Informe - Puertos abiertos y servicios asociados
10.0.0.102

Fecha/hora del escaneo: 2026-01-08 15:17 EST

Comando ejecutado: `sudo nmap -sS -sV -Pn 10.0.0.102`

1. Objetivo

Verificar si existen puertos abiertos innecesarios que incrementen la superficie de ataque del sistema, e identificar los servicios asociados a cada puerto detectado.

2. Evidencia del escaneo

Salida relevante de Nmap (detección de servicios y versiones):

```
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-08 15:17 EST
Nmap scan report for 10.0.0.102
Host is up (0.00095s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
Service Info: OS: Unix; CPE: cpe:/o:linux:linux_kernel
```

3. Puertos detectados y servicios asociados

Puerto	Estado	Servicio	Versión detectada	Riesgo / motivo
21/tcp	open	FTP	vsftpd 3.0.3	Aumenta superficie de ataque (fuerza bruta, exposición de archivos). Riesgo mayor si no usa TLS o si no es necesario.
22/tcp	open	SSH	OpenSSH 9.2p1 Debian 2+deb12u3	Administración remota. Debe restringirse (solo IPs permitidas/llaves). Innecesario si no se administra por red.
80/tcp	open	HTTP	Apache httpd 2.4.62 (Debian)	Servicio web expuesto. Innecesario si no se hospeda una aplicación web; si se usa, requiere hardening y parches.

4. Identificación de puertos potencialmente innecesarios

Un puerto se considera potencialmente innecesario cuando el servicio no es requerido por el objetivo del sistema o no debería estar accesible desde la red. Con base en el escaneo:

- 21/tcp (FTP): Suele considerarse innecesario salvo que el sistema requiera transferencia por FTP. Preferible SFTP/FTPS y limitar acceso.
- 80/tcp (HTTP): Innecesario si no existe un sitio/aplicación web que deba estar accesible. Si existe, aplicar hardening y mantener actualizado.
- 22/tcp (SSH): Normalmente necesario para administración, pero debe controlarse (solo IPs confiables, autenticación por llaves, deshabilitar root).

5. Recomendaciones de mitigación

- Deshabilitar servicios no requeridos para reducir superficie de ataque.
- Restringir acceso por firewall (UFW/iptables) a puertos administrativos (por ejemplo, SSH) solo desde IPs autorizadas.
- Aplicar actualizaciones de seguridad del sistema y de servicios (OpenSSH/Apache/vsftpd) y revisar configuración segura.
- Habilitar cifrado y autenticación robusta en servicios expuestos (por ejemplo, evitar FTP sin TLS y preferir SFTP).
- Auditar logs y revisar intentos de acceso (por ejemplo, /var/log/auth.log, logs de Apache y servicio FTP).

6. Comandos sugeridos para evidencia adicional

```
En la VM (Debian):
  sudo ss -lntup
  sudo ss -tulpn | egrep ':21|:22|:80'
  sudo systemctl status vsftpd ssh apache2 --no-pager

Desde la máquina atacante (Kali):
  sudo nmap -sS -sV -Pn 10.0.0.102
  sudo nmap -sS -sV -p- -Pn 10.0.0.102
```

Anexo - Captura de pantalla del escaneo

Figura 1. Salida del comando Nmap ejecutado desde Kali contra el host objetivo.