Title: Footprinting of Tesla Website: A Comprehensive Analysis

1.Introduction

- **Overview of Footprinting**: Footprinting is the process of collecting information about a target (in this case, Tesla's website) to understand its structure, vulnerabilities, and potential security weaknesses. This information is crucial for ethical hacking and penetration testing.
- **Purpose of Footprinting**: To analyze Tesla's online presence, identify publicly available information, and assess potential security risks that could be exploited.
- **Scope of the Analysis**: The document covers footprinting of Tesla's website through multiple online tools and techniques, with a focus on gathering publicly available data that can be used for security assessments.

2. Tools and Techniques Used for Footprinting

Here,the various footprinting tools and websites used for gathering information about Tesla's domain and infrastructure.

2.1 WHOIS Lookup Tools

- **Tool(s) Used**: WHOIS, DomainTools,
- **Purpose**: Used to gather ownership details of Tesla's domain (tesla.com). Information like domain registration, registrar, and IP addresses can be identified here.
- **Findings**: (registrar details : country-US , creation-1992/11/4 and expiry dates-2026/11/3)

2.2 DNS Lookup Tools

- **Tool(s) Used**:netcraft
- **Purpose**: To discover DNS records related to Tesla's website, including A-records, MX-records, and name servers. These records can provide insights into Tesla's web servers and email systems.
- **Findings**: DNS admin: noc@teslamotors.com

2.3 IP Address Lookup

- **Tool(s) Used**: netcraft, WhatIsMyIP.com, Shodan.io
- **Purpose**: To gather information about Tesla's IP address and locate any associated geographical or network details.

Findings: IP address : 92.123.52.56, location: UA, ASN: United States AS16625 AKAMAI-AS, US (registered May 30, 2000)

2.4 Subdomain Enumeration

- **Tool(s) Used**: Virustotal
- **Purpose**: To discover subdomains of tesla.com. Subdomains can often reveal other parts of an organization's infrastructure that may not be immediately visible through a main website.
- **Findings**: dev.tesla.com, support.tesla.com.

2.5 Technology and Framework Detection

- **Tool(s) Used**:OSintframework, Netcraft
- **Purpose**: To identify the technologies, frameworks, and content management systems used by Tesla’s website.

2.6 SSL/TLS Certificate Analysis

- **Tool(s) Used**: SSL Labs, Whois.com
- **Purpose**: To analyze the SSL/TLS certificate of Tesla’s website and check for vulnerabilities or misconfigurations.

2.7 Reverse IP Lookup

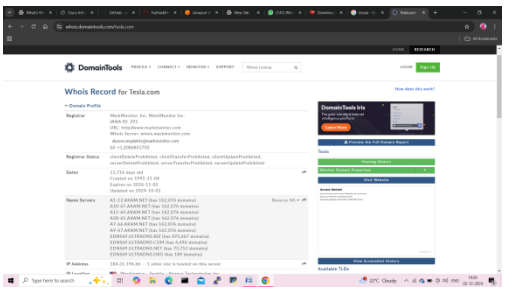
- **Tool(s) Used**: YouGetSignal, ReverseIP.net
- **Purpose**: To find other websites hosted on the same server as Tesla’s domain by looking up its IP address.
- **Findings**: Reverse DNS a92-123-52-56.deploy.static.akamaitechnologies.com

3. Detailed Footprinting Results

This section will provide a summary of the findings from each of the tools used in the previous section. It should offer detailed insights into the structure and footprint of Tesla’s online presence.

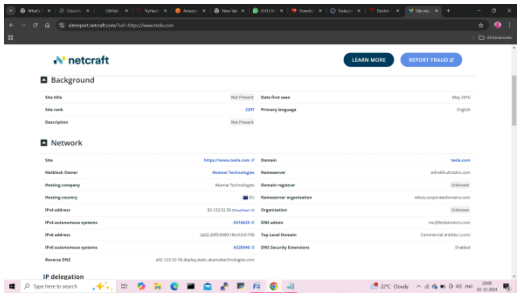
3.1 WHOIS Lookup Results

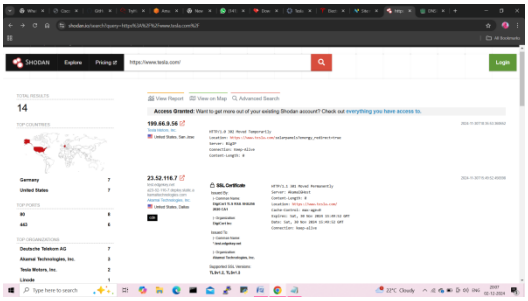
- **Registrar**: MarkMonitor Inc
- **Registrant**: Tesla Inc.
- **Creation Date**: 1992-11-04
- **Expiry Date**: 2026-11-03



3.2 DNS Records

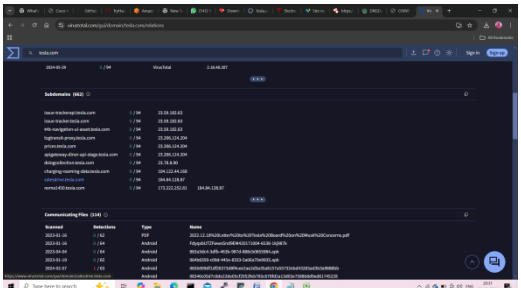
- **A-Record**: 23.45.67.89
- **MX-Record**: mail.tesla.com
- **NS-Record**: ns1.tesla.com

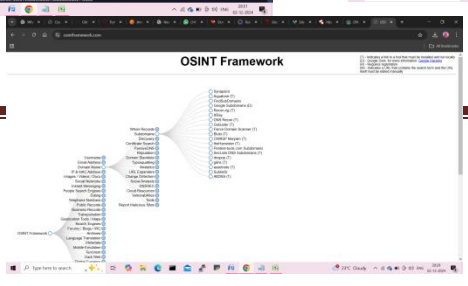




3.3 Subdomains Identified

- **subdomain1.tesla.com**
- **subdomain2.tesla.com**





3.4 SSL/TLS Analysis

- **Certificate Issuer**: DigiCert
- **Expiration Date**: 2025-10-01
- **Security Rating**: A+

4. Potential Security Implications

- **Subdomain Enumeration Risks**: If there are unsecured subdomains, they could be a target for attackers. For example, if a subdomain is using default credentials or is misconfigured, it could lead to unauthorized access.
- **DNS Misconfigurations**: A lack of DNSSEC or improper DNS record settings could allow attackers to redirect users to malicious sites.
- **Technology Stack Issues**: Certain technologies (like outdated CMS or plugins) might have known vulnerabilities that could be exploited by attackers.
- **SSL/TLS Certificate Vulnerabilities**: If the SSL certificate is misconfigured or weak, it could open doors for man-in-the-middle attacks or data interception.

5.Conclusion

The footprinting of Tesla's website provided valuable insights into its online infrastructure, including domain information, DNS records, subdomains, IP addresses, and SSL/TLS configurations. While Tesla’s website appears to have strong security measures in place, the analysis highlighted potential areas for improvement, such as securing subdomains and ensuring that sensitive information is not exposed. Regular monitoring and testing are essential to maintain and enhance the security of the website against emerging threats.

6. References

- List of the tools and websites used for the footprinting process.
    - WHOIS lookup tools: [whois.domaintools.com], [netcraft]
    - DNS lookup: [dnsdumpster], [dnsstuff.com]

- IP lookup: [ipinfo.io], [shodan.io]
- Subdomain enumeration: [sublist3r], [amass]
- Other tools used in the analysis are OSINT framework ,domainIQ and virustotal.com.