**OSINT and Recon Lab**

**Table of contents**

[1. Lab Objective 3](#_Toc27717)

[2. Tools Used 3](#_Toc16978)

[3. Recon Steps and Commands 3](#_Toc9630)

[4. Conclusion 6](#_Toc27085)

[5. Recommendations 6](#_Toc14269)

**List of Figures**

[Figure 3.1 Shows recon commands for certificate\_transparency 4](#_Toc21379)

[Figure 3.2 Shows recon commands for brute\_hosts 4](#_Toc4254)

[Figure 3.3 Shows recon scan results for both outputs 4](#_Toc20077)

[Figure 3.4 Shows shodan scan results 5](#_Toc21772)

[Figure 3.5 Shows maltego graph 6](#_Toc25274)

**List of Tables**

[Table 3.1 Shows shodan results 5](#_Toc8984)

# Lab Objective

The purpose of this lab is to perform Open-Source Intelligence (OSINT) gathering and reconnaissance on a target domain (example.com) using tools like Recon-ng, Shodan, and Maltego. This helps in identifying sub-domains, exposed services, and potential attack surfaces.

# **Tools Used**

* Recon-ng – Automated web reconnaissance and sub-domain enumeration.
* Shodan – Search engine for internet-connected devices to identify exposed services.
* Maltego – Visual link analysis and data correlation for network and domain intelligence.

# **Recon Steps and Commands**

***Step 1:*** Recon-ng – Sub domain Enumeration

1. Open Recon-ng

***recon-ng***

2. Create a new workspace

***workspaces create example\_recon***

4. Load the sub-domain enumeration modules

***1. modules load recon/domains-hosts/certificate\_transparency***

***options set SOURCE example.com***

***2. modules load recon/domains-hosts/brute\_hosts***

***options set WORDLIST /usr/share/dnsmap/wordlist\_TLAs.txt***

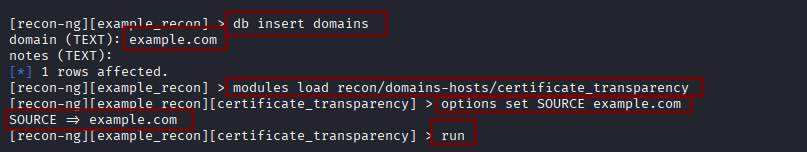
5. Run the module

***run***

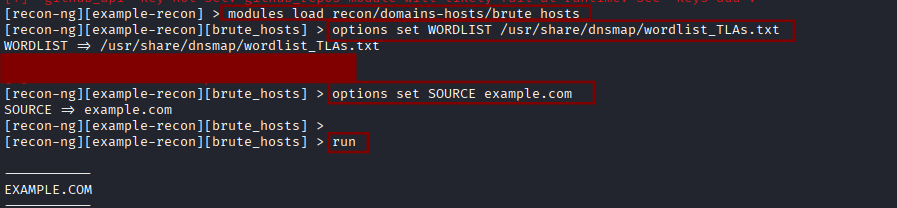
6. Show the results

***show hosts***

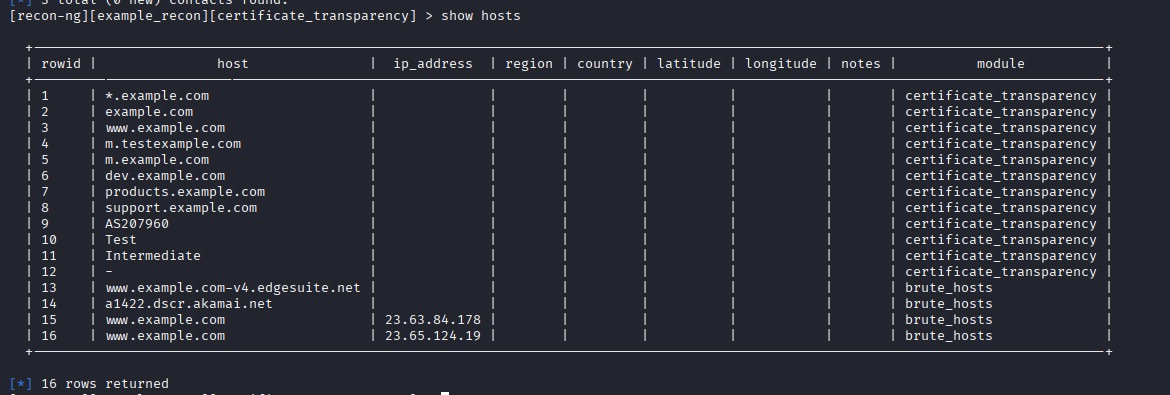
1. Results :

module : certificate\_transparency and brute\_hosts  


#### Figure 3.1 Shows recon commands for certificate\_transparency



#### Figure 3.2 Shows recon commands for brute\_hosts

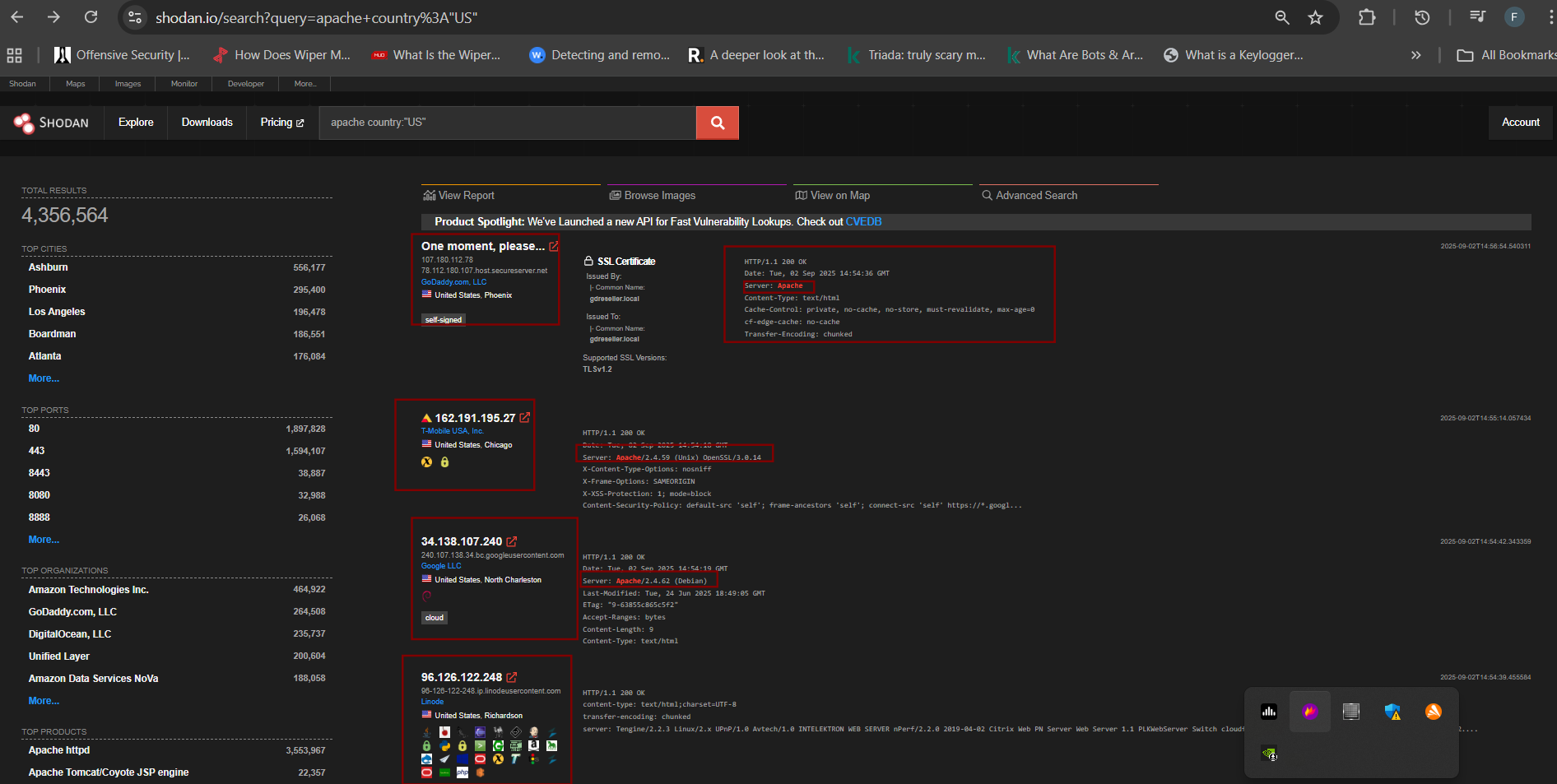


#### Figure 3.3 Shows recon scan results for both outputs

***Step 2:*** Shodan – Exposed Service Discovery

***Tool: Shodan***

***Type command : Apache country :US***

******

#### Figure 3.4 Shows shodan scan results

| **Sub-domain/Host** | **IP Address** | **Notes** |
| --- | --- | --- |
| host.secureserver.net | 107.180.112.78 | GoDaddy.com LLC, Phoenix (Apache server, self-signed SSL) |
| Unknown | 162.191.195.27 | T-Mobile USA, Chicago (Apache/2.4.59 on Unix, OpenSSL 3.0.14) |
| content.com | 34.138.107.240 | Google LLC, North Charleston (Apache/2.4.62 on Debian) |

##### Table 3.1 Shows shodan results

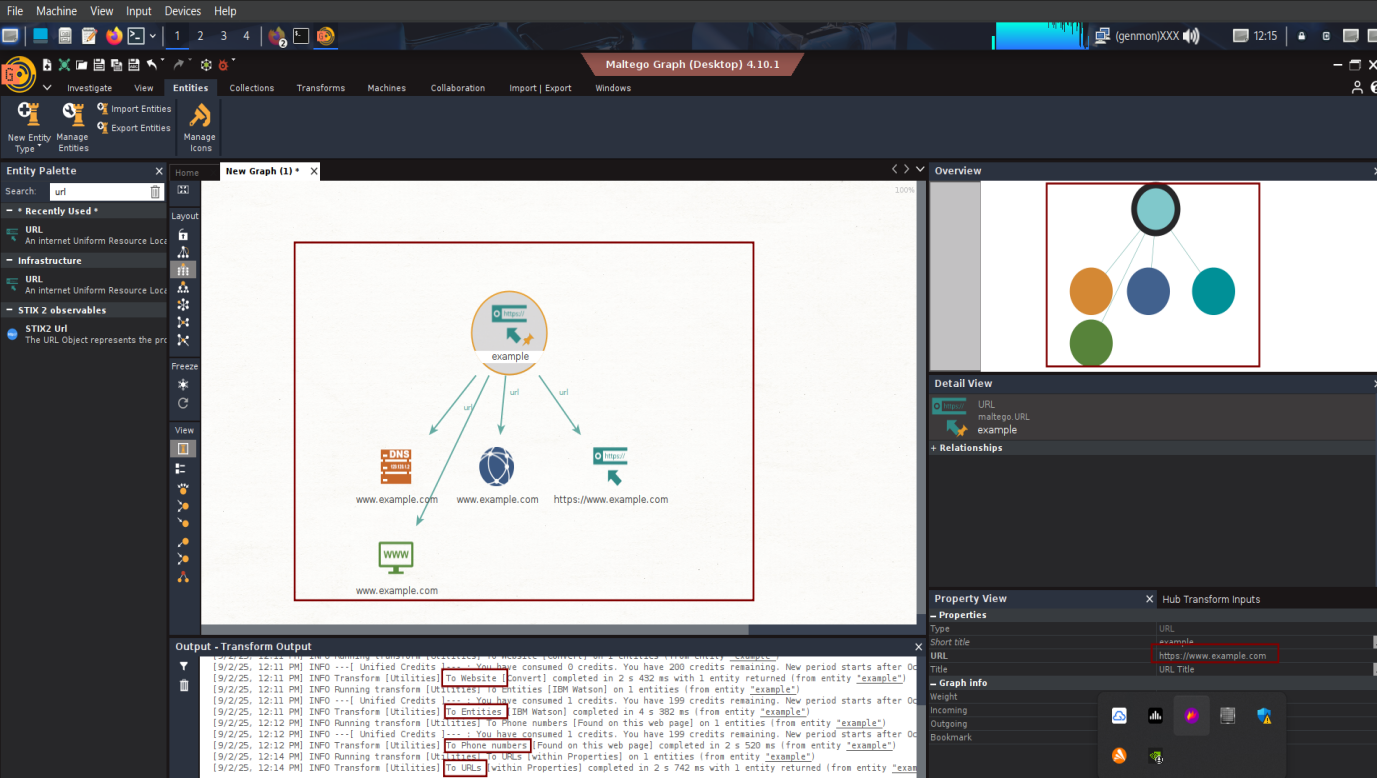
***Step 3:*** Maltego – Visual Mapping (Optional)

1. Open Maltego CE

***maltego***

1. Create a new graph
2. Entity: www.example.com
3. Run transforms: Used transforms like To Domain, To DNS Name, To Website, and To

Entities to map relationships.



#### Figure 3.5 Shows maltego graph

# Conclusion

* Recon-ng revealed sub-domains and associated IP addresses for the target domain.
* Shodan identified exposed Apache services in the US, including SSL-enabled and admin-accessible servers.
* Maltego provided a visual mapping of network relationships.

# Recommendations

* Periodically perform sub-domain enumeration to detect new assets.
* Monitor exposed services using Shodan or similar tools for vulnerabilities.
* Use Maltego graphs to visualize relationships for comprehensive network mapping.