Lecture notes - Chapter 5: Security Threats and Vulnerabilities

Topics: 1.5 hours

- Malware: Viruses, Worms, Trojans, Ransomware
- Social Engineering Attacks
- Denial-of-Service (DoS) and Distributed DoS (DDoS) Attacks
- Phishing and Spear Phishing
- Software and Application Vulnerabilities

Malware: Viruses, Worms, Trojans, Ransomware

Introduction to Malware

- **Malware (Malicious Software)**: Software intentionally designed to cause damage to a computer, server, client, or network.
- **Common Types**: Viruses, worms, Trojans, ransomware, spyware, adware.

Types of Malware

A. Viruses

- **Definition**: A virus is a type of malware that attaches itself to a legitimate file or program and spreads when that file or program is executed.
- **Characteristics**:
  - Requires a host (file or program).
  - Needs user interaction to spread (e.g., opening an infected file).
  - Can damage or modify files, disrupt services, or steal information.
- **Example**: The "ILOVEYOU" virus, which spread via email attachments.

B. Worms

- **Definition**: A worm is a standalone malware that replicates itself to spread to other computers, often exploiting vulnerabilities in networks.
- **Characteristics**:
  - Does not need a host or user interaction to spread.
  - Can self-replicate and spread across networks automatically.
  - May cause widespread network congestion or perform malicious actions like data deletion.
- **Example**: The "Conficker" worm, which spread rapidly through Windows systems.

C. Trojans

- **Definition**: A Trojan, or Trojan horse, is malware disguised as legitimate software to trick users into installing it.
- **Characteristics**:
  - Does not replicate like viruses or worms.

    - Typically used to create backdoors, steal data, or take control of the system.
    - Often hidden in seemingly harmless applications or downloads.
- **Example**: The "Zeus" Trojan, used to steal banking information.

D. Ransomware

- **Definition**: Ransomware is a type of malware that encrypts the victim's files or locks them out of their system, demanding payment (ransom) for restoring access.
- **Characteristics**:
    - Typically spread through phishing emails, malicious attachments, or exploits.
    - Encrypts user data, rendering it inaccessible until a ransom is paid.
    - Increasingly sophisticated; often uses cryptocurrency for anonymous payments.
- **Example**: The "WannaCry" ransomware attack that exploited a Windows vulnerability.

3. How Malware Spreads

- **Email Attachments**: Common for viruses and ransomware.
- **Network Vulnerabilities**: Worms exploit weaknesses in networks and systems to propagate.
- **Malicious Downloads**: Trojans are often disguised as legitimate software.
- **Phishing Attacks**: Used to trick users into downloading or executing malware.

4. Impacts of Malware

- **Data Loss**: Permanent loss of critical data.
- **Financial Loss**: Ransom payments, system recovery costs, downtime.
- **Reputational Damage**: Loss of trust from customers and partners.
- **System Disruption**: Inability to access files or use systems effectively.

5. Protection Against Malware

- **Antivirus Software**: Scans and removes known malware.
- **Firewalls**: Blocks unauthorized access and malicious traffic.
- **Regular Updates**: Patches vulnerabilities in software and systems.
- **User Education**: Training users to recognize phishing, suspicious downloads, and safe practices.

Social Engineering Attacks

Introduction to Social Engineering

- **Social Engineering**: Manipulation of individuals into divulging confidential information or performing actions that may compromise security.
- **Focus**: Exploits human psychology rather than technical vulnerabilities.
- **Common Targets**: Employees, users, administrators – anyone with access to sensitive information.

Types of Social Engineering Attacks

Phishing

- **Definition**: Deceptive attempt to obtain sensitive information by masquerading as a trustworthy entity via electronic communication (e.g., email).
- **Characteristics**:
  - Often involves fake websites, emails, or links.
  - Commonly targets credentials like usernames, passwords, credit card information.
- **Variants**:
  - **Spear Phishing**: Targeted attack aimed at specific individuals or organizations.
  - **Whaling**: Targeting high-profile individuals (e.g., executives).
  - **Smishing**: Phishing via SMS.
  - **Vishing**: Phishing via voice calls.
- **Example**: An email pretending to be from a bank, prompting the user to click a link and enter their login credentials.

Baiting

- **Definition**: Using false promises or the lure of something enticing to trick victims into compromising their security.
- **Characteristics**:
  - Can involve physical items (e.g., infected USB drives left in public) or online incentives (e.g., free downloads).
  - Users act out of curiosity or greed.
- **Example**: A USB drive labeled "Confidential" placed in a public area, hoping someone will insert it into their computer.

Quid Pro Quo

- **Definition**: An exchange-based attack where the attacker offers something of value in exchange for information or access.
- **Characteristics**:
  - Typically involves promises of help or rewards in return for sensitive information.
  - Often relies on the victim's willingness to reciprocate or receive assistance.
- **Example**: An attacker posing as tech support offering to fix a problem in exchange for the victim's login credentials.

Tailgating (Piggybacking)

- **Definition**: Gaining physical access to restricted areas by following authorized personnel.
- **Characteristics**:
  - Exploits human politeness and lack of suspicion.
  - Often done by pretending to have forgotten an access card or by carrying large items.
- **Example**: An attacker following an employee into a secure building by pretending to have lost their access badge.

Key Techniques Used in Social Engineering

- **Urgency**: Creating a sense of immediate action to prevent the target from thinking critically (e.g., "Your account will be locked unless you act now").
- **Authority**: Pretending to be a figure of authority to pressure the target into compliance (e.g., impersonating a manager or law enforcement).
- **Trust**: Building rapport or pretending to be someone familiar to the target to lower their defenses.
- **Fear**: Scaring the victim with potential consequences (e.g., legal threats, account compromise).

Why Social Engineering Works

- **Human Psychology**: Exploits cognitive biases like trust, urgency, and fear.
- **Lack of Awareness**: Users may not be educated about these types of attacks and how to recognize them.
- **Impersonation**: Attackers mimic legitimate sources (e.g., coworkers, vendors, or official organizations).

Protection Against Social Engineering

- **User Education and Awareness**: Training on how to recognize and respond to social engineering attacks.
- **Multi-Factor Authentication (MFA)**: Reduces the risk of unauthorized access, even if credentials are compromised.
- **Policies and Procedures**: Clear guidelines on how to handle requests for sensitive information.
- **Verification Mechanisms**: Always verify the identity of individuals requesting sensitive information, especially in unexpected situations.

Denial-of-Service (DoS) and Distributed DoS (DDoS) Attacks

Introduction to Denial-of-Service (DoS)

- **Denial-of-Service (DoS) Attack**: An attack that aims to make a system, network, or service unavailable by overwhelming it with a flood of illegitimate requests or traffic.
- **Goal**: Disrupt the availability of a service or system, preventing legitimate users from accessing it.

How DoS Attacks Work

- **Flooding**: Attackers send an overwhelming amount of traffic to a target, consuming resources like bandwidth, memory, or CPU.
- **Resource Exhaustion**: Consuming resources on a server, making it unable to respond to legitimate requests.
- **Vulnerability Exploitation**: Exploiting software vulnerabilities to crash or degrade system performance.

Types of DoS Attacks

A. Network-Level DoS

- **Traffic Overload**: The attacker floods the network with a massive volume of packets, saturating the target's bandwidth.
- **Examples**:
    - **ICMP Flood (Ping Flood)**: Sending a large number of ICMP Echo Request (ping) packets to overwhelm the target.
    - **UDP Flood**: Flooding the target with a large number of UDP packets.

B. Application-Level DoS

- **Resource Exhaustion**: Focuses on exhausting server resources by sending a large number of seemingly legitimate requests to the application.
- **Examples**:
    - **HTTP Flood**: Sending a high volume of HTTP GET or POST requests to overload the web server.
    - **Slowloris**: Keeping many HTTP connections open by sending incomplete requests, causing the server to keep connections open and eventually run out of resources.

Distributed Denial-of-Service (DDoS) Attacks

- **Distributed Denial-of-Service (DDoS) Attack**: A DoS attack originating from multiple compromised systems (often part of a botnet) to overwhelm the target.
- **Characteristics**:
    - **Scale**: Multiple machines are used to generate the attack traffic, making it much harder to mitigate.
    - **Botnets**: Networks of compromised computers (bots) controlled by the attacker.
    - **Global Reach**: Attack traffic can come from geographically dispersed locations.

Types of DDoS Attacks

A. Volume-Based Attacks

- **Purpose**: Saturate the target's bandwidth with massive amounts of traffic.
- **Examples**:
    - **DNS Amplification**: Using open DNS resolvers to send a high volume of DNS response traffic to the victim, amplifying the impact.
    - **SYN Flood**: Exploiting the TCP handshake process by sending numerous SYN requests without completing the connection.

B. Protocol-Based Attacks

- **Purpose**: Exhaust server resources by exploiting weaknesses in network protocols.
- **Examples**:
    - **Ping of Death**: Sending malformed or oversized packets to crash the target system.

    - **Smurf Attack**: Using spoofed ICMP packets to flood the target with response traffic.

C. Application Layer Attacks

- **Purpose**: Target specific application features with malicious intent to exhaust server resources.
- **Examples**:
    - **HTTP GET/POST Floods**: Sending a large number of HTTP requests to overwhelm the application server.
    - **DNS Query Flood**: Sending a massive number of DNS requests to exhaust the server's resources.

Real-World Examples of DoS and DDoS Attacks

- **GitHub DDoS Attack (2018)**: A DDoS attack that reached 1.35 Tbps, one of the largest recorded, which used Memcached servers to amplify traffic.
- **Dyn DDoS Attack (2016)**: A DDoS attack that used the Mirai botnet, causing widespread outages for websites like Twitter, Spotify, and Reddit by targeting DNS provider Dyn.

Impacts of DoS and DDoS Attacks

- **Service Downtime**: Websites or services become unavailable to legitimate users.
- **Revenue Loss**: Businesses lose potential sales or service opportunities during the outage.
- **Reputation Damage**: Loss of trust from customers and partners.
- **Mitigation Costs**: High costs associated with defending against the attack and restoring service.

Mitigating DoS and DDoS Attacks

- **Traffic Filtering**: Using firewalls, routers, or specialized DDoS mitigation services to block malicious traffic.
- **Rate Limiting**: Limiting the rate of requests to prevent overwhelming the system.
- **Redundancy**: Distributing traffic across multiple servers or data centers to balance the load.
- **Use of CDNs (Content Delivery Networks)**: Leveraging CDNs to distribute traffic and mitigate large-scale attacks.
- **Botnet Detection**: Identifying and neutralizing botnets used for DDoS attacks.

Lab: 1 hour

- Denial-of-Service attack using BURP
- Case Study on DoS based breaches

Social engineering - Bjorn's fav pet challenge