

Recon

Target: tesla.com

Objective: Perform passive reconnaissance (OSINT) to identify publicly exposed assets, technologies, and services without active exploitation.

1. Scope & Rules

- **In-scope:** tesla.com and publicly accessible subdomains discovered via passive methods
- **Out-of-scope:** Active exploitation, credential attacks, DoS, or any intrusive testing
- **Methodology:** Passive OSINT only (WHOIS, search engines, tech fingerprinting, asset discovery)

2. Tools Used

- **Shodan** – Internet-exposed services and metadata
- **WHOIS (Sysinternals)** – Domain registration and DNS information
- **Subfinder** – Passive subdomain enumeration
- **Wappalyzer** – Technology stack identification
- **Google Docs** – Central documentation

3. Domain Information (WHOIS)

- **Domain:** tesla.com
- **Registrar:** MarkMonitor Inc.
- **Creation Date:** 1992-11-04
- **Expiry Date:** 2026-11-03
- **Domain Status:** clientDeleteProhibited, clientTransferProhibited, serverDeleteProhibited
- **Name Servers:**
 - A1-A28.AKAM.NET
 - EDNS69.ULTRADNS.(COM/NET/ORG/BIZ)

Observation: Tesla uses enterprise-grade DNS (Akamai + UltraDNS) with registry locks enabled, indicating mature security posture.

4. Subdomain Enumeration (Subfinder)

Passive enumeration identified multiple subdomains related to business functions, testing, and infrastructure.

Sample Findings: - www.tesla.com - engage.tesla.com - mail.tesla.com - webmail.tesla.com - testing.tesla.com - legacy.tesla.com - extranet.tesla.com - ns*.tesla.com

Observation: Presence of testing and legacy subdomains increases attack surface if not properly hardened.

```
(kali@kali)-[~]
$ subfinder -d tesla.com

projectdiscovery.io

[INF] Current subfinder version v2.9.0 (outdated)
[INF] Loading provider config from /home/kali/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for tesla.com
engage.tesla.com
www.im.tesla.com
im.tesla.com
sip.tesla.com
uat.tesla.com
win-uat-sa-lsc.tesla.com
cms.tesla.com
hqtime01.tesla.com
testing.tesla.com
asset.tesla.com
mail.tesla.com
testing2.tesla.com
webmail.tesla.com
www.cwa.tesla.com
hqex1.tesla.com
hquag1.tesla.com
ftp.tesla.com
helpdesk.tesla.com
ns5.tesla.com
sipexternal.tesla.com
uat4.tesla.com
arran.tesla.com
extranet.tesla.com
www.hqlynccedge.tesla.com
www.hquag1.tesla.com
legacy.tesla.com
webmaildr.tesla.com
itym.itymcrm.tesla.com
hqex2010.tesla.com
ns4.tesla.com
ns9.tesla.com
```

5. Technology Stack Identification (Wappalyzer)

Analysis of <https://tesla.com/contact> revealed the following stack:

- **CMS:** Drupal 9
- **CDN:** Akamai
- **Frontend:** React 18.3.1
- **Analytics:** Google Analytics (GA4), Facebook Pixel
- **Tag Management:** Google Tag Manager
- **Monitoring:** Sentry
- **Maps:** Google Maps

Observation: Modern frontend with third-party integrations. Analytics and tag managers are common entry points for misconfigurations.

The image shows a web browser window displaying the Tesla contact page. A Wappalizer overlay is visible on the right side, listing various technologies detected on the page. The technologies listed include:

- CMS:** Drupal 9
- CDN:** Akamai
- Analytics:** Google Analytics GA4, Facebook Pixel 2.9.248
- JavaScript frameworks:** React 18.3.1
- Issue trackers:** Sentry
- Maps:** Google Maps
- Advertising:** Twitter Ads
- Tag managers:** Google Tag Manager
- JavaScript libraries:** core-js 3.32.2

The Tesla contact page content includes sections for Sales, Customer Support, Roadside Assistance, and Service, each with a brief description and a link to further information.

6. Exposed Services (Shodan)

Shodan search for Tesla-related assets returned a large dataset of indexed IPs and services.

General Observations: - Global distribution of assets - Cloud-hosted infrastructure - Use of enterprise CDNs and reverse proxies

Note: No direct vulnerability exploitation was performed. Findings are observational only.

The image shows the Shodan search results for the query "tesla.com". The interface includes a search bar, a "Login" button, and a "Product Spotlight" section. The search results are displayed in a table with columns for IP address, location, and service details.

IP Address	Location	Service Details
158.158.117.42	Microsoft Singapore Pte. Ltd. Spain, Madrid	228 tesla.com ESHTP service ready\r\n
52.141.46.221	Microsoft Corporation Korea, Republic of, Seoul	228 tesla.com ESHTP service ready\r\n
37.60.251.247	mail.edu-tesla.com Contabo GmbH Germany, Dusseldorf	228 mail.edu-tesla.com ESHTP Haraka ready (FAABC9) 250-mail.edu-tesla.com Hello 224.197.174.281 [224.197.174.281], Haraka@Cloudron is at your service. 250-PIPELINING 250-8BITMIME 250-SMTPUTF8 250-SIZE 25000000 250-STARTTLS

The "Product Spotlight" section promotes "Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB".

7. Asset Mapping Log (Slack-Friendly)

Timestamp (UTC)	Tool	Finding
2026-01-01 10:15:00	WHOIS	MarkMonitor registrar, Akamai + UltraDNS NS
2026-01-01 10:25:00	Subfinder	Subdomains: testing.tesla.com, legacy.tesla.com
2026-01-01 10:40:00	Wappalyzer	Drupal 9, React 18, Akamai CDN
2026-01-01 11:00:00	Shodan	Large global asset footprint detected

8. Reconnaissance Checklist

- ✓ Perform WHOIS lookup
- ✓ Identify DNS and registrar protections
- ✓ Enumerate subdomains (Subfinder)
- ✓ Identify technology stack (Wappalyzer)
- ✓ Review exposed services via Shodan
- ✓ Document findings in Google Docs

9. Recon Summary

Tesla.com demonstrates a mature security posture with enterprise DNS, CDN protection, and modern web technologies. Passive reconnaissance revealed a wide global asset footprint, multiple functional subdomains, and a Drupal-React stack. No immediate misconfigurations were observed during OSINT-only analysis.