Reporte de Pentesting - AlamOps.com

Fecha del Reporte: 10/04/2025

Dominio Evaluado: https://alamops.com

Índice

1. WHOIS — Información del Dominio

Herramienta: WHOIS (https://linux.die.net/man/1/whois)

Descripción: Protocolo para consultar información pública de un dominio.

Sitio oficial: https://whois.domaintools.com

Bash usado:
whois alamops.com

Resultado:
- Dominio: alamops.com
- Registrador: GoDaddy.com, LLC
- Fecha de creación: 09/10/2024
- Expira: 09/10/2027
- Estados del dominio: clientDeleteProhibited, clientRenewProhibited
- DNS: NS67.DOMAINCONTROL.COM, NS68.DOMAINCONTROL.COM

2. Nmap — Escaneo de Puertos y Servicios

Herramienta: Nmap (https://nmap.org/)

Descripción: Escáner de red para descubrir hosts, puertos abiertos y servicios.

Bash usado:
nmap -sV -O -T4 alamops.com -oN nmap_results.txt

Resultado:
Puerto 22/tcp - SSH (OpenSSH 9.6p1)
Puerto 80/tcp - HTTP (nginx 1.24.0)
Puerto 443/tcp - HTTPS (nginx 1.24.0)
Puerto 8008/tcp - Desconocido
Sistema operativo detectado: Linux Kernel

3. Nikto — Análisis de Seguridad Web

Herramienta: Nikto (https://cirt.net/Nikto2)

Descripción: Escáner web que detecta vulnerabilidades comunes en servidores.

Bash usado:
nikto -h https://alamops.com -output nikto_results.txt

Resultado:
- Faltan cabeceras de seguridad importantes:
  - X-Frame-Options
  - Strict-Transport-Security
  - X-Content-Type-Options

4. Sublist3r — Enumeración de Subdominios

Herramienta: Sublist3r (https://github.com/aboul3la/Sublist3r)

Descripción: Enumerador rápido de subdominios usando motores de búsqueda.

Bash usado:
sublist3r -d alamops.com -o subdominios.txt

Resultado:
Subdominios encontrados:

- www.alamops.com
- api-dev.alamops.com
- grafana.alamops.com
- jenkins.alamops.com
- pve.alamops.com

5. Amass — Enumeración de DNS

Herramienta: Amass (https://owasp.org/www-project-amass/)

Descripción: Enumeración avanzada de subdominios, relaciones DNS y trazado de infraestructura.

Bash usado:
amass enum -d alamops.com -o amass_subs.txt

Resultado:
- NS: ns68.domaincontrol.com, ns67.domaincontrol.com
- MX: Servidores de Google

6. SQLMap — Pruebas de Inyección SQL

Herramienta: SQLMap (https://sqlmap.org/)

Descripción: Herramienta automatizada para detectar e inyectar SQLi (inyecciones SQL).

Bash usado:
sqlmap -u "http://alamops.com/page.php?id=1" --batch --dbs

Resultado:
- Parámetro id analizado correctamente
- No se detectaron vulnerabilidades SQL
- Sitio redirige automáticamente a HTTPS
- No se detectó un WAF (firewall de aplicaciones web)

7. Recomendaciones Finales

Alta:
- Agregar cabeceras HTTP de seguridad (X-Frame-Options, HSTS)

Media:
- Configurar WAF / IPS en entorno de producción

Baja:
- Ocultar servicios sensibles (grafana, jenkins, pve)