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

1. Resumen de Información WHOIS

- **Dominio:** alamops.com
- **ID de Dominio:** 2923836650_DOMAIN_COM-VRSN
- **Registrador:** GoDaddy.com, LLC (http://www.godaddy.com)
- **Servidor WHOIS:** whois.godaddy.com
- **Fechas Clave:**
  - Creación: 09/10/2024
  - Última Actualización: 09/10/2024
  - Expiración: 09/10/2027
- **Estados del Dominio:**
  - `clientDeleteProhibited`

    - clientRenewProhibited
    - clientTransferProhibited
    - clientUpdateProhibited
- **Servidores de Nombre:**
    - NS67.DOMAINCONTROL.COM
    - NS68.DOMAINCONTROL.COM
- **DNSSEC:** No firmado (unsigned)

---

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

Resultados de Escaneo Nmap

- **Fecha:** 10/04/2025
- **IP:** 3.64.114.185
- **Hostname:** ec2-3-64-114-185.eu-central-1.compute.amazonaws.com

Puertos Abiertos y Servicios Detectados:

- **22/tcp - SSH**
    - Servicio: OpenSSH 9.6p1 (Ubuntu 3ubuntu13.8)
    - Claves Host: ED25519, ECDSA
- **80/tcp - HTTP**
    - Servicio: nginx 1.24.0 (Ubuntu)
    - Observación: Redirección a HTTPS
- **443/tcp - HTTPS**
    - Servicio: nginx 1.24.0 (Ubuntu)
    - Certificado SSL: Válido (19/02/2025 – 20/05/2025)
    - CN/SAN: alamops.com, www.alamops.com
    - Puerto 8008/tcp - Desconocido

Sistema Operativo Detectado: Linux (`cpe:/o:linux: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

. Análisis de Seguridad con Nikto

- **URL Analizada:** https://alamops.com
- **Servidor Web:** nginx/1.24.0 (Ubuntu)
- **Certificado SSL:** Let's Encrypt

Hallazgos de Seguridad:

- ❌ Falta cabecera `X-Frame-Options` (protección contra clickjacking).
- ❌ Falta cabecera `HTTP Strict-Transport-Security (HSTS).`
- ❌ Falta cabecera `X-Content-Type-Options` (protección contra MIME-sniffing).

Recomendaciones:

- Implementar cabeceras de seguridad faltantes.
- Actualizar configuraciones del servidor periódicamente.

---

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

Enumeración de Subdominios

- **Herramienta:** Sublist3r
- **Subdominios Identificados (7):**
  - www.alamops.com
  - api-dev.alamops.com

- grafana.alamops.com
- iac-dev.alamops.com
- jenkins.alamops.com
- pve.alamops.com
- registry.alamops.com

Hallazgos:

- Subdominios críticos detectados (ej. `grafana`, `jenkins`).
- Servicios de terceros (VirusTotal, DNSdumpster) bloquearon solicitudes.

Recomendaciones:

- Evaluar seguridad en subdominios de gestión interna.
- Ampliar técnicas de enumeración.

---

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

Enumeración de DNS

- **Herramienta:** Amass

Registros Clave:

- **Servidores de Nombre (NS):**
  - ns68.domaincontrol.com
  - ns67.domaincontrol.com
- **Registros MX:**
  - Servidores de Google Mail (aspmx.l.google.com y alternativos)

Recomendaciones:

- Reforzar seguridad contra ataques de DNS spoofing/hijacking.
- Validar configuraciones de correo electrónico.

---

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)