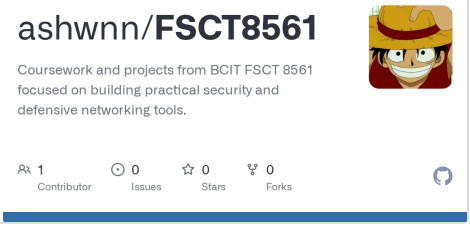
Lab4

Subjects	FSCT8561 - Security Applications
Date	@February 3, 2026

FSCT8561/Lab4 at main · ashwnn/FSCT8561

Coursework and projects from BCIT FSCT 8561 focused on building practical security and defensive networking tools. - ashwnn/FSCT8561

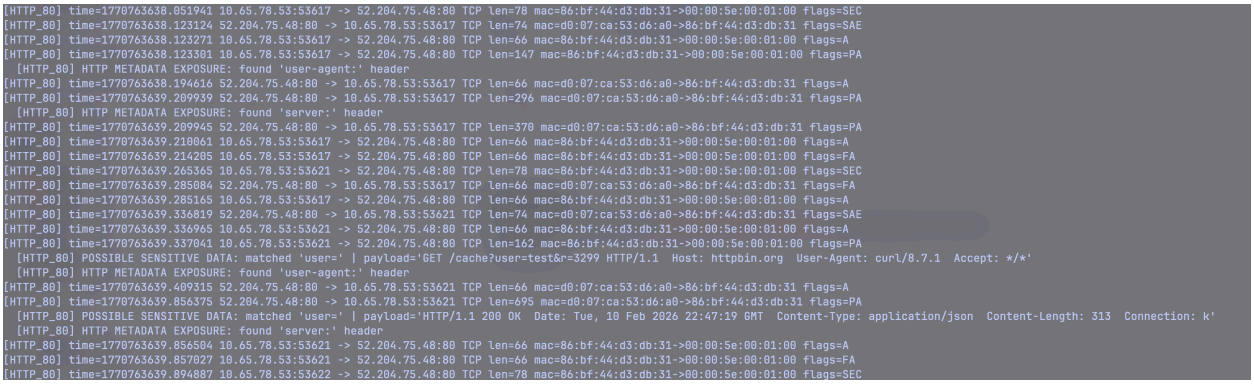
https://github.com/ashwnn/FSCT8561/tree/main/Lab4



Showcase

Traffic Sniffer

Running the python script via `sudo python Traffic_Sniffer.py` we can observe a number of things, filtering TCP, UDP and DNS (view log):



- The origin & destination of packets and the MAC Addresses are visible
- HTTP Metadata is flagged

- We can see the HTTP methods, and detailed information information for each flagged request (in this case I wrote a script to generate traffic, so thats why you see the user agent as `curl`)

Anomaly Detector

Running the script via `python Anomaly_Detector.py` we can analyze the `botnet-capture-20110812-rbot.pcap` and get the following report:

```
==================================================
Starting PCAP analysis...
Loading PCAP file: botnet-capture-20110812-rbot.pcap (~60 sec
onds)...
Loaded 495056 packets. Analyzing...
==================================================
[ALERT] Possible flooding: 147.32.84.165 sent 21 packets in 5
seconds
[ALERT] Possible flooding: 78.40.125.4 sent 21 packets in 5 s
econds
[ALERT] Possible flooding: 85.190.0.3 sent 21 packets in 5 se
conds
[ALERT] Possible flooding: 208.86.166.68 sent 21 packets in 5
seconds
[ALERT] Possible flooding: 64.31.13.148 sent 21 packets in 5
seconds
[ALERT] Possible flooding: 178.77.71.27 sent 21 packets in 5
seconds
[ALERT] Possible flooding: 109.74.55.27 sent 21 packets in 5
seconds

==================================================
Analysis complete!
==================================================
PCAP Summary
==================================================
Total TCP Packets:        474,035
```

```
Total UDP Packets:          2,386
Suspicious IPs Found:           7
================================================
```

Out of the ~128MB file we can see that a total of 7 IPs were flagged as being suspicious for sending over 20 requests within 5 seconds, all of which sent 21 packets within 5 seconds.

Reflection Questions

1. Why is packet inspection important for network security? Packet inspection is important because it shows what traffic is actually doing, can detect certain types of attacks, and leaked sensitive data.
2. What types of attacks rely on unencrypted network traffic? Attacks like credential sniffing, session hijacking via cookies, MITM rely on unencrypted traffic.
3. What are the limitations of passive packet sniffing? You cannot read encrypted payloads, only see traffic at the capture point.
4. How does encryption help prevent information leakage? Encryption makes captured data unreadable and helps prevent theft by protecting confidentiality and integrity in transit.

Security Analysis

From the traffic captures, the main takeaway is that network visibility reveals what services are in use and what data might be exposed. Even without doing anything “active,” a sniffer can identify source and destination IPs, ports, and communication patterns. When HTTP traffic is present, the biggest risk is information exposure in clear text. If usernames, passwords, session cookies, or tokens are sent over port 80, they can be captured and reused, which leads to compromise. Even when credentials are not directly visible, HTTP headers and URLs can leak sensitive context such as user identifiers, application paths, internal hostnames, and software details that can let someone fingerprint systems.

DNS queries can reveal what sites and services users access. If DNS is not protected, it can be monitored or manipulated, and abnormal query volume can

point to malware activity (for example, command and control lookups or tunneling). Generally though, high packet rates from a single source can usually indicate scanning, brute force attempts, or bot-like behaviour, which is why threshold based anomaly detection is useful as an initial indicator.

To reduce exposure, the most important mitigation is enforcing encryption for application traffic. HTTPS should always replace HTTP, and modern TLS settings should be used. For DNS, using encrypted DNS options (like DNS over HTTPS or DNS over TLS) can reduce monitoring tactics, and DNS security controls (filtering, logging, and validation) can help detect suspicious domains. Network segmentation, firewall rules, and least privilege access are the standard in limiting how much an adversarial can learn or reach if they gain a foothold.

In many environments you can only see partial traffic during a capture due to switching, encryption, or limited capture points. Large scale networks can drop packets, and capturing everything raises storage, privacy, and legal concerns. Packet inspection is powerful, but it is just the basics and works best alongside detailed logs, IDS/IPS, and centralized monitoring.