ASSIGNMENT-1 SOLUTION

Q1.Run nmap with Metasploit to find target machines: Run nmap in your subnet with Metasploit environments. Use hosts and services commands. Find the ip addresses along with port addresses of the samba, smb, netbios applications.

ANSWER:-

To run Nmap with Metasploit to find target machines and identify services like **Samba**, **SMB**, or **NetBIOS**, follow these steps:



✓ 1. Start Metasploit Framework

msfconsole

2. Use Nmap inside Metasploit to Scan Your Subnet

You can run Nmap from within Metasploit or outside Metasploit.

Option 1: Run Nmap inside Metasploit

db_nmap -sS -Pn 192.168.1.0/24

- -sS: Stealth SYN scan
- -Pn: Skip ping (assume host is up)
- 192.168.1.0/24: Replace with your actual subnet

This will store results directly in Metasploit's database.

Option 2: Run Nmap in terminal (outside Metasploit)

nmap -sS -Pn -p 139,445,137,138 192.168.1.0/24 -oX smb_scan.xml Then you can import it into Metasploit:

msfconsole

db_import smb_scan.xml

✓ 3. Check Hosts Found

After the scan:

hosts

This lists all discovered IPs.

✓ 4. Check Services Detected

services

This lists open ports and services. Look for:

- Port 445 (SMB over TCP)
- Port 139 (NetBIOS Session Service)
- Port 137 (NetBIOS Name Service)
- Port 138 (NetBIOS Datagram Service)

Q Look for SMB/Samba/NetBIOS

You might see output like this:

Host Port Protocol Service

192.168.1.5 445 tcp smb

192.168.1.8 139 tcp netbios-ssn

192.168.1.8 137 udp netbios-ns

Let me know if you want to go further—like checking vulnerabilities or using an auxiliary scanner for SMB!

Q2. Investigate with a domain and a person name with maltego. Domain Investigation: 1)Use Maltego CE to investigate "example.com". 2)Identify associated subdomains, email addresses, and related IPs. 3)Summarize your findings and create a report.

ANSWER:-

Alright! Here's a step-by-step walkthrough on how to investigate a domain and a person using Maltego CE, and how to gather intel like subdomains, emails, and IPs. Then I'll show you how to summarize it all into a clean report.



✓ 1. Launch Maltego CE

- Open Maltego CE.
- Choose "Maltego CE" graph type when prompted.
- Start with a new blank graph.

2. Investigate the Domain (example.com)

A. Add a Domain Entity

- On the left sidebar, search for "Domain".
- Drag it onto the canvas.
- Double-click and change the name to: example.com

B. Run Transforms on the Domain

Right-click on the domain \rightarrow Run these **transforms**:

- To IP Address
- To DNS Name (A Records, MX Records)

- To WHOIS Info
- To Email Addresses (if available)
- To Websites (Associated URLs)

You'll now see branches of entities connecting to:

- Subdomains
- IP addresses
- Emails
- WHOIS ownership info

✓ 3. Optional: Person Name Investigation

If you have a person's name (e.g., "John Doe"):

- Drag the **Person** entity to the canvas.
- Enter the name (e.g., "John Doe").
- Right-click → Run transforms like:
 - To Email addresses
 - To Social Networks
 - To Phone Numbers
 - o To Domains

This helps if you're trying to see a person's connection to a domain or online presence.

✓ 4. Organize and Analyze

- Use Layout Tools to organize your graph for clarity.
- Label important findings (right-click on entities \rightarrow Set Label).
- Export the graph if needed (File > Export > Graph Image/PDF).

✓ 5. Summarize Your Findings – Report Template

Here's a simple report format you can use:

Maltego Domain Investigation Report

Target Domain: example.com

Date of Investigation: [Insert Date]

☐ Findings:

1. Subdomains Identified:

- sub1.example.com
- mail.example.com
- ftp.example.com

2. Associated Email Addresses:

- <u>admin@example.com</u>
- <u>info@example.com</u>

3. Associated IP Addresses:

- 93.184.216.34 (A record)
- 192.0.2.1 (MX record)

4. WHOIS Info:

• Registrant: Example Corp.

• Country: United States

• Registrar: IANA-Reserved

5. Additional Notes:

- Hosting appears to be on AWS.
- No public social media links or data breaches found.

Attachments:

• Maltego Graph Screenshot

• Exported .mtgx (Maltego case file)

Let me know if you want a real example with a real (non-placeholder) domain, or if you want to generate a PDF report together!

Q3. Name Investigation: 1)Use Maltego CE to investigate "Elon Musk".

2)Identify related social media accounts, companies, and email addresses.

3)Summarize your findings and create a report

ANSWER:-

Perfect, here's how you'd go about investigating "Elon Musk" using Maltego CE, and then how to summarize the findings in a clean report format.

⚠ Note: Since Maltego CE has limitations on transforms (especially for personal data due to privacy reasons), some results may be limited. However, we can still gather useful public data via **Person**, **Social**, and **Company** transforms.



✓ 1. Launch Maltego CE and Create a New Graph

- Open Maltego CE
- Create a new blank graph
- From the left sidebar, drag and drop a **Person** entity

✓ 2. Set the Target Name

- Double-click the Person entity and change the name to:
- Elon Musk

✓ 3. Run Transforms on the Person

Right-click on the Person entity → Run these transforms (from Maltego Standard, Social Links, or any installed Hub transforms):

Transforms to Run:

- To Social Media Accounts
- To Email Addresses
- To Phone Numbers
- To Domains/URLs
- To Companies/Organizations
- To Location (if possible)

✓ 4. Analyze the Graph

You should see entities linked to:

- Social media accounts (like Twitter, LinkedIn, etc.)
- Companies (Tesla, SpaceX, etc.)
- Possibly websites and domains
- No personal email addresses due to privacy, but may find public work emails or contact forms

✓ 5. Summarize Findings into a Report

Maltego Person Investigation Report

Target Name: Elon Musk

Date of Investigation: [Insert Date]

☐ Findings:

1. Social Media Accounts (Public):

- <u>Twitter/X</u>
- <u>Instagram</u> (fan/parody)

• <u>LinkedIn</u> (likely unofficial)

2. Related Companies/Organizations:

- Tesla Inc. CEO
- **SpaceX** Founder & CEO
- Neuralink
- The Boring Company
- X.AI
- **OpenAI** Co-founder (no longer active)
- X Corp. Umbrella company for Twitter

3. Public Email Addresses / Contact Pages:

- <u>press@tesla.com</u> (Tesla press contact)
- <u>media@spacex.com</u> (SpaceX media)
- No personal email found (Maltego CE blocks personal PII)

4. Associated Domains/URLs:

- https://www.tesla.com
- https://www.spacex.com
- https://www.neuralink.com
- https://x.ai
- https://twitter.com/elonmusk

5. Notable Mentions / Entities:

- Appears in news, Wikipedia, and corporate press pages
- Public ownership of Twitter (now X)

Attachments:

- Maltego Graph Screenshot
- Exported .mtgx case file
- CSV Export of Entities (if needed)

Want help creating a PDF version of the report or an image of a Maltego-style graph? I can mock that up for you too!