black with a pattern of small, dark brown dots. Two thick, orange brushstrokes are visible: one in the top left corner curving downwards, and another in the bottom right corner forming a loop.

HERRAMIENTAS GESTIÓN DE PUERTOS

NMAP

Nmap (Network Mapper) es una de las herramientas más completas para **escanear puertos y detectar servicios**. Con ello se puede saber qué puertos abiertos, qué servicios están en ejecución, y qué sistemas operativos están presentes. Constituye una de las herramientas más potentes para detectar vulnerabilidades dentro de la red

TIP

- **Automatiza escaneos periódicos** para tener siempre bajo control qué puertos están abiertos en tu red.



NMAP

@saulruizplaza

WIRESHARK

Analizador de protocolos de red, viene en formato gratuito y de código abierto para **analizar, en tiempo real, el tráfico de red en una red en vivo** garantizándote la visualización para que examines lo que ocurre en tu red; considerando de manera adecuada la detección de problemas, anomalías o atacantes que exploten los puertos.

TIP

- Filtra el tráfico por puertos específicos para analizar el comportamiento y la seguridad de servicios concretos. Por ejemplo, usa el filtro `tcp.port == 80` para ver el tráfico HTTP.



Wireshark

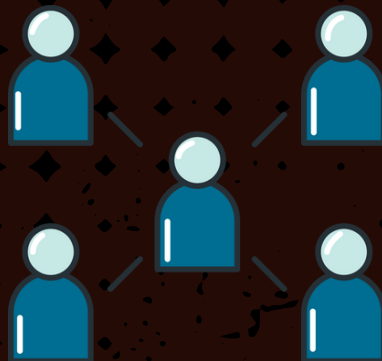
@saulruizplaza

NETSTAT

Netstat es una herramienta que te permite ver las **conexiones activas en tu dispositivo**, mostrando qué puertos están abiertos y qué servicios los están utilizando. Es muy útil para ver en tiempo real qué puertos están siendo utilizados por procesos en tu sistema.

CONSEJO

- Usa **Netstat** junto con el comando **-p** para ver qué procesos están utilizando los puertos. Esto te permite identificar si algún servicio sospechoso está escuchando en un puerto específico.



@saulruizplaza

A thick, orange brushstroke graphic that starts from the left edge, loops around, and ends near the top center of the image.

MUCHAS GRACIAS



[@saulruizplaza](#)