

Reconnaissance Report

Target Domain: example.com

Date: fri, jan 2

Tools Used: Maltego, Shodan

example.com

WHOIS Information

IP Address: [104.18.27.120](#)

Registrar Information

Registrar

RESERVED-Internet Assigned Numbers Authority

WHOIS Server

whois.iana.org

Referral URL

<http://res-dom.iana.org>

Important Dates

Created

1/1/1992

Updated

12/16/2025

Expires

8/13/2026

Nameservers

Hostname	IP Address
hera.ns.cloudflare.com	108.162.192.162
elliott.ns.cloudflare.com	108.162.195.228

Activities:
Perform Open-Source Intelligence (OSINT), map assets, and document findings.

- Tools:**
- Maltego
 - Shodan
 - Google Docs

- Tasks:**
- Gather domain information
 - Enumerate subdomains
 - Identify exposed services
 - Document steps in a structured format

Asset Mapping Table

Timestamp	Tool	Finding
2025-08-18 10:00:00	Shodan	Exposed SSH on 192.168.1.50
2025-08-18 10:30:00	Maltego	Subdomain: dev.example.com

WHOIS

Domain Name: example.com
Registrar: NameCheap, Inc.
Creation Date: 2010-08-14
Expiry Date: 2026-08-14
Name Servers: ns1.example.com, ns2.example.com

www.example.com – Main website
dev.example.com – Development environment
mail.example.com – Email server

Timestamp	Tool	Finding
2025-08-18 10:00	WHOIS	Domain registered to Example Org
2025-08-18 10:30	Maltego	Found dev.example.com
2025-08-18 11:00	Shodan	SSH exposed on 203.0.113.45

Domain Info

Domain Name: example.com
Registrar: NameCheap, Inc.
Creation Date: 2010-08-14
Expiry Date: 2026-08-14
Name Servers: ns1.example.com, ns2.example.com
Organization: Example Organization

Wappalyzer

Web Server: Nginx
CMS: WordPress
Language: PHP
Frameworks: jQuery
Security: Cloudflare CDN

Access Shodan

IP Address: 203.0.113.45

Open Port: 22
Service: SSH
Banner: OpenSSH 7.2p2
Observation: SSH publicly accessible

IP Address	Port	Service	Observation
203.0.113.45	22	SSH	Public SSH access
203.0.113.45	80	HTTP	Web service exposed

Timestamp	Tool	Finding
2025-08-18 11:00	Shodan	SSH exposed on 203.0.113.45
2025-08-18 11:10	Shodan	HTTP service detected

Perform OSINT (Information Gathering)

WHOIS lookup → domain ownership

Subdomain discovery → public DNS records

Tech stack identification → visible technologies

Internet exposure → open services

Tools used

- WHOIS (ICANN / who.is)
- Maltego
- Sublist3r

- Wappalyzer
- Shodan

OSINT was conducted using public tools to gather domain details, subdomains, technologies, and exposed services without interacting with target systems.

Asset types

- Domains & subdomains
- IP addresses
- Open ports
- Services (HTTP, SSH, SMTP)

Asset	Type	Tool	Notes
example.com	Domain	WHOIS	Primary domain
dev.example.com	Subdomain	Maltego	Development environment
203.0.113.45	IP	Shodan	Public-facing server

Summary

Reconnaissance identified critical assets and exposed services using OSINT tools. Domain information, subdomains, and technology stacks were documented systematically. Findings reveal potential attack surfaces, including open SSH services and publicly accessible subdomains, providing a foundation for further security assessment and prioritization of mitigation efforts.