5 Protocolos que los hackers explotan

X SEC
YOUR PATH TO CYBERSECURITY

Telnet

Es un protocolo que permite **conectarse de forma remota** a dispositivos como routers, switches o servidores. Fue creado en los años 70. Su gran problema es que transmite toda la **información en texto plano**. Esto significa que cualquier persona que intercepte esa comunicación puede ver los comandos enviados. Muchos dispositivos aún lo tienen habilitado por defecto.

Tips:

- Desactivá Telnet en todos los equipos si no lo usás.
- Usá SSH como alternativa: cifra las conexiones.
- No expongas el puerto 23 a Internet.

SNMP

SNMP (**S**imple **N**etwork **M**anagement **P**rotocol) se usa para **monitorear y administrar** dispositivos de red. El problema es que muchas veces se deja configurado con **valores por defecto**, como las cadenas “public” o “private”, que funcionan como contraseñas débiles. Además, SNMPv1 y SNMPv2 no cifran la información, lo que permite que un atacante obtenga detalles de la red, nombres de usuarios o configuraciones sin mucho esfuerzo.

Tips:

- Cambiá las “*community strings*” por valores seguros y únicos.
- Usá SNMPv3, que agrega autenticación y cifrado.
- Restringí el acceso solo a IPs de confianza.

RDP

RDP (**R**emote **D**esktop **P**rotocol) permite **acceder de forma remota** a una computadora con **Windows y controlarla** como si estuvieras sentado frente a ella. Es muy útil para administración remota, pero si está **expuesto** a Internet sin seguridad, es un **gran riesgo**. Los atacantes suelen buscar sistemas con RDP habilitado en el puerto 3389 y probar contraseñas débiles o usar credenciales filtradas.

Tips:

- Nunca expongas el puerto 3389 a Internet.
- Usá una VPN para acceder de forma segura.
- Establecé contraseñas fuertes y políticas de bloqueo por intentos fallidos.

NTP

NTP (**N**etwork **T**ime **P**rotocol) se usa para **sincronizar el reloj de los dispositivos con servidores** confiables. Pero algunos servidores NTP están mal configurados y permiten responder con grandes cantidades de datos a pequeños pedidos. Los atacantes abusan de esto para lanzar ataques de denegación de servicio distribuida (**DDoS**), **amplificando el tráfico hacia una víctima**. Este tipo de ataque se conoce como NTP amplification.

Tips:

- No expongas servidores NTP a Internet.
- Configurá el servicio para que no permita comandos como "*monlist*" si es público.
- Usá firewalls para restringir acceso.

UPnP

UPnP (**U**niversal **P**lug a**n**d **P**lay) permite que **dispositivos** dentro de una red, como cámaras, **abran puertos automáticamente en el router** para facilitar la conexión con el exterior. El problema es que UPnP **no requiere autenticación**: cualquier malware en la red interna puede abrir un puerto y exponer un servicio sensible a Internet. Muchos routers permiten esto por defecto sin mostrar ninguna alerta.

Tips:

- Desactivá UPnP en el router si no lo necesitás.
- Revisá regularmente qué puertos están abiertos.
- Evitá usar UPnP en redes donde haya dispositivos no confiables.

Seguinos y unite al discord para seguir aprendiendo

Guardar **Compartir** **Seguir**