Prox Offensive

Sample Recon Audit

Target: acme-demo.net

Date: June 2025

Executive Summary

This sample audit illustrates how the Prox Offensive Recon Toolkit identifies exposed digital surface areas, including DNS configurations, open ports, subdomains, and OSINT trace data — all through non-intrusive methods.

DNS & Subdomain Discovery

```
A Record:       203.0.113.15
MX Record:      mail.acme-demo.net
Nameservers:    ns1.acme-demo.net, ns2.acme-demo.net

Discovered Subdomains:
- dev.acme-demo.net
- cpanel.acme-demo.net
- staging.acme-demo.net
- testmail.acme-demo.net
```

Email Exposure

```
support@acme-demo.net
admin@acme-demo.net
marketing@acme-demo.net

These emails were discovered via open directories,
breach data, and search engine footprints.
```

Service & Port Recon

```
203.0.113.15:
- 22/tcp   OpenSSH 8.0 (Linux)
- 80/tcp   Apache 2.4.41
- 443/tcp  Nginx 1.18.0 (TLS Cert expiring in 11 days)

Recommendations:
- Harden SSH config (consider key auth only)
- Apply SSL certificate renewal automation
- Mask staging environments from public DNS
```

OSINT Surface

- SSL Certificates: dev.acme-demo.net expired 3 months ago
- Shodan: lists Apache config version and open directory on /test
- Public Repos: hardcoded email discovered in GitHub commit logs
- WHOIS: Registrar data exposed admin email

Powered by Prox Offensive

This report was generated using tools like Nmap, crt.sh, theHarvester, and GPT-assisted summarization, bundled under the Prox Offensive Recon Toolkit.

Author: Felix Gutierrez (Don Trabajo)
Website: proxoffensive.com | GitHub: github.com/DonTrabajo