Foundation of Web, Network and HTTP

Prepared By: Aatiz Ghimire, for Herald Center for AI.

Summer, 2025

1 Learning Objectives.

- Linux server configuration
- Web server deployment
- SSL/TLS fundamentals
- Network traffic analysis with Wireshark

Question 1: Install and Configure Nginx with a Self-Signed Certificate

Task:

1. Install **Nginx** in your WSL Ubuntu environment.
2. Generate a **self-signed SSL certificate** valid for 1 year.
3. Configure Nginx to:
   - Serve HTTP on port 80.
   - Redirect all HTTP requests to HTTPS.
   - Serve HTTPS on port 443 using your self-signed certificate.
4. Create a simple `index.html` page containing:
   `Hello from WSL + Nginx + HTTPS`
5. Start Nginx and verify there are no errors.
6. Open your browser and:
   - Visit `http://localhost`
   - Confirm redirection to `https://localhost`
   - Accept the security warning to view the page.

Deliverables:

- Screenshot of your browser showing the HTTPS page.
- Screenshot of `systemctl status nginx`.

Question 2: Capture and Analyze HTTP and HTTPS Traffic with Wireshark

Task:

1. Launch **Wireshark** on your machine.
2. Start capturing packets on the network interface connected to WSL (e.g., `vEthernet (WSL)` or Loopback).
3. In your browser:
   - Visit `http://localhost` and refresh twice.
   - Visit `https://localhost` and refresh twice.

4. In Wireshark, filter traffic:
    - Show only packets on port 80.
    - Show only packets on port 443.
5. Inspect a sample HTTP packet and record:
    - Request method (e.g., GET)
    - Host header
    - Response status code
6. Inspect a sample TLS handshake packet and record:
    - Server certificate information
    - Client Hello details

Deliverables:

- Screenshot of Wireshark showing HTTP traffic.
- Screenshot of Wireshark showing HTTPS traffic.
- Written notes comparing HTTP and HTTPS packet contents.

Important Note for Linux Users

Note: If you are installing Wireshark on Linux, you may need to run these additional commands to enable non-root packet capture:

```
sudo usermod -aG wireshark <your-username>
sudo chmod +x /usr/bin/dumpcap
```

After running these commands, log out and log back in to apply the group changes.

Question 3: Reflect on Encryption and Port Usage

Task:

Answer the following questions in your own words:

1. What port does HTTP typically use? What port does HTTPS use?
2. Why is HTTPS traffic not readable in Wireshark?
3. What is the purpose of the self-signed certificate you created?
4. What risks are associated with using self-signed certificates in production?
5. How could you replace the self-signed certificate with a trusted certificate in a real scenario?

Deliverables:

- A short document answering all questions.

Optional Challenge

Set up a **Cloudflare Tunnel** or **Ngrok Tunnel** to expose your Nginx server publicly and observe differences in Wireshark traffic.

Reference Link:

- DigitalOcean Tutorial: How to Install Nginx on Ubuntu 20.04
- DigitalOcean Tutorial: Self-Signed SSL Certificate for Nginx
- Wireshark Official Download Page

The - End