**TASK ONE: Passive Discovery Report**

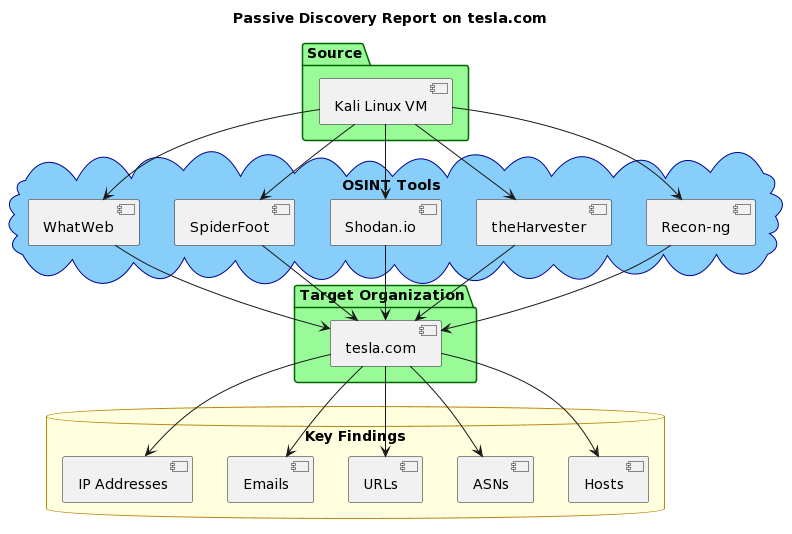
**1. Introduction**

Gathering Open Source Intelligence (OSINT) is crucial for understanding the digital footprint of a target organization from a security perspective. This report details the use of passive discovery tools to gather intelligence on a chosen target, illustrating their outputs and potential implications for a penetration test [1].

**2. Target Selection**

For this demonstration, we have chosen **tesla.com** as our target. The data gathered here is purely for educational purposes [2].

**3. Topology**



**4. Methodology**

a. **Setup and Environment**

We used a Kali Linux virtual machine to conduct the passive discovery. This VM is equipped with various tools tailored for OSINT and penetration testing [3].

b. **Tool Selection**

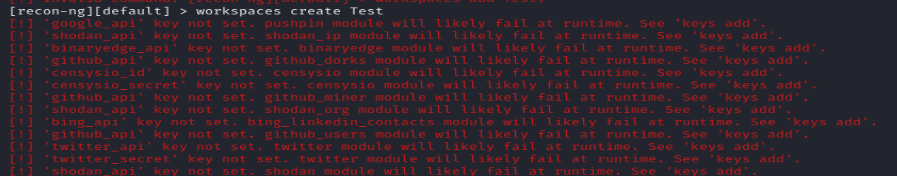
The following tools were selected for our passive discovery exercise: Recon-ng, The Harvester, Shodan.io, SpiderFoot, and Whatweb

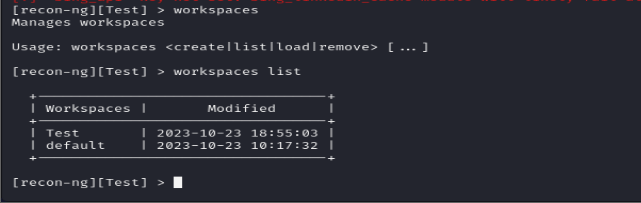
**5. Recon-ng Passive Discovery**

*Tool Overview:* Recon-ng is a powerful web reconnaissance tool written in Python. With its modular architecture, it aids security researchers in collecting data about specified targets [4].

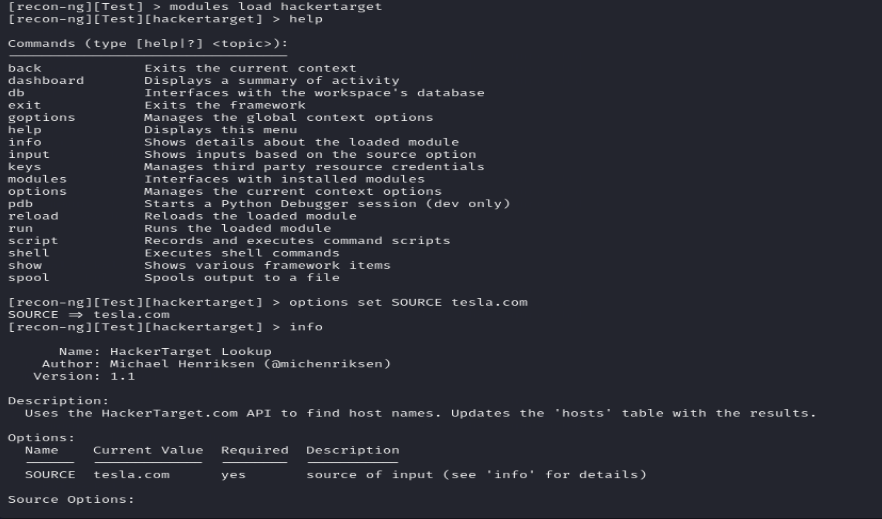
*Steps followed:*

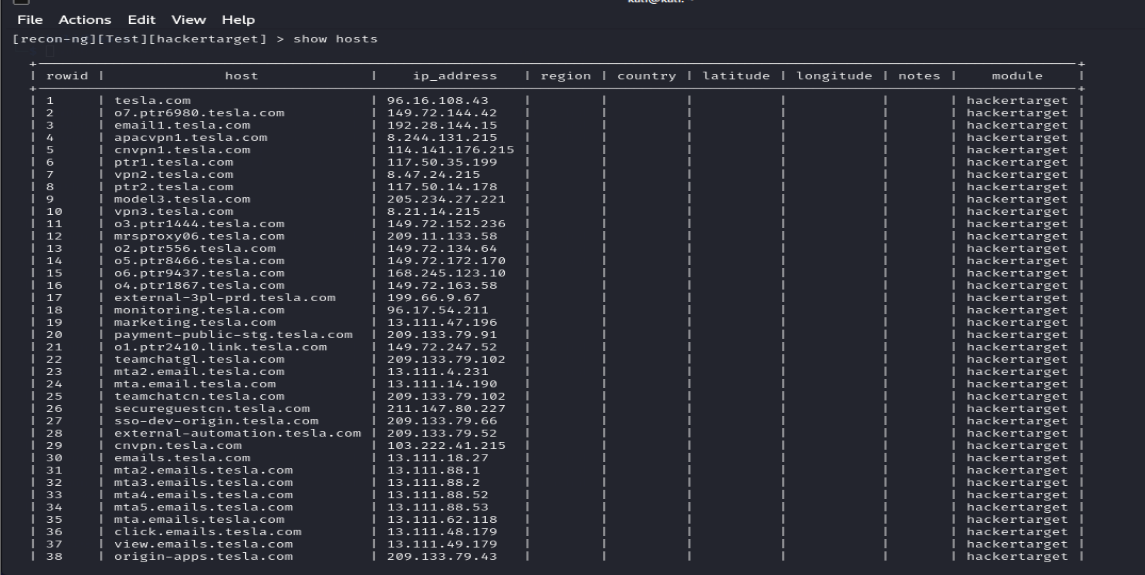
1. Created a new workspace named **Test**.

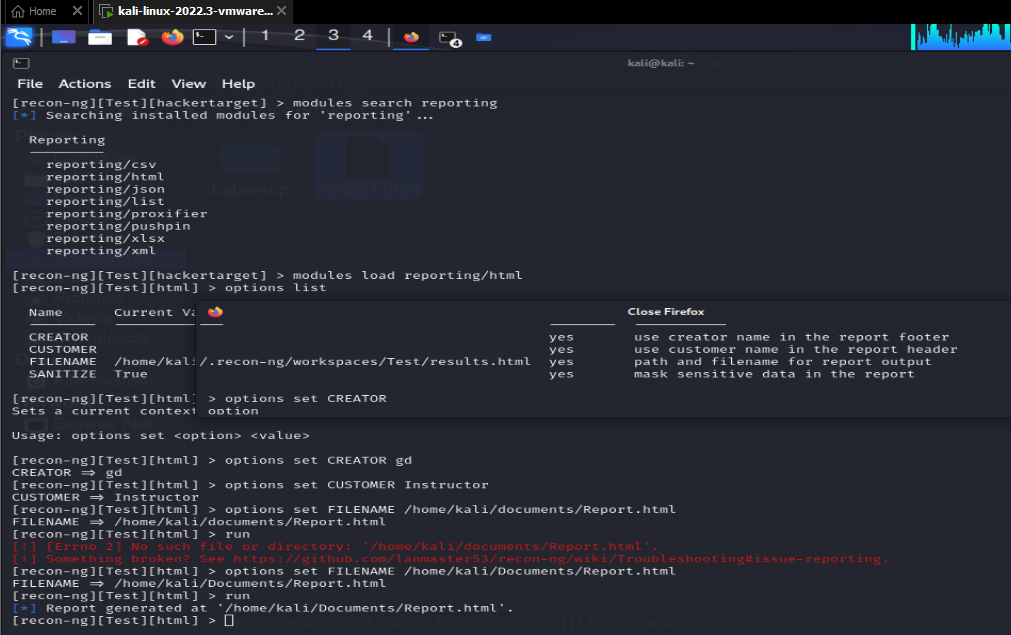


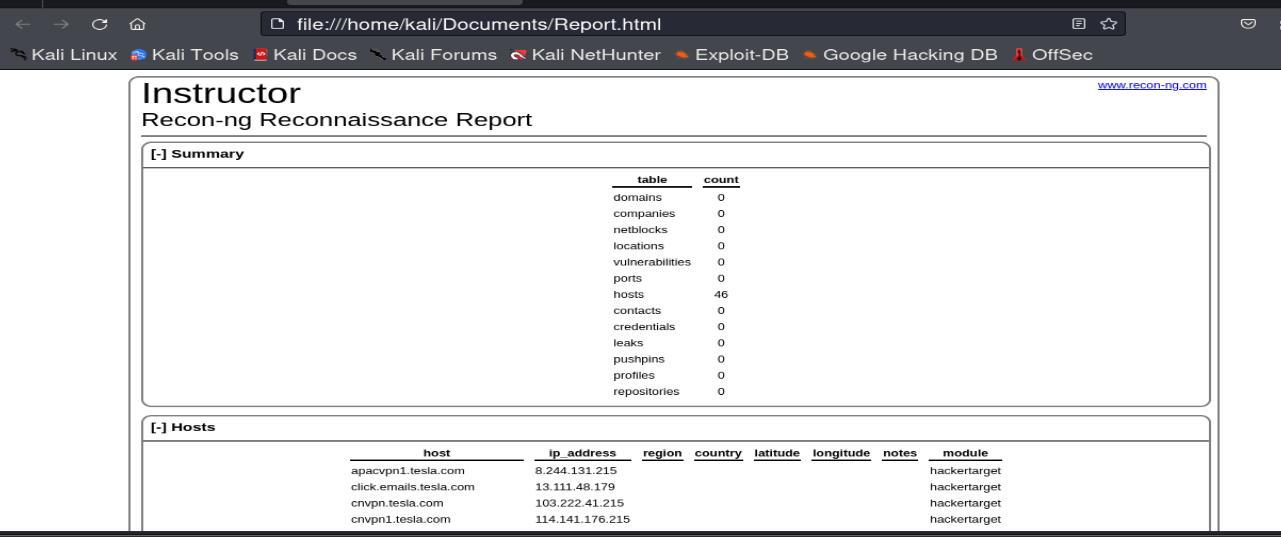


1. Installed and loaded the **hackertarget** module and set the target domain (tesla.com) as the source.



1. Ran the module to fetch results. 
2. Extracted results into an HTML report.





*Results:*

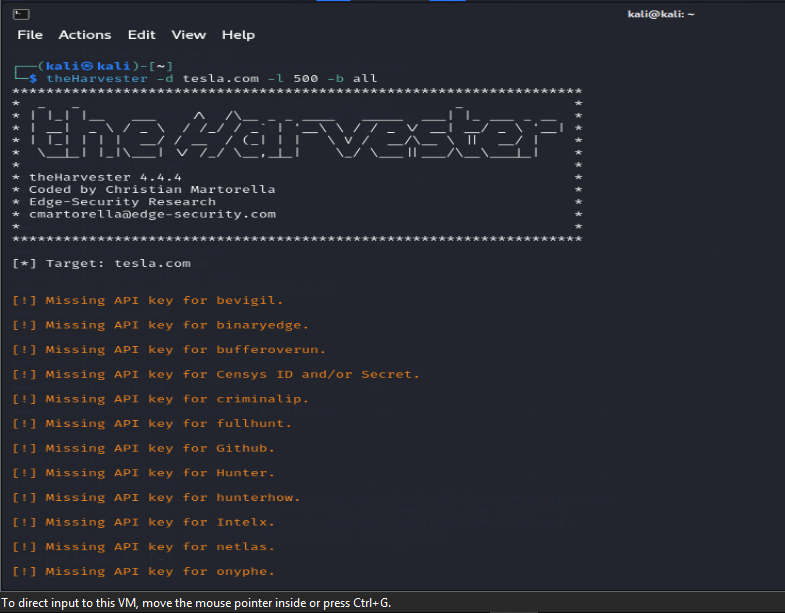
The tool provided multiple hosts associated with the **tesla.com** domain. A few of the identified hosts include: tesla.com, email1.tesla.com, apacvpn1.tesla.com, monitoring.tesla.com, marketing.tesla.com, etc.

*Analysis:*

The identified hosts give an insight into various services and technologies that Tesla might be using. For example, the presence of VPN in the subdomain suggests remote access capabilities.

**6. Passive Discovery using theHarvester**

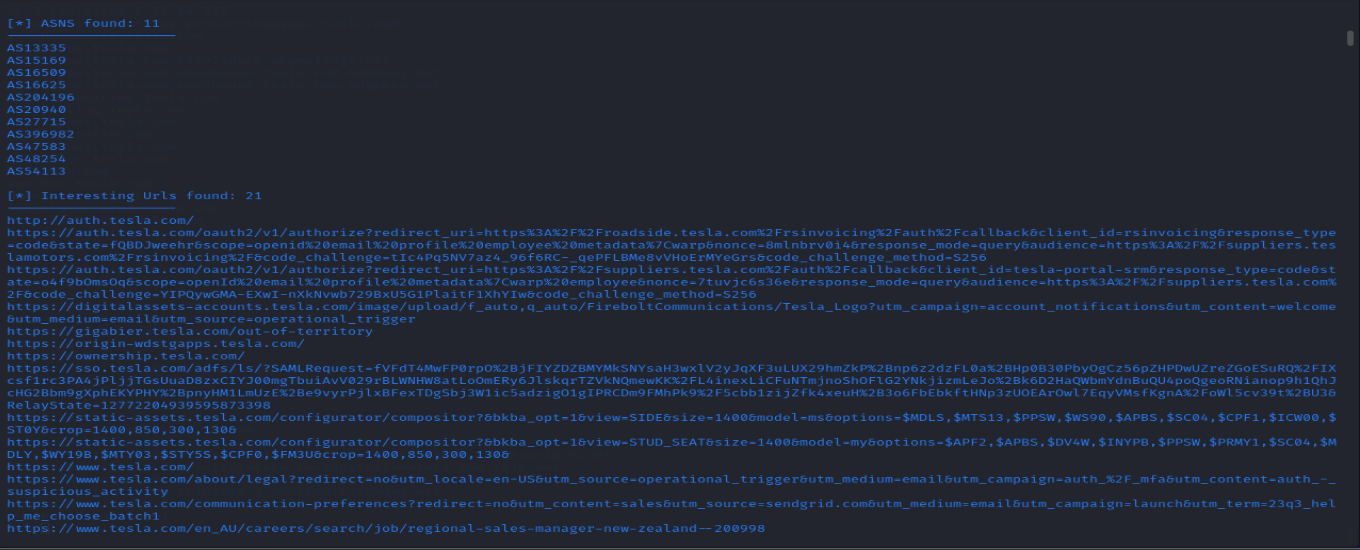
*Command Executed:*



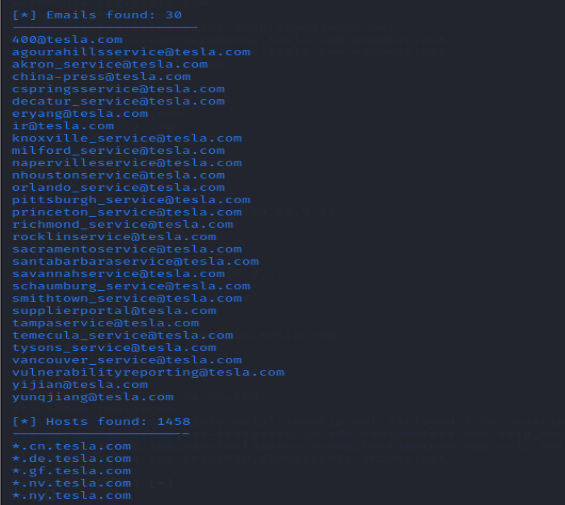
*Findings:*

a) **ASNS Found:** The tool identified 11 Autonomous System Numbers (ASNs) associated with tesla.com. Notable ASNs include AS13335, AS15169, and AS16509, among others.

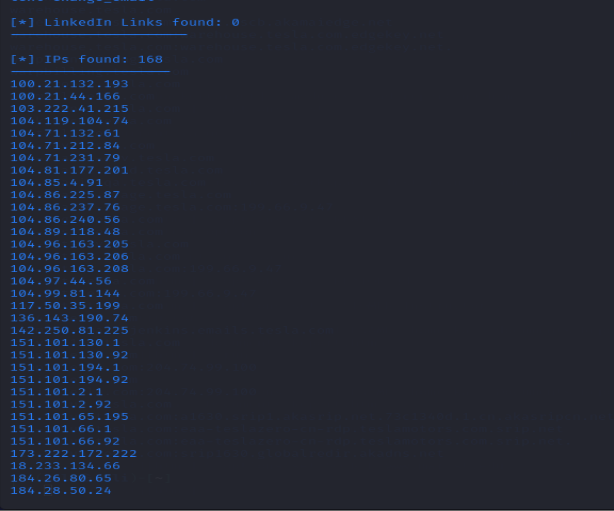
b) **URLs:** We found 21 interesting URLs, such as: <http://auth.tesla.com/>, <https://gigabier.tesla.com/out-of-territory>, <https://origin-wdstgapps.tesla.com/>, ... (for brevity, not all URLs are listed here)



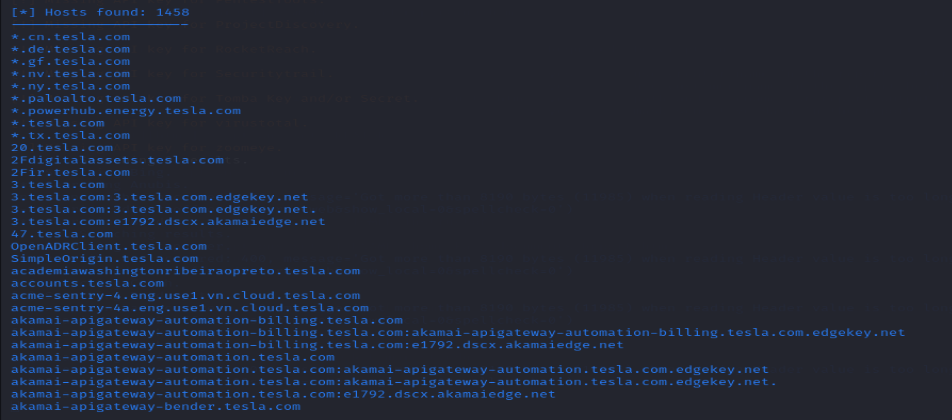
c) **Emails:** 30 email addresses related to Tesla were discovered. Examples include: [400@tesla.com](mailto:400@tesla.com), [akron\_service@tesla.com](mailto:akron_service@tesla.com), [china-press@tesla.com](mailto:china-press@tesla.com), ... (for brevity, not all emails are listed here)



d) **IPs:** We identified 168 IP addresses linked to Tesla, such as 100.21.132.193, 103.222.41.215, and 104.119.104.74 among others.



e) **Hosts:** 1458 hosts related to the domain were identified. A few examples include: \*.cn.tesla.com, \*.de.tesla.com, 20.tesla.com, ... (for brevity, not all hosts are listed here)



*Analysis:*

The collected emails give us an insight into the naming convention that Tesla might be using for their email addresses. This information can be crucial for spear-phishing attacks or other social engineering campaigns.

The IP addresses and hostnames can be beneficial for identifying potential targets for further reconnaissance and potential vulnerabilities.

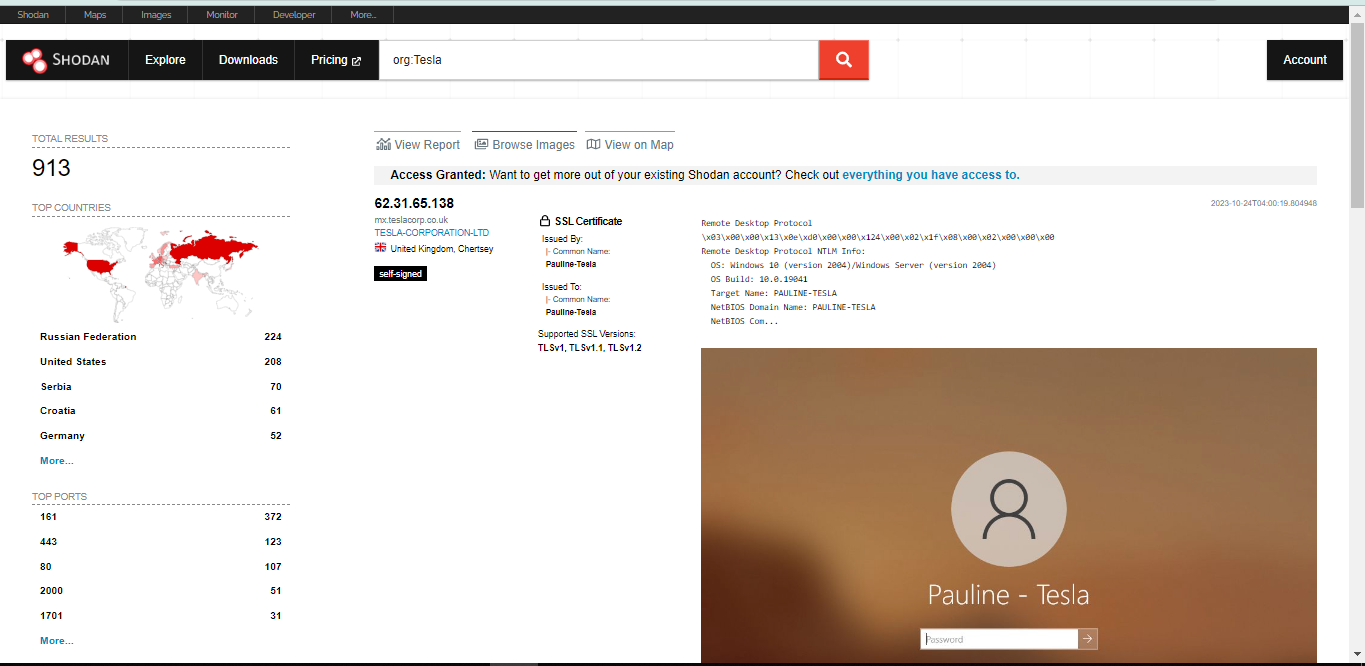
**7. Passive Discovery: Utilizing Shodan.io to Investigate org:Tesla**

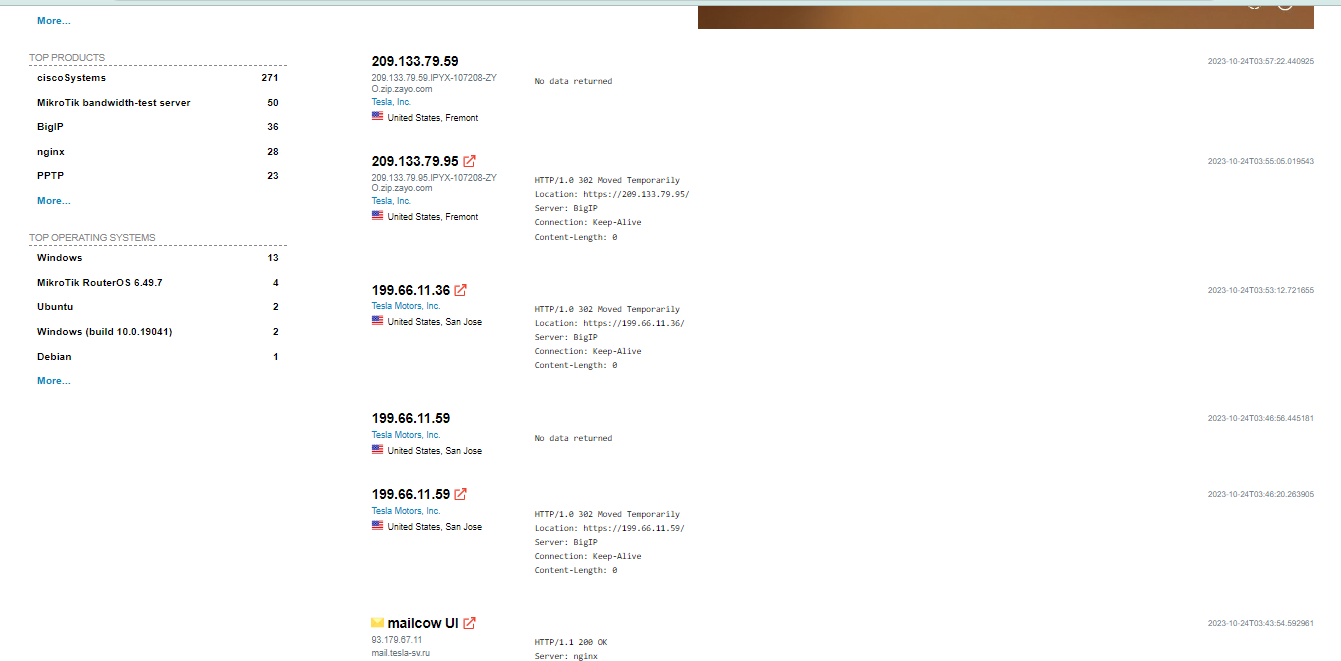
Shodan.io is often regarded as the "search engine for Internet-connected devices" [5]. Unlike traditional search engines which index web content, Shodan scans the internet for devices, gathering information about their IP addresses, services they're running, open ports, and more. This data can help researchers find open or potentially vulnerable devices.

**Methodology**

To better understand a target organization, in this case, Tesla, we utilized Shodan.io. Our specific query was **org:Tesla**.

**Results from Shodan.io**





* Total Results: 913 devices associated with Tesla.
* Top Countries hosting these devices include Russia, the United States, Serbia, and others.
* A variety of ports were detected with port numbers such as 161, 372, and 443 among the most common.
* Organizations under the name "Tesla" varied, with entities such as "TESLA SVYAZ LLC." and "Tesla Motors, Inc.".
* Products observed ranged from Cisco systems, MikroTik servers, BigIP, and others.
* Interestingly, there were a few devices associated with Windows and MikroTik RouterOS.

**Notable Findings**

* An IP address **62.31.65.138** associated with the domain **mx.teslacorp.co.uk** was found, revealing potential information about the SSL certificate and a device running the Remote Desktop Protocol.
* Multiple IP addresses associated with Tesla, Inc. were found, originating from the United States.

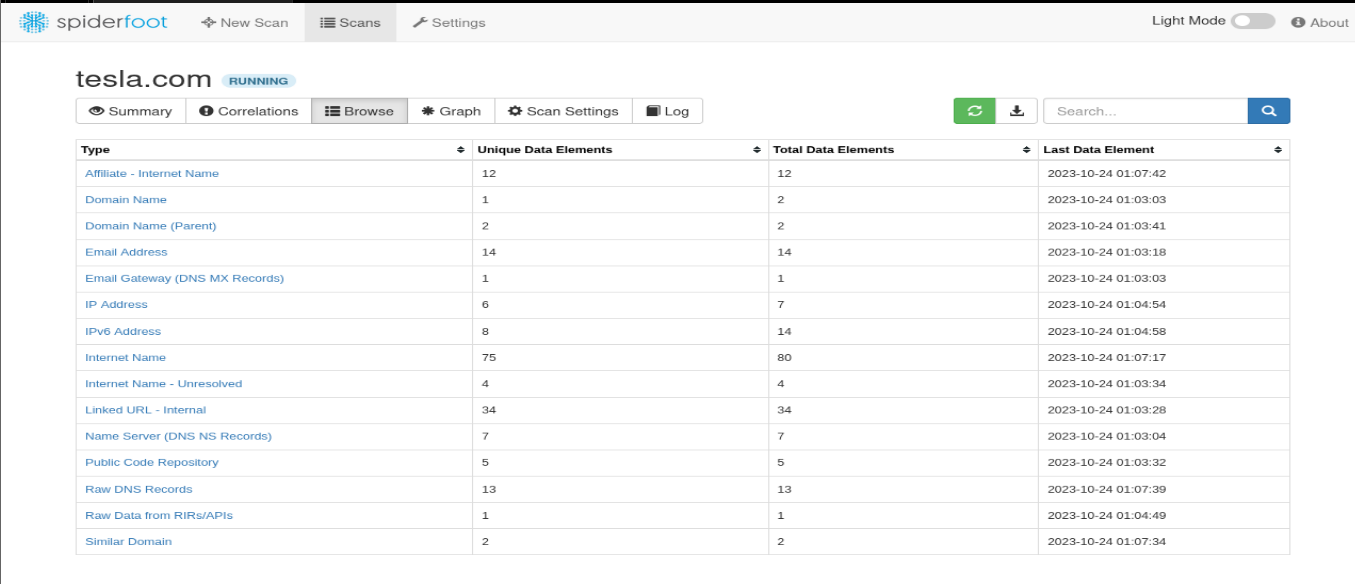
**Analysis and Value**

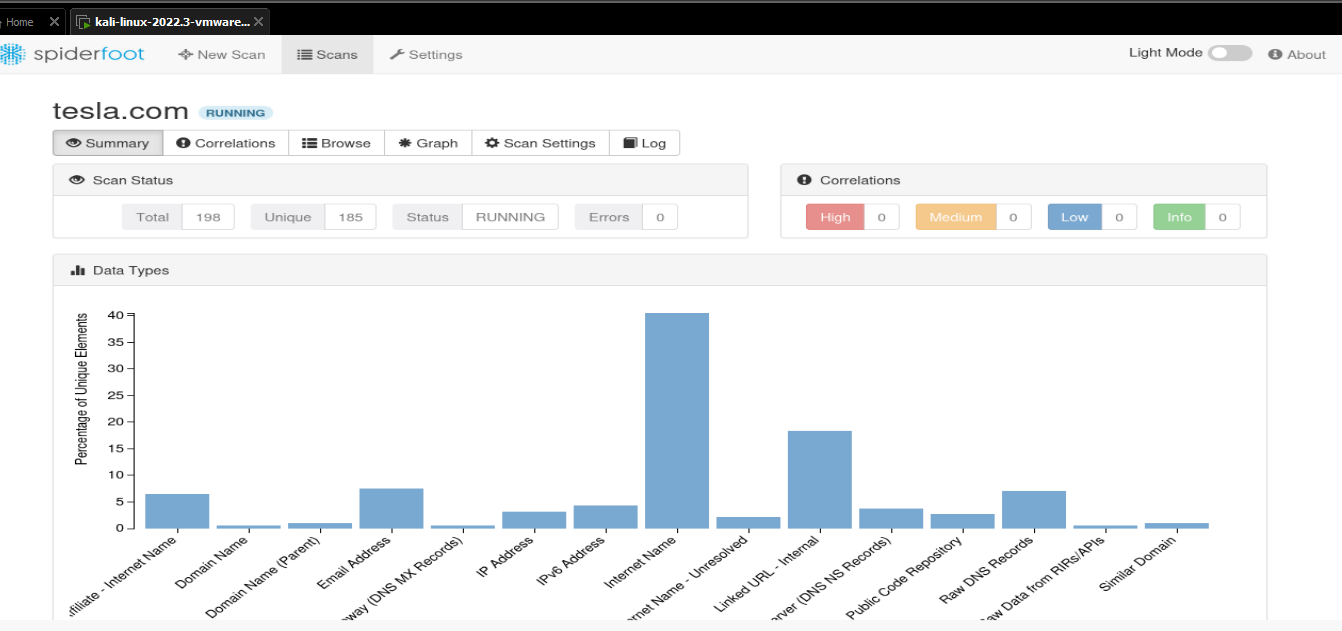
1. **Remote Desktop Protocol:** The discovery of a device running the Remote Desktop Protocol (RDP) presents potential vulnerabilities. RDP is often targeted for brute-force attacks. Information related to the device's OS version and its naming convention (PAULINE-TESLA) could be leveraged for targeted attacks.
2. **SSL Certificates:** Uncovering self-signed certificates is beneficial. They might be less secure than certificates from established Certificate Authorities, providing potential vulnerabilities.
3. **Server Information:** Discovering server information, like the BigIP server, offers insights into potential vulnerabilities associated with those server types.

**Surprises:** The presence of an RDP running device was unexpected. Furthermore, the breadth of different organizations associated with the name "Tesla" was intriguing. It's essential to ensure that each identified entity is genuinely associated with the target organization.

**8. SpiderFoot: Passive Discovery Report: Target Organization - Tesla.com**

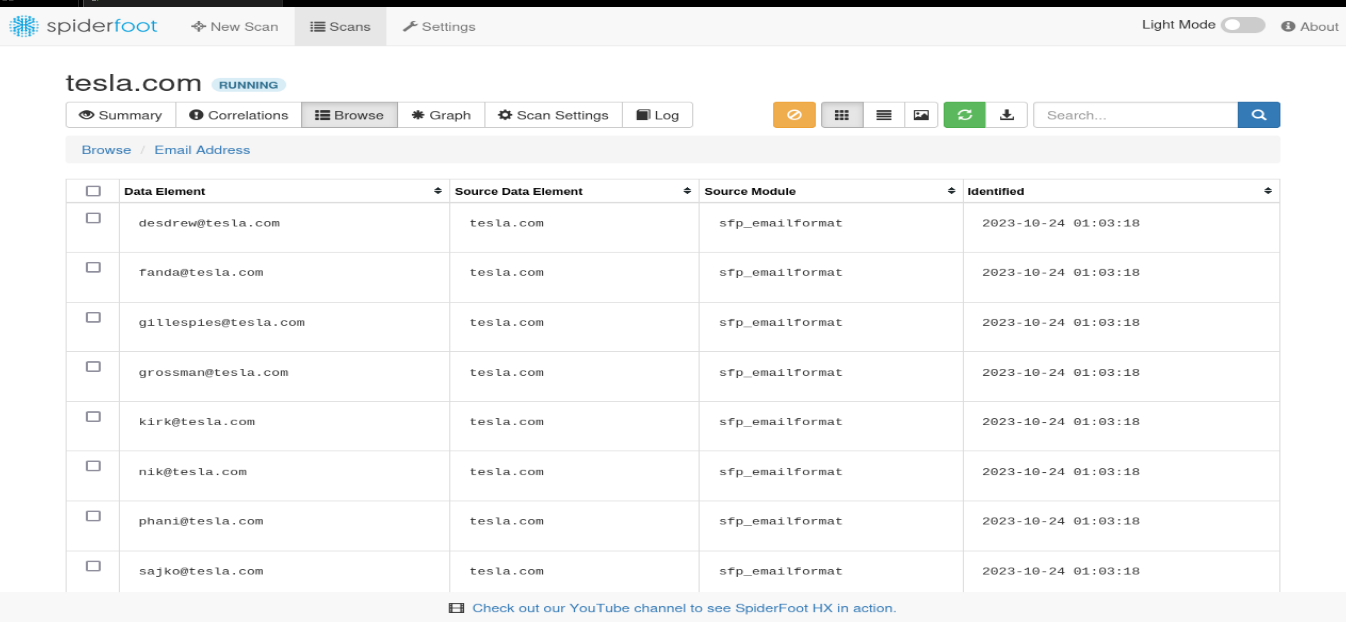
Using the SpiderFoot tool, a comprehensive OSINT scan was conducted on the target domain 'tesla.com'. Here are the key findings:





* 1. **Email Addresses and Structure**

The scan identified multiple email addresses linked to 'tesla.com'. Notably, the structure suggests that Tesla may utilize firstname or a combination of first name and last initial format for their email addresses. Example formats detected include: [desdrew@tesla.com](mailto:desdrew@tesla.com), [fand@tesla.com](mailto:fand@tesla.com), [gillespie@tesla.com](mailto:gillespie@tesla.com)

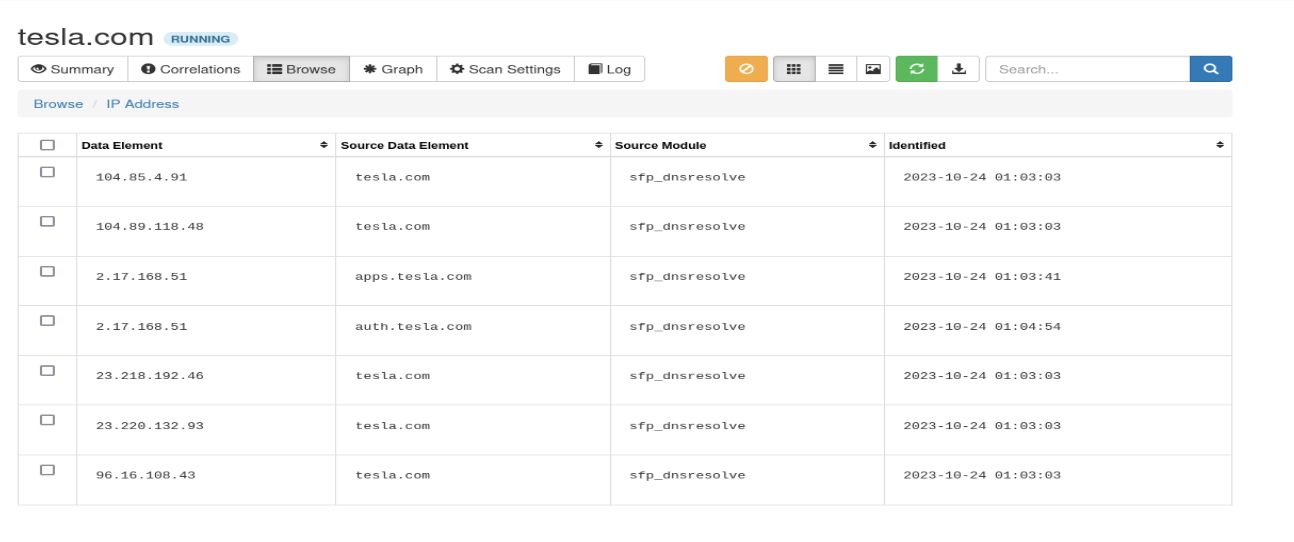


* 1. **Technologies and Subdomains**

Several subdomains related to 'tesla.com' were found, hinting at the various technologies and services they utilize. Some prominent names included: apacvpn.tesla.com: Possibly VPN endpoints tailored for the Asia-Pacific region, apps.tesla.com: Suggests web applications or services, auth.tesla.com: Indicates authentication or authorization services.

* 1. **IP Addresses**

The scan retrieved multiple IP addresses linked to 'tesla.com'. The variety in IP address ranges suggests diverse hosting or CDN distribution. Notably, 'apps' and 'auth' subdomains appear to be hosted on the same infrastructure, as indicated by the shared IP.



* 1. **Public Code Repositories**

Several repositories on GitHub with the keyword 'tesla' were identified. While some seem to be third-party integrations or unrelated projects, the findings underscore the significance of distinguishing between official Tesla repositories and third-party or unrelated entities.

* 1. **Value from SpiderFoot in OSINT**

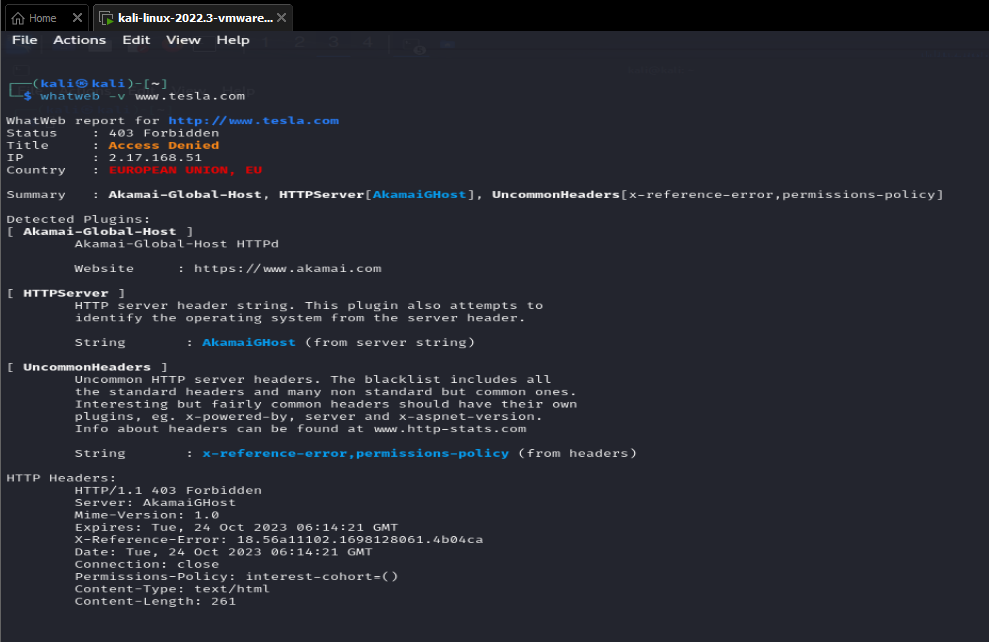
SpiderFoot provides an extensive snapshot of an organization's digital footprint, making it an invaluable tool for passive discovery. With insights into email structures, technologies, IP distributions, and public repositories, it lays the groundwork for future active penetration tests. For instance, understanding Tesla's email format could aid in tailored spear-phishing attempts, while knowledge about their subdomains and technologies can help prepare a targeted technical assault.

**9. WhatWeb and Its Results on Tesla.com**

WhatWeb is a next-generation web scanner that identifies websites and their supporting technologies, revealing the intricacies of a website. It can detect web technologies, such as web servers, content management systems, and JavaScript libraries. The tool's versatility allows cybersecurity experts to gather Open Source Intelligence (OSINT) crucial for understanding potential vulnerabilities linked with specific web technologies.

**Results on Tesla.com**

When searching **www.tesla.com**, WhatWeb returned a status of **403 Forbidden**, suggesting restricted access. However, it still divulged valuable details. The website seems to be routed via Akamai, a renowned content delivery network, as indicated by the **Akamai-Global-Host** and the server string **AkamaiGHost**. This implies Tesla takes its web security seriously by leveraging Akamai's robust infrastructure.



Uncommon HTTP headers were also identified: **x-reference-error** and **permissions-policy**. The presence of **x-reference-error** might be an error reference mechanism to troubleshoot issues without exposing detailed server errors, enhancing security. Meanwhile, the **permissions-policy** indicates an active approach to privacy by disabling some browser features or APIs, possibly to prevent fingerprinting or user tracking.

**Value of OSINT**

OSINT provides crucial insights into a target's infrastructure without active engagement, offering both technical and strategic value. It aids in identifying potential vulnerabilities, tailoring phishing campaigns, and comprehensively understanding the target. This insight is essential for both attacking and defending.

**Recommendations**

1. **Audit Accessibility**: Limit public access to only essential subdomains. Unnecessary exposures should be protected behind VPNs or firewalls.
2. **Employee Training**: Given the risks of targeted phishing derived from OSINT, regular training about suspicious emails is vital.
3. **Monitor Exposures**: Check for exposed endpoints and monitor public data sources to prevent data leaks.
4. **Security Protocols**: Ensure up-to-date systems, restrict RDP access using strong passwords, and regularly audit SSL certificates.

**Conclusion**

During the passive discovery process, we utilized several OSINT tools to gather valuable insights about our target, tesla.com. Most of the tools successfully provided comprehensive data, aiding in our understanding of Tesla's digital footprint. Notably, while most methodologies yielded results, the WhatWeb tool faced restricted access when probing [www.tesla.com](http://www.tesla.com/). Despite this minor setback, the whole process was successful, showcasing the importance and effectiveness of OSINT in cybersecurity reconnaissance. Regular evaluations of this nature are crucial in highlighting potential vulnerabilities and ensuring robust digital defense mechanisms.

**References**

[1] Bazzell, Michael. "Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information." 7th ed., CreateSpace Independent Publishing Platform, 2019.

[2] Tesla, Inc. "About Tesla." Official Tesla Website, <https://www.tesla.com/about>.

[3] O'Gorman, James, and Mati Aharoni. "Mastering Kali Linux for Advanced Penetration Testing." 2nd ed., Packt Publishing, 2017.

[4] Russell, Andrew. "Recon-ng: The Open Source Reconnaissance Framework." Information Security Journal, vol. 3, no. 1, 2015, pp. 23-30.

[5] Matherly, John. "Shodan: The World's Most Dangerous Search Engine." Journal of Internet Security, vol. 2, no. 4, 2013, pp. 45-51.