

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 tesl.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[INF] Current subfinder version v2.9.0 (outdated)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 tesl.com
engage.tesl.com
www.jm.tesl.com
im.tesl.com
sip.tesl.com
uat.tesl.com
win-uat-sa-lsc.tesl.com
cms.tesl.com
hqtime01.tesl.com
testing.tesl.com
asset.tesl.com
mail.tesl.com
testing2.tesl.com
webmail.tesl.com
www.cwa.tesl.com
hhex1.tesl.com
hquag1.tesl.com
ftp.tesl.com
helpdesk.tesl.com
ns5.tesl.com
sipexternal.tesl.com
uat4.tesl.com
arran.tesl.com
extranet.tesl.com
www.hqlyncedge.tesl.com
www.hquag1.tesl.com
legacy.tesl.com
webmaildr.tesl.com
itym.itymcrm.tesl.com
hhex2010.tesl.com
ns4.tesl.com
ns9.tesl.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 screenshot shows a browser window with the URL tesla.com/contact. The main content is the Tesla contact page, which includes sections for Sales, Customer Support, Roadside Assistance, Service, and Safety Recalls. Overlaid on the right side is the Wappalyzer extension interface, which provides detailed information about the technologies used in the page. Key findings include:

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

At the bottom right of the Wappalyzer panel, there is an email address: china-press@tesla.com.

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 screenshot shows the Shodan search interface with the query `tesla.com`. The results section displays 15 indexed assets, each with a summary and a detailed view option. The results are categorized by country and port.

Country	IP Address	Port	Description	Last Seen
Spain, Madrid	158.158.117.42	220	tesla.com ESHTP service ready\n\ncloud	2025-12-30T19:26:04.243864
Korea, Republic of, Seoul	52.141.46.221	220	tesla.com ESHTP service ready\n\ncloud	2025-12-29T11:14:24.023676
Germany, Dusseldorf	37.60.251.247	220	mail.edu-tesla.com ESHTP Haraka ready (FAABC9) Issued By: Let's Encrypt Common Name: mail.edu-tesla.com Organization: Let's Encrypt Subject Alternative Name: *.edu-tesla.com	2025-12-28T23:05:29.024117

Below the results, there are sections for **TOP COUNTRIES** and **TOP PORTS**, showing the most active regions and ports for the indexed assets.

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.