Topic 335: Threats and Vulnerability Assessment

335.1 Common Security Vulnerabilities and Threats (weight: 2)

Threats against individual nodes:

- **Malware infections:** Malware is a type of software designed to cause harm to a computer system. It can infect individual nodes, such as laptops or servers, and spread to other systems within a network.
- **Physical theft or tampering:** Physical threats to individual nodes can include theft or tampering, which can compromise the confidentiality and integrity of sensitive data stored on the device.
- **Unauthorized access**: Unauthorized access to individual nodes can occur through hacking or exploitation of vulnerabilities, leading to unauthorized data access or theft.
- **Outdated software vulnerabilities:** Outdated software can contain known vulnerabilities that are easy targets for attackers.

Threats against networks:

- **DDoS attacks:** A Distributed Denial of Service (DDoS) attack is a type of attack that floods a network with traffic, overwhelming its resources and making it unavailable.
- **Man-in-the-middle attacks:** A man-in-the-middle (MitM) attack is a type of cyber attack where an attacker intercepts and alters communications between two parties, often without either party being aware.
- **Rogue devices/attacks from inside the network:** Rogue devices and attacks from within a network can be a major threat, as insiders may have access to sensitive data and systems.
- **Unsecured network protocols:** Unsecured network protocols can be vulnerable to exploitation by attackers, leading to data theft or unauthorized access.

Threats against applications:

- **SQL injections:** SQL injection is a type of attack where an attacker inserts malicious code into a web application's SQL statement, allowing them to gain unauthorized access to sensitive data stored in a database.
- **Cross-site scripting (XSS):** Cross-site scripting (XSS) is a type of attack that allows an attacker to inject malicious code into a web application, which can then be executed by unsuspecting users.
- **Remote code execution:** Remote code execution is a type of vulnerability that allows an attacker to execute code on a target system, often with the same privileges as the user running the vulnerable application.
- **Improper authentication and authorization:** Improper authentication and authorization can lead to unauthorized access to sensitive data and systems, as well as data theft.

Threats against credentials and confidentiality:

- **Phishing attacks:** Phishing is a type of social engineering attack where an attacker pretends to be a trusted entity in order to trick a user into revealing sensitive information, such as login credentials.
- **Social engineering:** Social engineering is the use of psychological manipulation to trick individuals into divulging sensitive information or performing actions that compromise their security.
- **Password cracking:** Password cracking is the process of attempting to guess or uncover a password, often using automated tools or exploiting vulnerabilities in password storage systems.
- **Unsecured data storage:** Unsecured data storage refers to the failure to properly secure sensitive data, such as through encryption or proper access controls, leaving it vulnerable to theft or unauthorized access.

Honeypots:

- **Decoy systems to distract attackers:** A honeypot is a decoy system designed to distract and divert attackers away from more valuable systems and data.
- **Collect information on attacker behavior and tools:** Honeypots can be used to collect information on attacker behavior and tools, providing valuable intelligence for security teams.

- **Help identify and mitigate emerging threats:** By monitoring attacker behavior, honeypots can help identify and mitigate emerging threats, improving overall security posture.
- **Monitor and detect unauthorized access attempts:** Honeypots can also be used to detect unauthorized access attempts, providing early warning of security incidents and helping to prevent more serious breaches.

The following is a partial list of the used files, terms and utilities:

Trojans: A Trojan is a type of malicious software that is disguised as a legitimate program. Trojans can be used to perform a variety of malicious activities, such as stealing sensitive information, installing other malicious software, or giving an attacker remote access to the infected system.

Viruses: A virus is a type of malicious software that replicates itself by infecting other files on a computer. Viruses can cause damage to files and systems, or use the infected computer as a platform for further attacks.

Rootkits: A rootkit is a type of malicious software that is designed to hide its presence and actions on an infected system. Rootkits can be used to gain persistent access to a system, bypass security measures, or steal sensitive information.

Keylogger: A keylogger is a type of malicious software or hardware device that records every keystroke made on a computer or device. Keyloggers are often used to steal passwords, credit card numbers, and other sensitive information.

DoS and DDoS: A Denial of Service (DoS) attack is an attempt to make a network resource unavailable to its intended users. A Distributed Denial of Service (DDoS) attack is a type of DoS attack that involves multiple devices attacking a single target. DoS and DDoS attacks can be used to disrupt online services, websites, and other networked systems.

Man-in-the-Middle: A man-in-the-middle (MitM) attack is a type of security attack where the attacker intercepts and alters the communication between two parties. MitM attacks can be used to steal sensitive information, alter data, or perform other malicious activities.

ARP and NDP Forgery: Address Resolution Protocol (ARP) and Neighbor Discovery Protocol (NDP) forgery are types of security attacks that involve falsifying ARP or NDP packets in a network. These attacks can be used to redirect network traffic, steal sensitive information, or perform other malicious activities.

Rogue Access Points, Routers, and DHCP Servers: Rogue access points, routers, and DHCP servers are unauthorized network devices that are placed on a network without the knowledge or consent of network administrators. These devices can be used to perform various malicious activities, such as intercepting network traffic, redirecting network traffic, or stealing sensitive information.

Link Layer and IP Address Spoofing: Link layer address spoofing and IP address spoofing are types of security attacks that involve falsifying the source address of a network packet. These attacks can be used to perform various malicious activities, such as intercepting network traffic, redirecting network traffic, or stealing sensitive information.

Buffer Overflows: A buffer overflow is a type of security vulnerability that occurs when a program writes more data to a buffer than it can hold. This can result in overwriting adjacent memory and causing the program to crash or execute arbitrary code.

Cross-Site Request Forgery (CSRF): Cross-site request forgery (CSRF) is a type of security Privilege Escalation: Privilege escalation is a type of security attack that involves a malicious actor gaining access to higher-level privileges on a computer system. This can be achieved through exploiting vulnerabilities in software, stealing credentials, or using social engineering tactics.

Brute Force Attacks: A brute force attack is a type of security attack that involves attempting to guess the password or key for a system or service by trying every possible combination. Brute force attacks can be used to gain unauthorized access to systems, steal sensitive information, or perform other malicious activities.

Rainbow Tables: A rainbow table is a precomputed table of hashes used in password cracking. Rainbow tables are used to speed up the process of guessing a password by reducing the number of hashes that need to be calculated.

335.2 Penetration Testing (weight: 3)

Penetration testing, also known as ethical hacking, is a simulated attack on a computer system or network to identify vulnerabilities and assess the security posture of the target. It is performed by ethical hackers who use the same tools and techniques as malicious hackers, but with the permission of the target organization.

The legal implications of penetration testing vary by jurisdiction and must be considered before conducting a test. In some countries, unauthorized access to computer systems is illegal, and penetration testers must have written permission from the target organization to perform the test.

Penetration testing is a method of evaluating the security of a computer system or network by simulating an attack. It involves several phases that help to identify vulnerabilities and evaluate the effectiveness of security measures. Here's an overview of the phases of a penetration test:

- **Active and passive information gathering:** This phase involves collecting information about the target system or network, both passively (without interacting with the target) and actively (by interacting with the target). Passive information-gathering techniques include researching public information about the target, while active techniques include using tools like **Nmap** to scan the target network.

- **Enumeration:** This phase involves actively interacting with the target to gather information about its systems, services, and users. This information can be used to identify potential vulnerabilities and attack vectors.
- **Gaining access:** This phase involves attempting to exploit vulnerabilities and gain access to the target system or network. This can involve techniques like brute force attacks, exploiting software vulnerabilities, or social engineering attacks.
- **Privilege escalation:** This phase involves increasing the level of access or control on the target system once access has been gained. This can be done by exploiting vulnerabilities in the operating system or applications, or by compromising additional systems or user accounts.
- **Access maintenance:** This phase involves maintaining access to the target system, including covering tracks to conceal the presence of the attacker and creating backdoors to allow future access.

- **Covering tracks:** This phase involves removing the evidence of the attack, such as log files or configuration changes, and cleaning up any malware or other malicious software that may have been installed during the attack.

These phases are not always performed in a strict order, and the focus and scope of a penetration test can vary depending on the specific requirements and objectives of the test. However, they provide a general framework for conducting a penetration test and evaluating the security of a computer system or network.

Metasploit is a popular framework for security testing that includes a collection of modules for various purposes. These modules can be divided into three main categories: exploits, payloads, and auxiliary modules.

- **Exploits:** Exploits are modules that take advantage of vulnerabilities in software or systems to gain unauthorized access or control. Exploits are typically used to deliver payloads to target systems.
- **Payloads:** Payloads are modules that are executed on the target system once an exploit has been successful. Payloads can perform a variety of actions, such as capturing keystrokes, stealing data, or establishing a reverse shell connection back to the attacker.
- **Auxiliary modules:** Auxiliary modules are modules that perform a variety of other functions, such as reconnaissance, network scanning, and vulnerability analysis. Auxiliary modules can be used to gather information about a target system or network, identify potential vulnerabilities, and assist in the execution of exploits and payloads.

Each of these types of modules has a specific purpose and can be used together to achieve different objectives during a penetration test. The Metasploit framework provides a flexible and modular platform for security testing that can be customized to meet specific needs.

Nmap is a tool used for network exploration and security auditing. It allows users to scan networks and hosts to identify open ports, operating systems, and running services. Nmap supports different scan methods, including version scans and operating system recognition, and also has a scripting engine that allows users to automate and customize their scans. Here are some of the most important Nmap scans and the corresponding commands:

- **Ping scan (-sP):** This scan is used to determine if a host is up and responding. It sends a simple ping request to the target host and reports if it received a response.
  Command: **nmap -sP <target_host>**
- **Port scan (-p):** This scan is used to identify open ports on a target host. It sends packets to the specified ports and analyzes the response to determine if the port is open, closed, or filtered.
  Command: **nmap -p <port_range> <target_host>**

- **Version scan (-sV):** This scan is used to determine the version of services running on a target host's open ports. It sends requests to the open ports and analyzes the responses to determine the software and version being used.
  Command: **nmap -sV <target_host>**
- **OS scan (-O):** This scan is used to determine the operating system running on a target host. It analyzes the responses from the target host to determine the operating system type and version.
  Command: **nmap -O <target_host>**
- **Stealth scan (-sS):** This scan is a type of port scan that is designed to be less detectable. It uses a technique called half-open scanning, where only a single packet is sent to the target host to determine if the port is open.
  Command: **nmap -sS <target_host>**

- **TCP scan:** A TCP scan is used to determine if a target host's TCP ports are open, closed, or filtered. It sends packets to the target host's TCP ports and analyzes the responses to determine the status of the port.
  Command: **nmap -sT <target_host>**

- **UDP scan:** A UDP scan is used to determine if a target host's UDP ports are open, closed, or filtered. It sends packets to the target host's UDP ports and analyzes the responses to determine the status of the port.
  Command: **nmap -sU <target_host>**

It is important to note that UDP scans are typically slower than TCP scans because the UDP protocol does not provide the same level of reliability as TCP. As a result, UDP scans may not receive a response from all target hosts, and false negatives can occur. However, UDP scans are useful for identifying open UDP ports, which can sometimes be overlooked during a TCP scan.

Kali Linux is a widely used distribution of Linux designed specifically for security testing and ethical hacking. It comes pre-installed with a variety of tools, including Nmap, Metasploit, and Armitage, a graphical interface for Metasploit. **The Social Engineer Toolkit (SET)** is another tool that can be used for penetration testing and is focused on exploiting human vulnerabilities through social engineering techniques.