Module 4.3: Mitigating Common Network Attacks

Endpoint Security | Cisco Networking Academy

Prepared by: Kudzaishe Majeza

Agenda

- Defending the Network
- Mitigating Malware
- Mitigating Worms
- Mitigating Reconnaissance Attacks
- Mitigating Access Attacks
- Mitigating DoS Attacks
- Summary

Defending the Network

- Defending the network means putting security controls in place **before attacks happen**. This includes firewalls, network segmentation, access control lists, and monitoring systems.
- Strong network defense limits how far attackers can move if they gain access.
- **Real-Life Incident: Target Data Breach (2013)** Attackers accessed Target's network through a third-party HVAC vendor. Poor internal segmentation allowed them to reach payment systems and steal over 40 million card records.
- **Source:** https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

Mitigating Malware

- Malware refers to malicious software such as **viruses, trojans, spyware, and ransomware**. Malware mitigation includes antivirus software, regular patching, endpoint protection, and user awareness training.
- Unpatched systems are the most common malware entry point.
- **Real-Life Incident: WannaCry Ransomware (2017)** WannaCry exploited unpatched Windows systems and spread globally, disrupting hospitals, businesses, and governments.
- **Source:** https://www.bbc.com/news/technology-39901382

Mitigating Worms

- Worms are a type of malware that **self-replicate without user interaction**.
  They spread rapidly across networks.
- Defenses include patch management, network monitoring, and traffic filtering.
- **Real-Life Incident: SQL Slammer Worm (2003)**
  The worm spread worldwide in minutes, causing internet outages and system failures.
- **Source:**
  https://www.cisa.gov/news-events/news/lessons-learned-sql-slammer-worm

Mitigating Reconnaissance Attacks

- Reconnaissance attacks involve **scanning and probing networks** to collect information before launching attacks.
- Defensive measures include intrusion detection systems, logging, and anomaly monitoring.
- **Real-Life Incident: SolarWinds Supply Chain Attack (2020)**
  Attackers silently monitored networks for months before deploying malicious updates.
- **Source:**
  https://www.cisa.gov/supply-chain-compromise

Mitigating Access Attacks

- Access attacks exploit **weak passwords or stolen credentials**.
  Defenses include strong password policies, multi-factor authentication (MFA), and least-privilege access.
- **Real-Life Incident: Colonial Pipeline Attack (2021)**
  Attackers gained access using a compromised password without MFA, causing fuel shortages across the U.S.
- **Source:**
  https://www.cisa.gov/news-events/alerts/aa21-131a

Mitigating DoS Attacks

- Denial of Service (DoS) attacks overwhelm systems with traffic, making services unavailable. When launched from many systems, they are called Distributed Denial of Service (DDoS) attacks.
- Mitigation includes rate limiting, traffic filtering, and cloud-based DDoS protection.
- **Real-Life Incident: Cloudflare DDoS Attacks (2023)** Cloudflare reported DDoS attacks exceeding 2 terabits per second, the largest ever recorded.
- **Source:** https://blog.cloudflare.com/2023-ddos-threat-report/

Summary

- Network attacks target critical systems
- Malware, worms, access attacks, and DDoS attacks are common
- Real-world incidents show severe impact
- Strong defense requires layered security, patching, and monitoring