# Puertos vulnerables, problemas comunes en un servicio de red

Puertos vulnerables, problemas comunes en un servicio de red. Las vulnerabilidades en los servicios de red **pueden provocar la pérdida de datos**, la denegación de servicios o permitir que los atacantes faciliten los ataques contra otros dispositivos.

La verificación de servicios inseguros o no esenciales es fundamental para reducir el riesgo en la red. Al identificar puertos abiertos junto con sus servicios asociados, puede garantizar que dichos servicios sean necesarios y que los riesgos asociados se mitiguen en consecuencia.
La gran mayoría de los ataques a la red se centran en vulnerabilidades fácilmente identificables que pueden ser explotadas. Los ataques dirigidos utilizan una vulnerabilidad particular y una metodología bien definida.

## ¿Qué estamos protegiendo y por qué son importantes los puertos abiertos?


Un puerto puede considerarse como un **refinamiento de la dirección IP** de una computadora. Un paquete destinado a una dirección IP se enrutará al dispositivo que posee esa dirección IP en particular. Esta dirección IP solo identifica el dispositivo en la red. Un puerto define además dónde se debe entregar ese paquete, y define el tipo de conexión que se debe hacer. Un puerto abierto es esencial para que los dispositivos que usan un protocolo específico se conecten entre sí. La Autoridad de Números Asignados de Internet (IANA) ha desarrollado varias categorías de puertos:

- 1 a 1023 son conocidos como puertos bien conocidos
- 1024 a 49151 son conocidos como puertos registrados
- 49152 a 65535 son conocidos como puertos dinámicos

Los puertos bien conocidos generalmente hacen algún tipo de conexión de red y, por lo general, se asignan a un protocolo de red en particular. Estos puertos conocidos son descritos por la IANA como puertos que «solo pueden ser utilizados por procesos del sistema (o raíz) o por programas ejecutados por usuarios privilegiados». Los puertos en este rango tienen asignado un protocolo de red específico.

Los puertos registrados se definen como puertos que «pueden ser utilizados por procesos de usuarios ordinarios o programas ejecutados por usuarios comunes». Los puertos registrados suelen estar disponibles para cualquier programa que desee utilizarlos. Si bien la IANA de hecho registra números de puerto en este rango, no asignan un protocolo de red.

Finalmente, los puertos dinámicos se definen como «puertos no asignados y no registrados para aplicaciones privadas, procesos del lado del cliente u otros procesos que asignan números de puertos de forma dinámica».

## Aumento de la visibilidad de la red con datos de uso de puertos

«Puertos comunes» es un refinamiento adicional de los rangos de puertos de puertos conocidos para describir los puertos que se encuentran comúnmente en varios sistemas. Por ejemplo, es probable que encuentre puertos como 22 / SSH, 25 / SMTP, 80 / HTTP y 443 / HTTPS, abiertos en la mayoría de las organizaciones. Las vulnerabilidades asociadas con esos puertos pueden ser fácilmente atacadas por intrusos por parte de los atacantes. **Comprender qué puertos están abiertos dentro de la red es un buen paso para reducir la probabilidad de compromiso** y, en algunos casos, mejorar el rendimiento.

Los ataques a la red no siempre son identificables rápidamente. Muchos ataques son bajos y lentos, creando canales de comando y control que les permiten filtrar más datos y permanecer sin ser detectados por más tiempo. La **complejidad de las redes y la multitud de puertos abiertos** en una organización hacen que la identificación de amenazas sea cada vez más difícil.

El enfoque más simple, directo y costoso es una postura reactiva en la que esperas a que suceda algo y lo arregle. Pero ese no es el mejor enfoque. La mejor solución es escanear y analizar proactivamente la infraestructura de red. Tenable.io permite a los analistas comparar puertos abiertos conocidos entre exploraciones. Se pueden detectar nuevos puertos activos y

vulnerabilidades, evitando posibles puntos ciegos donde se instalan o habilitan nuevos servicios.

Leer también:Vulnerabilidades “Meltdown” y “Spectre” afectan a los servidores web ; se pueden falsificar los certificados SSL; ¿puede Cpanel ser hackeado? Si asi fuere, cómo limpiarlo