Reporte de Vulnerabilidades de Servicios Detectados

Introducción

Este informe documenta las vulnerabilidades detectadas en los servicios identificados durante un escaneo con Nmap al host 192.168.18.60. Las vulnerabilidades se identificaron utilizando bases de datos públicas como NVD y CVE Details, y están asociadas a versiones específicas de servicios detectados.

Resumen del Escaneo Nmap

Host escaneado: 192.168.18.60

Puerto abierto detectado:

- 80/tcp: Apache httpd 2.4.62 (Debian)

Port	Service	Version	Vulnerability	Description	Reference
80	HTTP	Apache 2.4.62	CVE-2021-40438	Server Side Request Forgery (SSRF) in mod_proxy.	https://nvd.nist.gov E-2021-40438

Vulnerabilidades Detectadas

- Vulnerabilidad en `mod_proxy` permite a un atacante hacer peticiones a servidores internos.

- Actualizar Apache HTTP Server a la última versión disponible que corrija las vulnerabilidades conocidas.

- Configurar adecuadamente los módulos como mod_proxy si no son necesarios.

- Implementar monitoreo continuo y escaneos de vulnerabilidad regulares.

- Aplicar principios de seguridad en profundidad para mitigar el riesgo ante servicios expuestos.

Conclusión

Las vulnerabilidades identificadas demuestran la importancia de mantener actualizados los servicios del sistema. Se recomienda seguir buenas prácticas de gestión de parches y realizar escaneos periódicos para detectar servicios expuestos y vulnerabilidades asociadas.