OSINT and Recon Lab

Table of contents

List of Figures

List of Tables

1. 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.

2. 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.

3. 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

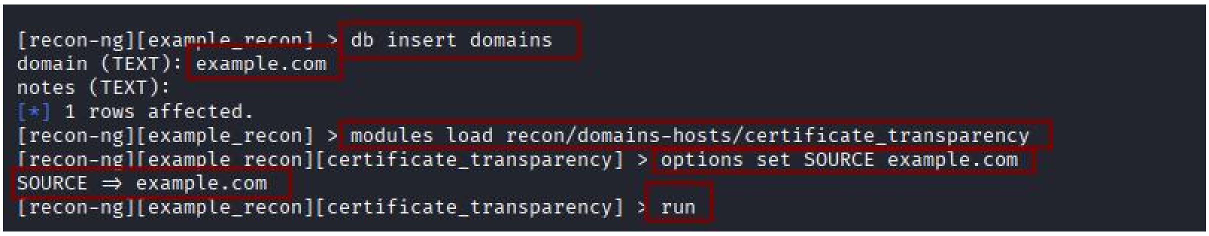
```
run
```

6. Show the results

```
show hosts
```

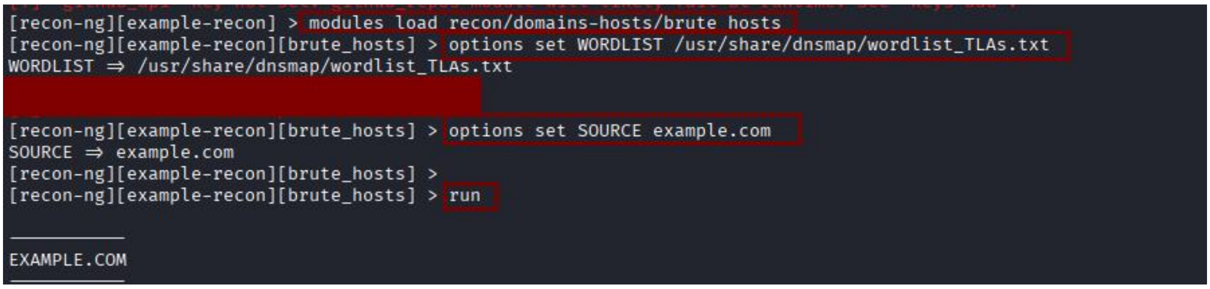
7. Results :

module : certificate_transparency and brute_hosts



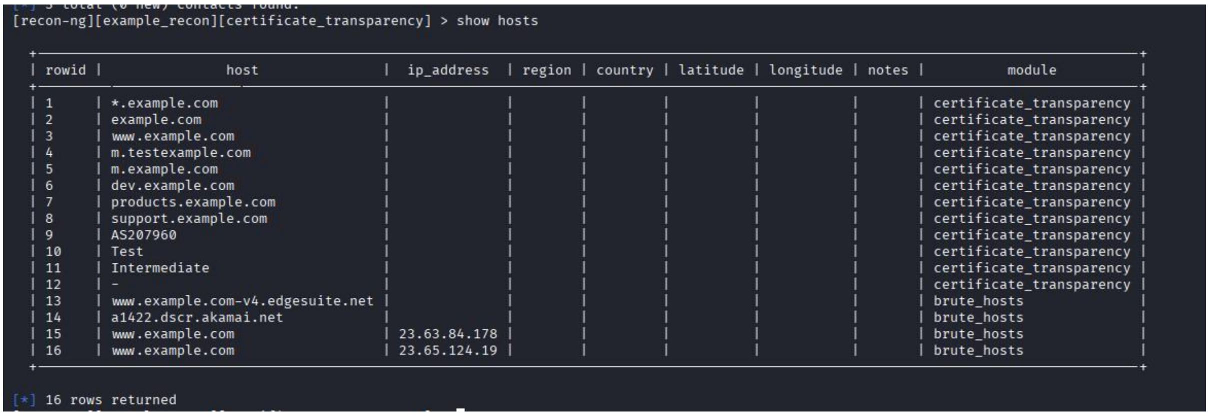
```
[recon-ng][example_recon] > db insert domains
domain (TEXT): example.com
notes (TEXT):
[*] 1 rows affected.
[recon-ng][example_recon] > modules load recon/domains-hosts/certificate_transparency
[recon-ng][example_recon][certificate_transparency] > options set SOURCE example.com
SOURCE ⇒ example.com
[recon-ng][example_recon][certificate_transparency] > run
```

Figure 3.1 Shows recon commands for certificate_transparency



```
[recon-ng][example-recon] > modules load recon/domains-hosts/brute_hosts
[recon-ng][example-recon][brute_hosts] > options set WORDLIST /usr/share/dnsmap/wordlist_TLAs.txt
WORDLIST ⇒ /usr/share/dnsmap/wordlist_TLAs.txt
[redacted]

[recon-ng][example-recon][brute_hosts] > options set SOURCE example.com
SOURCE ⇒ example.com
[recon-ng][example-recon][brute_hosts] >
[recon-ng][example-recon][brute_hosts] > run

___________
EXAMPLE.COM
___________
```

Figure 3.2 Shows recon commands for brute_hosts



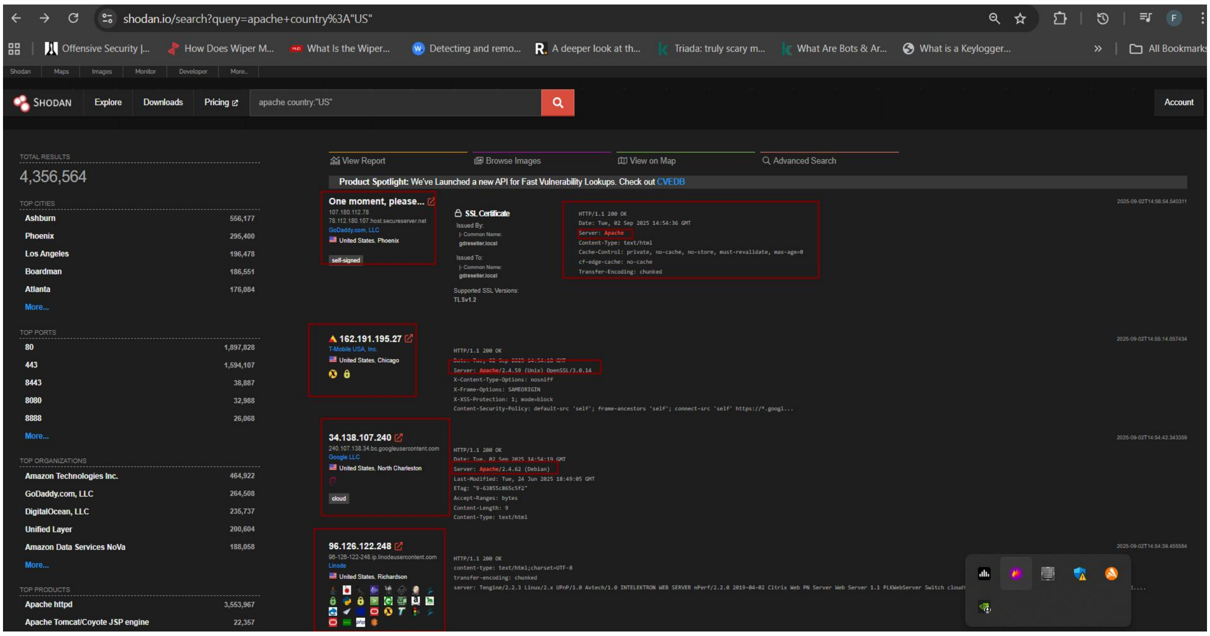
```
[*] 5 total (0 new) contacts found.
[recon-ng][example_recon][certificate_transparency] > show hosts

  +-------------------------------------------------------------------------------------------------------------------------------------+
  | rowid |                host                |  ip_address   | region | country | latitude | longitude | notes |          module          |
  +-------------------------------------------------------------------------------------------------------------------------------------+
  | 1     | *.example.com                      |               |        |         |          |           |       | certificate_transparency |
  | 2     | example.com                        |               |        |         |          |           |       | certificate_transparency |
  | 3     | www.example.com                    |               |        |         |          |           |       | certificate_transparency |
  | 4     | m.testexample.com                  |               |        |         |          |           |       | certificate_transparency |
  | 5     | m.example.com                      |               |        |         |          |           |       | certificate_transparency |
  | 6     | dev.example.com                    |               |        |         |          |           |       | certificate_transparency |
  | 7     | products.example.com               |               |        |         |          |           |       | certificate_transparency |
  | 8     | support.example.com                |               |        |         |          |           |       | certificate_transparency |
  | 9     | AS207960                           |               |        |         |          |           |       | certificate_transparency |
  | 10    | Test                               |               |        |         |          |           |       | certificate_transparency |
  | 11    | Intermediate                       |               |        |         |          |           |       | certificate_transparency |
  | 12    | -                                  |               |        |         |          |           |       | certificate_transparency |
  | 13    | www.example.com-v4.edgesuite.net   |               |        |         |          |           |       | brute_hosts              |
  | 14    | a1422.dscr.akamai.net              |               |        |         |          |           |       | brute_hosts              |
  | 15    | www.example.com                    | 23.63.84.178  |        |         |          |           |       | brute_hosts              |
  | 16    | www.example.com                    | 23.65.124.19  |        |         |          |           |       | brute_hosts              |
  +-------------------------------------------------------------------------------------------------------------------------------------+

[*] 16 rows returned
```

Figure 3.3 Shows recon scan results for both outputs

Step 2: Shodan – Exposed Service Discovery

Tool: Shodan

Type command : Apache country :US



Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out CVEDB

TOTAL RESULTS	
4,356,564	
TOP CITIES	
Ashburn	556,177
Phoenix	295,400
Los Angeles	196,478
Boardman	186,551
Atlanta	176,084
More...	
TOP PORTS	
80	1,897,828
443	1,594,107
8443	38,887
8080	32,988
8888	26,068
More...	
TOP ORGANIZATIONS	
Amazon Technologies Inc.	464,922
GoDaddy.com, LLC	264,508
DigitalOcean, LLC	235,737
Unified Layer	200,604
Amazon Data Services NoVa	188,058
More...	
TOP PRODUCTS	
Apache httpd	3,553,967
Apache Tomcat/Coyote JSP engine	22,357

One moment, please...
107.180.112.78
78.112.180.107.host.secureserver.net
GoDaddy.com, LLC
United States, Phoenix
self-signed

SSL Certificate
Issued By:
|- Common Name:
gdreseller.local
Issued To:
|- Common Name:
gdreseller.local
Supported SSL Versions:
TLSv1.2

2025-09-02T14:56:54.540311

```
HTTP/1.1 200 OK
Date: Tue, 02 Sep 2025 14:54:36 GMT
Server: Apache
Content-Type: text/html
Cache-Control: private, no-cache, no-store, must-revalidate, max-age=0
cf-edge-cache: no-cache
Transfer-Encoding: chunked
```

162.191.195.27
T-Mobile USA, Inc.
United States, Chicago

2025-09-02T14:55:14.057434

```
HTTP/1.1 200 OK
Date: Tue, 02 Sep 2025 14:54:18 GMT
Server: Apache/2.4.59 (Unix) OpenSSL/3.0.14
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Content-Security-Policy: default-src 'self'; frame-ancestors 'self'; connect-src 'self' https://*.googl...
```

34.138.107.240
240.107.138.34.bc.googleusercontent.com
Google LLC
United States, North Charleston
cloud

2025-09-02T14:54:42.343359

```
HTTP/1.1 200 OK
Date: Tue, 02 Sep 2025 14:54:19 GMT
Server: Apache/2.4.62 (Debian)
Last-Modified: Tue, 24 Jun 2025 18:49:05 GMT
ETag: "9-63855c865c5f2"
Accept-Ranges: bytes
Content-Length: 9
Content-Type: text/html
```

96.126.122.248
96-126-122-248.ip.linodeusercontent.com
Linode
United States, Richardson

2025-09-02T14:54:39.455584

```
HTTP/1.1 200 OK
content-type: text/html;charset=UTF-8
transfer-encoding: chunked
server: Tengine/2.2.3 Linux/2.x UPnP/1.0 Avtech/1.0 INTELEKTRON WEB SERVER nPerf/2.2.0 2019-04-02 Citrix Web PN Server Web Server 1.1 PLKWebServer Switch cloud
```

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)

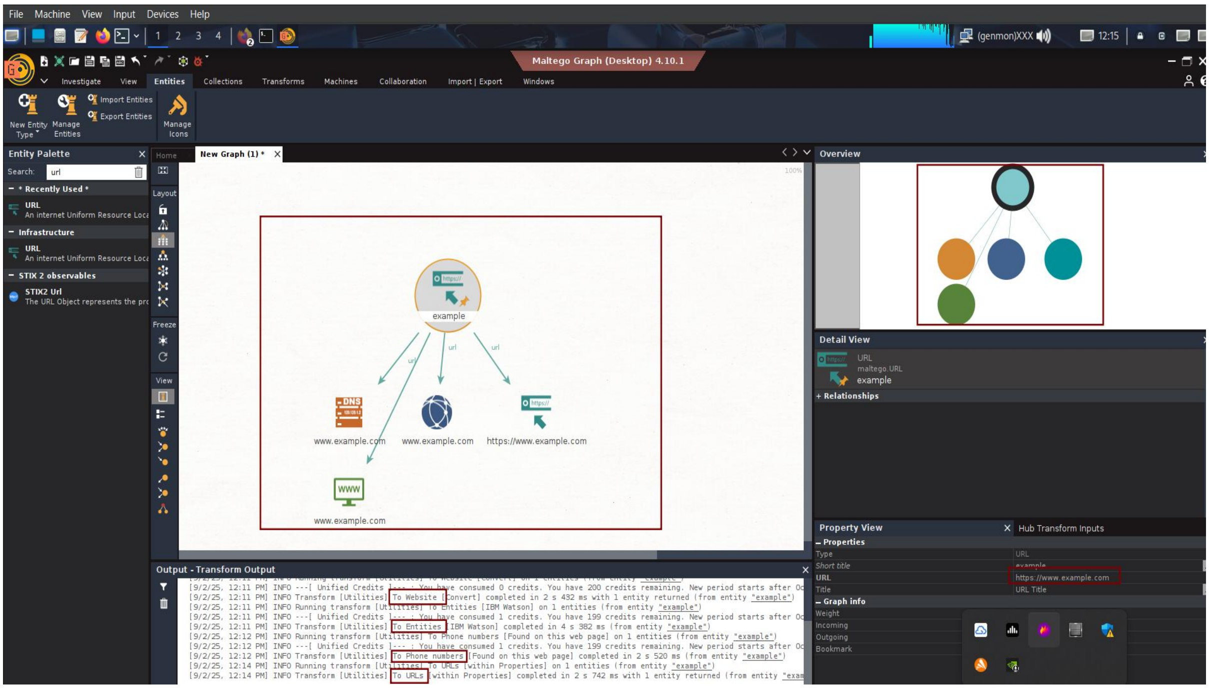
1. Open Maltego CE

maltego

2. Create a new graph

3. Entity: www.example.com

4. Run transforms: Used transforms like To Domain, To DNS Name, To Website, and To Entities to map relationships.



```
[9/2/25, 12:11 PM] INFO ---[ Unified Credits ]--- : You have consumed 0 credits. You have 200 credits remaining. New period starts after Oc
[9/2/25, 12:11 PM] INFO Transform [Utilities] To Website [Convert] completed in 2 s 432 ms with 1 entity returned (from entity "example")
[9/2/25, 12:11 PM] INFO Running transform [Utilities] To Entities [IBM Watson] on 1 entities (from entity "example")
[9/2/25, 12:11 PM] INFO ---[ Unified Credits ]--- : You have consumed 1 credits. You have 199 credits remaining. New period starts after Oc
[9/2/25, 12:11 PM] INFO Transform [Utilities] To Entities [IBM Watson] completed in 4 s 382 ms (from entity "example")
[9/2/25, 12:12 PM] INFO Running transform [Utilities] To Phone numbers [Found on this web page] on 1 entities (from entity "example")
[9/2/25, 12:12 PM] INFO ---[ Unified Credits ]--- : You have consumed 1 credits. You have 199 credits remaining. New period starts after Oc
[9/2/25, 12:12 PM] INFO Transform [Utilities] To Phone numbers [Found on this web page] completed in 2 s 520 ms (from entity "example")
[9/2/25, 12:14 PM] INFO Running transform [Utilities] To URLs [within Properties] on 1 entities (from entity "example")
[9/2/25, 12:14 PM] INFO Transform [Utilities] To URLs [within Properties] completed in 2 s 742 ms with 1 entity returned (from entity "exam
```

Figure 3.5 Shows maltego graph

4. 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.

5. 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.