03

Detecting and Analyzing Network Attacks

Network Security Attacks: Statistics

- As of 2022, a network attack occurs every 39 seconds (University of Maryland).
- Approximately 43% of these attacks target small businesses, which often have less robust security measures (Cybercrime Magazine).
- Man-in-the-Middle Attacks: These types of attacks, potentially capturing sensitive information, represent about 35% of all network attacks (NortonLifeLock).
- It's estimated that by 2025, there will be over 75 billion IoT devices worldwide (Statista). Given the growing number of IoT devices, they have become an attractive target for network attacks. Symantec reported a 600% increase in IoT attacks in 2017.

Network Security Attacks: Statistics

- While ransomware attacks can affect individual devices, they increasingly target networks to maximize impact. According to the SonicWall Cyber Threat Report, there was a 62% increase in worldwide ransomware attacks in 2020.

- With the shift to remote work due to the COVID-19 pandemic, network attacks targeting remote workers have seen an increase. Check Point's mid-year 2020 report noted that cyberattacks on remote access networks (VPN) increased by almost 800% during the first half of 2020.

- According to a 2020 report from Absolute Software, 42% of endpoints are unprotected at any given time, making them vulnerable to network attacks.

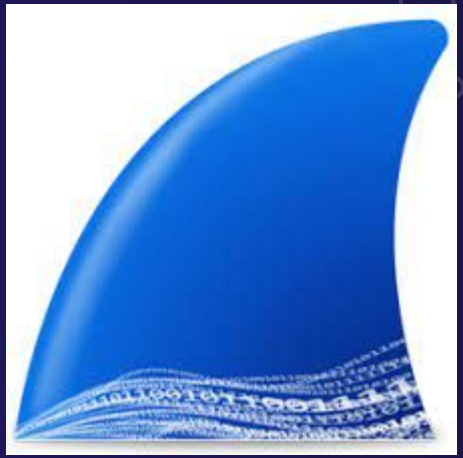
Why is Network Attack Analysis critical in Cybersecurity training?

- In depth knowledge of TTPs enables cybersecurity professionals to predict, detect, and counteract threats.
- By studying past and current attack patterns, we can anticipate future threats and vulnerabilities and develop proactive security measures and protocols.
- Familiarity with attacker behavior aids in the early detection of anomalies, reducing the likelihood of successful breaches.
- Knowledge of network attack patterns allows us to isolate the breach quickly and prevent further network compromise improving incident response and recovery time.

Using Wireshark in Network Attack Analysis

- By analyzing captured packets, you can spot unusual patterns or activities that suggest a network attack.

- Wireshark's filters can be used to narrow down the data and focus on potential issues. For example, you might filter by protocol to look for suspicious TCP or UDP activity, or by IP address to focus on activity involving a specific device.



Using Wireshark in Network Attack Analysis

- Signs of an attack may include an unusually large number of requests from a single IP address (potential DDoS attack), ARP packets where the sender and target IP addresses are the same (potential ARP spoofing), or TCP packets with the SYN flag set but no corresponding ACK (potential SYN flood).