TRAINING DAY 18 REPORT:

- ## Traceroute Analysis

  Traceroute is a command-line network diagnostic tool used to track the path that packets take from a source computer to a destination host across the internet.

  ### How It Works:

  It sends packets with increasing Time-To-Live (TTL) values. Each router that handles the packet decrements the TTL, and when TTL reaches 0, the router replies with a "Time Exceeded" message.

  ### Purpose:

  - Identify path of data
  - Find latency or packet loss at each hop
  - Troubleshoot routing loops or failures

Example Command:

```
traceroute example.com      # Linux/macOS
tracert example.com         # Windows
```

Used In:

1. Network troubleshooting
2. Footprinting to identify intermediate routers
3. Understanding infrastructure between attacker and target

- ## Introduction to Maltego

  Maltego is an open-source intelligence (OSINT) and graphical link analysis tool. It is used in cybersecurity and forensics to map the relationships between people, groups, websites, domains, IPs, and more.

  Made By: Paterva (South Africa)

Interface: Drag-and-drop graph system with nodes (entities) and links (relationships)

- ## Features of Maltego :

1. **Graph-Based Interface**:

   Visualizes entities like domains, IPs, emails, organizations, etc.

2. **Transforms**:

   Automated queries to gather OSINT data from many public databases.

3. **Custom Entities and Transforms**:

   Users can add their own data sources and transforms.

4. **Data Correlation**:

   Automatically connects related data points.

5. **Integration**:

   Works with external tools like Shodan, HaveIBeenPwned, etc.

Transform Example: Convert a domain name to DNS records, then to IP, then find location, owners, etc.

Information Gathering Using Maltego

Maltego can perform:

1. Passive Reconnaissance (without alerting target)
2. Mapping out:
   - Domain Names
   - IP Addresses
   - Nameservers, MX Records
   - Email addresses
   - Organizations and Social Media links

For example: From a single domain like `example.com`, Maltego can discover associated emails, phone numbers, IPs, servers, and related websites.

- ## Maltego – Using the Tool Efficiently

  Tips for effective Maltego usage:

1. **Use Case Planning** – Know your objective (e.g., track phishing, find breach source, etc.)
2. **Use proper transform sets** – Limit noise by choosing relevant transforms
3. **Entity Management** – Rename, tag, and organize entities for clarity
4. **Combine Entities** – Merge graphs to correlate different data points
5. **Export Reports** – Graphs and relationships can be exported for reporting or presentation

- ## Maltego Transform Hub

  The **Transform Hub** in **Maltego** is a built-in marketplace that provides **ready-to-use data sources** called **transforms**. These transforms are small programs that **automatically gather related data** from the internet and add it to your Maltego graph.

  ### What Are Transforms?

  - A **transform** takes one data point (like a domain name) and finds related ones (like IPs, emails, or DNS).

  Example: You right-click a domain → select a transform → it fetches subdomains or WHOIS info.

  ### What You Can Find in the Transform Hub?

  There are three types of transform sets:

1. **OSINT Transforms (Free)**
   Example:
   - **Shodan**: Finds devices and open ports
   - **VirusTotal**: Checks malware

- **DNSDumpster**: Finds subdomains

2. **Commercial Transforms (Paid)**
   Example:
   - **DomainTools**, **Recorded Future** – provide deep threat intelligence
   - Require API keys or subscriptions
3. **Custom/Internal Transforms**
   - Made by organizations for their private use
   - Useful in enterprise or red-team operations

Why It's Useful

- Saves time – no need to manually search

- Access multiple tools from one place

- Great for **OSINT**, **cyber investigations**, **ethical hacking**

• How to Create Shodan Account

1. Go to shodan.io
2. Click **Sign Up**
3. Enter your email, create a username & password
4. Verify via email
5. Once signed in, you'll get **limited free credits**
6. You can upgrade to **Shodan Membership** to unlock more powerful features like advanced search and filters

• Maltego Integration with Shodan

- Shodan provides transforms (data fetchers) inside Maltego

- Steps:

   1. Get your **Shodan API key** from your Shodan account
   2. Open Maltego > Go to **Transform Hub**

3. Search for **Shodan** and install it

4. Paste your API key when prompted

- You can now right-click entities in Maltego and run Shodan transforms to find:

5. Open ports

6. Services

7. Connected devices

8. Geo-location of IPs

- # OSINT Framework

1. OSINT = Open-Source Intelligence

2. The **OSINT Framework** is a web-based resource that categorizes tools and websites used for information gathering.

3. Website: osintframework.com

4. Organized by:

- People (usernames, emails)
- Infrastructure (domains, IPs)
- Social networks
- Dark web, and more

5. It links you to external tools and resources

6. It's not a tool by itself, but a collection of **OSINT sources**