1213سبر

Network Defense

Lecture #7 Part 1

Protecting Against Advanced Attacks

Topics

- Understanding Attack Frameworks
- Identifying Network Attacks
- Summarizing Secure Coding Concepts
- Identifying Malicious Code and Scripts
- Identifying Application Attacks

Attack Frameworks

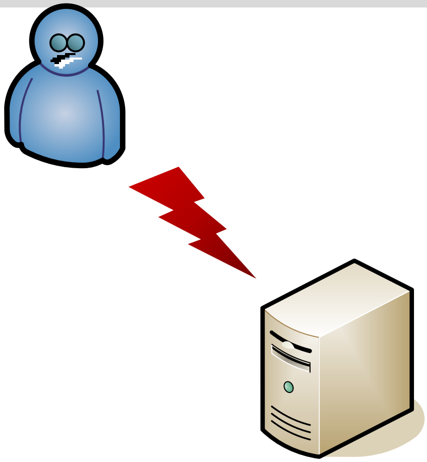
- Cyber Kill Chain
  - includes seven elements tracking an attack from reconnaissance to performing actions
    - Reconnaissance
    - Weaponization
    - Delivery
    - Exploitation
    - Installation
    - Command and Control (C2)
    - Actions on Objectives

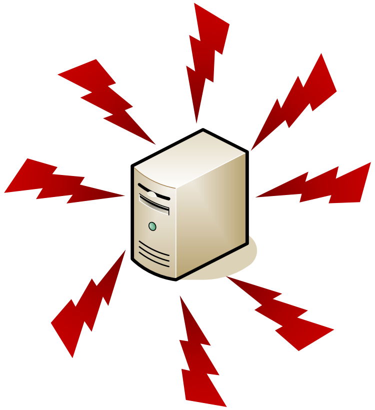
Attack Frameworks

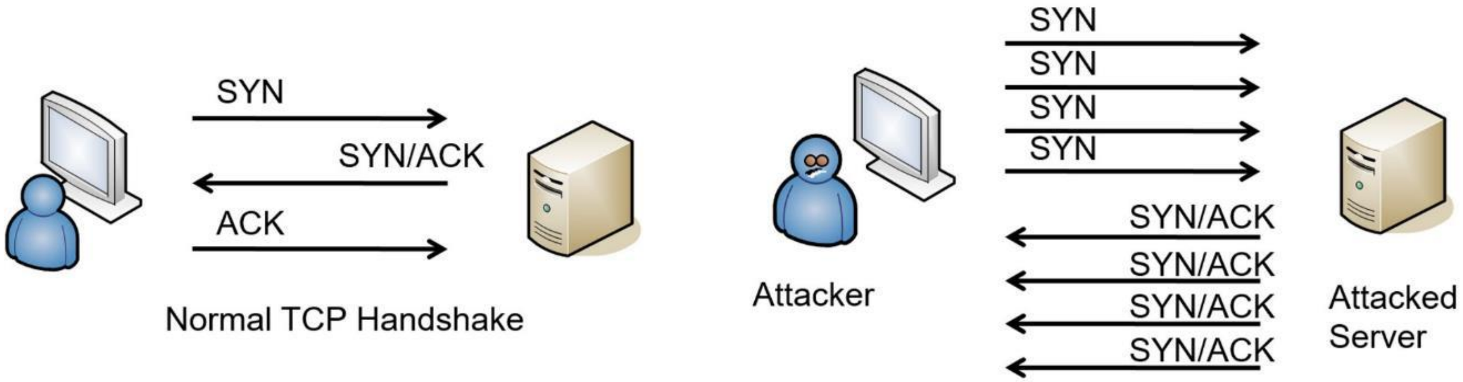
- Diamond Model of Intrusion Analysis
  - identifies four key components of every intrusion event
    - Adversary
    - Capabilities
    - Infrastructure
    - Victim
- MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)
  - matrix of ten tactics and techniques attackers use to achieve each

Network Attacks

- Denial-of-service (DoS)
  - Comes from one system
- Distributed denial-of-service (DDoS)
  - Multiple attacking computers
  - Typically include sustained, abnormally high network traffic







- SYN flood attack
  - Common attack against Internet servers
  - Disrupts the TCP three-way handshake
  - Withholds 3rd packet

Network Attacks

- Spoofing
  - Impersonating or masquerading as someone or something else
    - MAC spoofing
    - IP spoofing
- On-Path Attacks
  - sometimes referred to as a man-in-the-middle attack
  - is a type of proxy Trojan horse that infects vulnerable web browsers

Network Attacks

- Secure Sockets Layer (SSL) stripping attack
  - Hypertext Transfer Protocol Secure (HTTPS) connection to a Hypertext Transfer Protocol (HTTP) connection

- Layer 2 Attacks
  - attempt to exploit vulnerabilities at the Data Link layer (Layer 2) of the Open Systems Interconnection (OSI) model

Network Attacks

- Secure Sockets Layer (SSL) stripping attack
  - Hypertext Transfer Protocol Secure (HTTPS) connection to a Hypertext Transfer Protocol (HTTP) connection

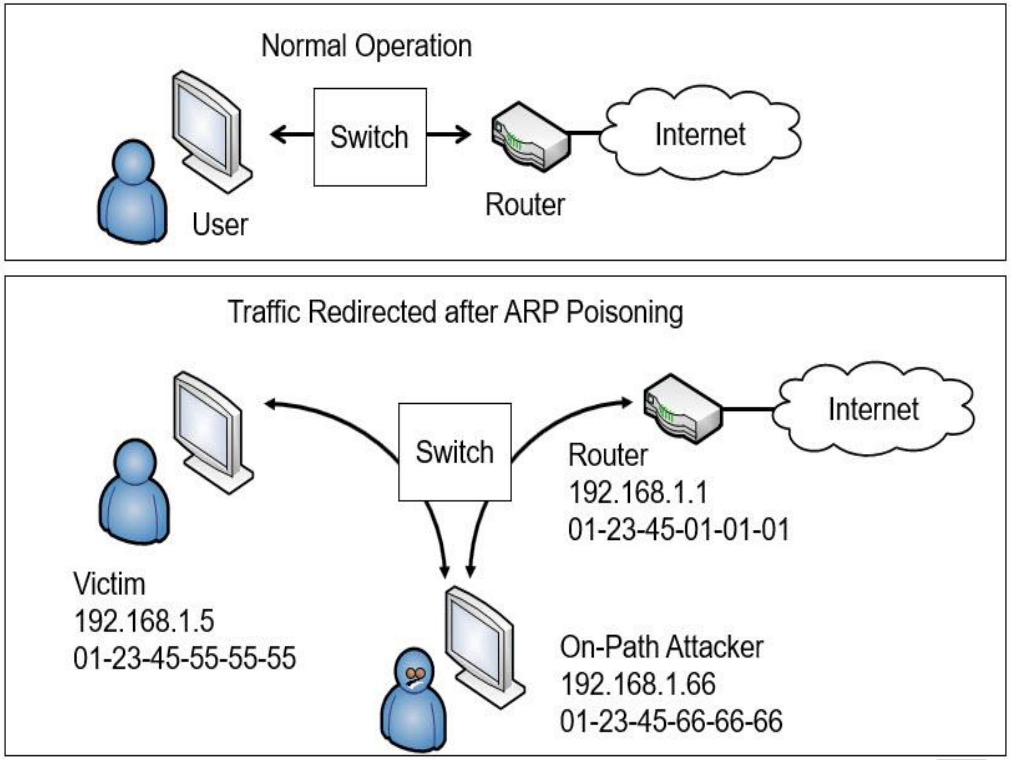
- Layer 2 Attacks
  - attempt to exploit vulnerabilities at the Data Link layer (Layer 2) of the Open Systems Interconnection (OSI) model

Network Attacks

ARP Poisoning

- **ARP request**
- **ARP reply**

- **ARP on-path attacks**
  - **Previously known as man-in-the-middle attack**



Layer 2 Attacks

- MAC flooding
  - attack against a switch that attempts to overload it with different MAC addresses
  - sends a Simple Network Management Protocol (SNMP) trap or error message
- MAC Cloning
  - changing a system's MAC address to another MAC address

DNS Attacks

- DNS poisoning
  - Attempt to corrupt DNS data
  - Protect against with DNSSEC
- URL redirection
  - used to redirect traffic to a different page within a site
- Domain hijacking
  - Attacker changes the registration of the domain name
  - Typically done by using social engineering techniques to guess owner’s password