Video: Lab4_Demo_ThomasDuong.mp4

Code: https://github.com/DThomas230/FSCT-8561_Security-Applications

Part 6 – Reflection Questions

1. Why is packet inspection important for network security?
   a. The packet inspection is very essentially the "security guard" of network. It examine the data packet sent across a network to ensure they are legitimate and safe. It is important because it help to prevent like threat detection, policy enforcement.
2. What types of attacks rely on unencrypted network traffic?
   a. There are several types of exploits through unencrypted network traffic like eavesdropping, Man-in-the Middle, Session Hijacking, Replay Attacks.
3. What are the limitations of passive packet sniffing?
   a. The limitation of the passive packet sniffing are the encryption, switched networks), no active prevention (the file is "read-only" activity), and high volume data.
4. How does encryption help prevent information leakage?
   a. There are few ways to prevent information leakage like Increase the confidentiality and data integrity by provide the encryption on the file and have the decryption key to decryt the file and to read it.

Part 7 – Security Analysis

Write 300–400 words analyzing the security implications of your observations. Include:

• Risks observed from captured traffic

The anomaly detector detected the suspicious IPs that produced traffic volume of more than 20 packets at 5-second windows, which is a sign of potential flooding attacks or botnets. The evidence of organized malicious activity can be found in the [botnet-capture-20110812-rbot.pcap] file (Lab 4/botnet-capture-20110812-rbot.pcap) as several source IPs show an abnormal distribution of traffic. The large number of TCP connections indicates the possibility of command-and-control communications or data exfiltration. Moreover, the implementation of the Traffic sniffer [Traffic sniffer.py] exposes the risk of sensitive data exposure with the help of the payload inspection as keywords such as password, login, session, etc. are found in the unencrypted traffic.

- Potential threats and vulnerabilities

The analysis reveals several threat vectors for example DoS/DDoS attacks from the detected traffic floods, botnet infections evidenced by coordinated communication patterns, and data breach risks from unencrypted sensitive information transmission. The sliding-window detection mechanism exposes reconnaissance activities where attackers probe network defenses before launching full-scale attacks. Man-in-the-middle vulnerabilities become apparent when analyzing HTTP traffic containing authentication credentials or session tokens in plaintext.

- Suggestions for mitigating exposure

Analysis shows a number of threat vectors like DoS/DDoS attacks due to the detected traffic jams, botnet infection due to coordinated communication patterns, and the danger of information leakage due to unencrypted transmission of sensitive information. The sliding-window detection system reveals reconnaissance attacks in which attackers scan network defenses prior to initiating actual attacks. Man-in-the-middle attacks are also visible in the case of plaintext analysis of HTTP traffic with authentication credentials or session tokens.

- Limitations of packet capture in real-world environments

Packet capture analysis has serious practical limitations. Encryption of traffic makes it ineffective to inspect the payload, restricting the option to study the metadata. The rapid networks produce huge amounts of data that must be analyzed selectively through selective capture strategies because they overwhelm the traditional analysis tools. Privacy laws limit the deep packet inspection facility and the administration of capture infrastructure may be heavy. Typical traffic bursts can also give false positives, leading to unnecessary alerts, and advanced attackers can use techniques of traffic obfuscation, which avoids detection. Storage capacity to perform complete packet capture is prohibitive in enterprise space, and hence intelligent policies of filtering and retention are required.