FSCT 8561 – Lab 4: Network Traffic Analysis Using Scapy

By: Jose Bangate, A01271709

Part 6 – Reflection Questions

1. Because it allows defenders to view real traffic contents and behaviour rather than just connection counts or firewall logs, packet inspection is crucial for network security.
2. Attacks that rely on unencrypted network traffic exploit the ease with which attackers with access to the same network segment can intercept, read, and alter plaintext data as it travels across a network.
3.
    a. Restricted access to encrypted traffic
    b. Limitations to local traffic
    c. Unable to find corrupted or hidden packets
4. By making data unreadable to anyone who intercepts it without the right key, encryption helps stop information from leaking.

Part 7 – Security Analysis

When packet captures are thoroughly analyzed, network traffic inspection can uncover significant security threats. The presence of sensitive information in plain text that has not been encrypted is a clear concern. All network traffic is captured by packet sniffing programs, and credentials, session tokens, and other private information can be seen directly in packet payloads when protocols such as HTTP, FTP, or Telnet are used. By capturing these data flows and making them publicly available to anybody with access to the network interface in promiscuous mode, packet sniffing allows hackers to steal data, including login credentials and personal information.

Network traffic can reveal metadata that helps attackers, even without explicit passwords. The services that are in use and possibly susceptible are identified by header information such as source/destination IPs, ports, and unprotected protocol details. Frequent connection attempts or odd port usage could be signs of pre-attack reconnaissance or scanning activity. Additionally, by recording session identifiers and repeating them, attackers can use sniffed traffic to carry out more complex attacks like man-in-the-middle or session hijacking.

Numerous threat vectors are produced by these vulnerabilities. On unprotected public networks or internal segments, passive sniffing can be used to gather private information without changing traffic. Attackers can reroute data through their systems using active sniffing techniques, such as ARP spoofing, which gives them the ability to intercept and possibly alter communications. Credential theft, illegal access, and data exfiltration are made possible by both strategies.

Traffic must be strongly encrypted in order to reduce these exposures. Plaintext interception can be avoided by using HTTPS rather than HTTP and requiring SSL/TLS for all critical communications. Additionally, data is encrypted over untrusted networks using virtual private networks (VPNs), making it unreadable even if intercepted. Potential sniffers can see less important communication when insecure protocols are used sparingly and networks are segmented. Administrators can receive real-time alerts about unusual activity through routine monitoring using intrusion detection systems that incorporate deep packet inspection (DPI).