TRAINING DAY 15 REPORT:

- ## Port Forwarding

Port Forwarding is a technique used to **allow external devices to access services on a private network** (like accessing your local web server from the internet).

When a request comes to a specific port on your router or firewall, it gets forwarded to a device on your internal network.

How Port Forwarding Works:

- Suppose a request comes to your public IP: `203.0.113.10:8080`

- Your router receives it and **forwards** it to your local machine at `192.168.1.5:80`

- So the user actually accesses your **local server**, but through the **public IP and port**

Types of Port Forwarding:

Type	Purpose	Direction	Usage Example
Local	Forward a local port to a remote server	Local → Remote	Accessing remote web server locally
Remote	Expose a local port to the outside world	Remote → Local	Letting someone access your local server
Dynamic	Uses SOCKS proxy to route traffic	Dynamic tunnels	Secure internet browsing via SSH

1. Local Port Forwarding

- You forward a local port to a **remote IP and port**

- Used to **access a remote service securely** via SSH

Example:

```
ssh -L 8080:example.com:80 user@sshserver.com
```

Now, opening `localhost:8080` in your browser will open `example.com:80`.

2. Remote Port Forwarding

- You **expose your local service** to the remote server

- Useful for **sharing local apps** over the internet

Example:

```
ssh -R 8080:localhost:80 user@remote.com
```

Now, users on `remote.com` can access your local web server at `remote.com:8080`.

3. Dynamic Port Forwarding (SOCKS Proxy)

- You set up a **SOCKS proxy server** using SSH

- Used for **secure web browsing**

Example:

```
ssh -D 1080 user@sshserver.com
```

Now, set your browser proxy to `localhost:1080` to route traffic securely via SSH.

- ## How To Use Proxy To Become Anonymous Online

Goal: Hide your identity (IP address), browse privately, bypass restrictions.

What is a Proxy?

A proxy server acts as an **intermediary** between your device and the internet. Your traffic goes **through the proxy**, and websites see the **proxy's IP**, not yours.

Ways to Use Proxies for Anonymity:

1. HTTP/S proxies: Route web traffic only.

2. SOCKS proxies: Route any type of traffic (used in apps).

3. Proxychains: Chain multiple proxies in Linux for better privacy.

4. Tor: A special kind of anonymous network with multiple layers.

Benefit: Websites can't easily track your real location or identity.

- ## How To Use Free Proxy Servers in Firefox

Setup Steps:

1. Open Firefox.
2. Go to `Settings > General > Network Settings`.
3. Click **"Settings"** under “Connection”.
4. Choose **Manual Proxy Configuration**.
5. Enter a free proxy IP and port (from sites like `free-proxy-list.net`).
6. Click OK and start browsing anonymously.

Tip: Use HTTPS proxies for better security.

- ## How To Use Free Proxy Server in Chrome – Windows OS

Chrome doesn’t have its own proxy setting. It uses **Windows system proxy**.

Setup Steps:

1. Open `Settings > Network & Internet > Proxy`.
2. Enable **"Manual proxy setup"**.
3. Add the proxy IP and port.
4. Save and open Chrome — it will now use this proxy.

Tool: You can also use extensions like **FoxyProxy** for easier proxy switching in Chrome.

- ## Proxy Chaining – Use of Proxifier

Proxy chaining means connecting through two or more proxy servers one after another.

Example:
Your PC → Proxy 1 (USA) → Proxy 2 (Germany) → Proxy 3 (Japan) → Website

This adds **layers of security and anonymity** and makes it harder to trace your original IP.

What is Proxifier?

Proxifier is a Windows software that:

- Forces **any application** to connect through a proxy (even if it doesn't support it natively).

- Allows you to **chain multiple proxies** together.

How to use Proxifier:

1. Download and install from proxifier.com.

2. Add multiple proxy servers in settings.

3. Create rules to route traffic through those proxies.

4. Launch any app — traffic goes through the chain.

Why it's useful: Adds extra layers of anonymity and bypasses geo-blocks.

- ## What is Proxy Bouncing – Proxy Switcher Tool

Proxy Bouncing means switching between proxies **automatically or manually**.

Use Case:

If one proxy fails or gets blocked, your connection **"bounces"** to the next one.

Tools:

1. Proxy Switcher: A Windows tool for managing and bouncing between multiple proxies.

2. FoxyProxy (browser): Also allows proxy rotation.

Why it’s useful:

- Prevents detection or IP blocking.

- Helps with scraping, penetration testing, or staying anonymous.

- ## How To Install VPN in Kali Linux OS

Steps :

1. Use **OpenVPN** as the VPN client.

2. Install packages via:

```
sudo apt install openvpn network-manager-openvpn network-manager-openvpn-gnome
```

3. Download `.ovpn` config files from a VPN provider.

4. Import into Network Manager (GUI) or connect via terminal:

```
sudo openvpn --config filename.ovpn
```

Use case: Browse anonymously, access region-locked content, secure data on public Wi-Fi.