FR. CONCEICAO RODRIGUES COLLEGE OF ENGG.
Fr. Agnel Ashram, Bandstand, Bandra (W) Mumbai 400 050.

SEMESTER / BRANCH: V (CE/AIDS/ECS)

Subject code: HCSC501

SUBJECT: Cyber Security (HONORS): Ethical Hacking / First Assignment

Date: 20-08-23 Due Date : 25-08-23

Roll no : - 9633

-> The OSI Model we just looked at is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components.

TCP/IP was designed and developed by the Department of Defense (DoD) in the 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike the seven layers in the OSI model.

The number of layers is sometimes referred to as five or four. Here In this article, we'll study five layers. The Physical Layer and Data Link Layer are referred to as one single layer as the 'Physical Layer' or 'Network Interface Layer' in the 4-layer reference.

The main work of TCP/IP is to transfer the data of a computer from one device to another. The main condition of this process is to make data reliable and accurate so that the receiver will receive the same information which is sent by the sender. To ensure that, each message reaches its final destination accurately, the TCP/IP model divides its data into packets and combines them at the other end, which helps in maintaining the accuracy of the data while transferring from one end to another end.

-> IP routing is one of the important topics in computer networks. IP routing is performed on the data which describes the path that data follows to reach from source to destination in the network. Through IP routing only the shortest path for the data is determined to reach the destination which decreases cost and data is sent in minimum time. IP routing uses different protocols and technologies for different networks. For IP routing we require some basics of IP addresses, routers, and different networks.

IP routing is the process that defines the shortest path through which data travels to reach from source to destination. It determines the shortest path to send the data from one computer to another computer in the same or different network. Routing uses different

protocols for the different networks to find the path that data follows. It defines the path through which data travel across multiple networks from one computer to other. Forwarding the packets from source to destination via different routers is called routing. The routing decision is taken by the routers.

-> Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system, application, or data. Carrying out an ethical hack involves duplicating strategies and actions of malicious attackers. This practice helps to identify security vulnerabilities which can then be resolved before a malicious attacker has the opportunity to exploit them.

Also known as “white hats,” ethical hackers are security experts that perform these security assessments. The proactive work they do helps to improve an organization’s security posture. With prior approval from the organization or owner of the IT asset, the mission of ethical hacking is opposite from malicious hacking.

-> The OSI (Open Systems Interconnection) model and the TCP/IP (Transmission Control Protocol/Internet Protocol) model are both conceptual frameworks that describe the functions and interactions of networking protocols and services. They are significant in understanding network communication because they provide a structured way to conceptualize and discuss the various layers of network protocols, making it easier to design, troubleshoot, and manage complex networking systems. Below, I'll compare and contrast these two models:

OSI Model:
1. **Seven Layers:** The OSI model divides network communication into seven distinct layers, each responsible for specific functions.
2. **Conceptual Model:** The OSI model is more of a theoretical or conceptual framework and is not directly tied to the actual protocols used on the internet.
3. **Structured Approach:** It provides a structured approach to understanding network communication, making it easier to isolate and solve problems in each layer.
4. **Universal Standard:** While not as widely adopted as the TCP/IP model, the OSI model serves as a universal standard for discussing network layers and concepts.
5. **Layers:** The seven layers, from top to bottom, are: Application, Presentation, Session, Transport, Network, Data Link, and Physical.

TCP/IP Model:
1. **Four Layers:** The TCP/IP model simplifies network communication into four main layers, which are more closely aligned with the actual protocols used on the internet.
2. **Practical Model:** It is a practical model that directly maps to the suite of protocols used in the Internet, including TCP, IP, UDP, and more.
3. **Real-World Relevance:** It is the model most commonly used for describing and understanding the internet and its communication protocols, making it highly relevant for network engineers.
4. **Layers:** The four layers, from top to bottom, are: Application, Transport, Internet, and Network Interface (or Link) Layer.

Comparison:
1. **Layer Count:** The OSI model has seven layers, while the TCP/IP model has four. The TCP/IP model combines the Application, Presentation, and Session layers of the OSI model into a single Application layer, and the Data Link and Physical layers into a single Network Interface or Link Layer.

2. **Real-World Application:** The TCP/IP model is more practical and directly maps to the protocols used on the Internet, while the OSI model is more of a theoretical concept that is not directly tied to real-world protocols.

3. **Widespread Use:** The TCP/IP model is the de facto standard for describing internet communication, used in most networking contexts, while the OSI model is less commonly used in practice.

4. **Layer Functionality:** In both models, there is a general correspondence between layers in terms of functionality, such as the Transport layer being responsible for end-to-end communication and the Network layer handling routing.

In summary, both models serve as valuable tools for understanding network communication, with the OSI model providing a more detailed and theoretical approach, and the TCP/IP model being the more practical and widely adopted model that directly corresponds to the protocols used on the internet. Understanding these models helps network professionals design, troubleshoot, and manage network systems effectively.

-> Information gathering and reconnaissance, often the first phase of a cyberattack, involve the systematic collection of data about a target network or system. In this context, it is typically used by both ethical security professionals and malicious hackers. During this phase, attackers aim to gather as much information as possible about the target, such as IP addresses, network topology, server names, software versions, and potentially vulnerabilities. Attackers use various techniques like port scanning, OS fingerprinting, and web scraping to discover weaknesses or entry points. This phase is crucial for attackers, as it provides them with the necessary insights to plan and execute more targeted and effective attacks, such as exploiting known vulnerabilities, social engineering, or crafting specific malware. Exploiting this phase allows attackers to increase the chances of their attacks succeeding while minimizing the risk of detection.

->

Vulnerability Assessment:

1. **Purpose:** Vulnerability assessment is a proactive approach to identifying and quantifying vulnerabilities in a system, network, or application. It focuses on finding weaknesses in the target environment, which may be used to launch attacks.

2. **Scope:** It involves scanning and assessing the system for known vulnerabilities. It does not typically involve actively exploiting these vulnerabilities.

3. **Tools:** Examples of tools used for vulnerability assessment include:
   - Nessus
   - OpenVAS (Open Vulnerability Assessment System)
   - Qualys
   - Rapid7 Nexpose
   - Microsoft Baseline Security Analyzer (MBSA)

4. **Outcome:** The primary outcome is a report listing identified vulnerabilities and their severity levels. This information helps organizations prioritize and address security issues.

Penetration Testing:

1. **Purpose:** Penetration testing, often referred to as ethical hacking, involves actively simulating cyberattacks to discover vulnerabilities that could be exploited by malicious actors. The aim is to assess the security of the system and determine its resilience against real-world threats.

2. **Scope:** It goes beyond identifying vulnerabilities and actively attempts to exploit them to gauge the system's response and the potential impact of an attack.

3. **Tools:** Examples of tools used for penetration testing include:
   - Metasploit
   - Burp Suite
   - Nmap
   - Wireshark
   - Aircrack-ng

4. **Outcome:** The outcome of penetration testing is a detailed report that not only lists vulnerabilities but also provides insights into the likelihood and potential impact of a successful attack. This information is valuable for organizations to improve their security posture.

In summary, vulnerability assessment is a more passive process focused on identifying vulnerabilities in a system, while penetration testing is an active process that involves trying to exploit these vulnerabilities to assess the system's security under real-world conditions. Both processes are essential for a comprehensive security strategy, with vulnerability assessments providing the foundation for understanding weaknesses, and penetration testing simulating how those weaknesses could be exploited by attackers.

-> **Key Characteristics of Social Engineering Attacks:**

1. **Manipulation of Human Psychology:** Social engineering attacks exploit human psychology and emotions, such as trust, fear, curiosity, and authority. Attackers use these emotions to manipulate individuals into divulging sensitive information or performing actions they wouldn't normally do.

2. **Deception and Impersonation:** Social engineers often impersonate someone trusted, like a colleague, boss, or service provider. They use various communication methods, such as phone calls, emails, or in-person interactions, to gain the victim's trust.

3. **Pretexting:** Attackers create a fabricated scenario or pretext to manipulate the victim into disclosing information. This can involve pretending to be from IT support, a bank, or a government agency, and asking for sensitive data under the guise of solving an issue.

4. **Phishing and Spear Phishing:** Phishing emails are a common social engineering tactic. Attackers send emails that appear legitimate, containing malicious links or attachments. Spear phishing targets specific individuals or organizations with personalized messages.

5. **Baiting:** This involves enticing victims with an offer, such as free software or a fake survey, which requires them to provide personal or sensitive information when they take the bait.

Educating Employees to Prevent Social Engineering Attacks:

1. **Training and Awareness Programs:** Organizations should implement regular training and awareness programs to educate employees about social engineering techniques and how to recognize them. These programs should include examples of phishing emails and common social engineering tactics.

2. **Phishing Simulations:** Conducting simulated phishing campaigns can help employees recognize phishing emails and report them. It also provides a safe environment for learning.

3. **Multi-Factor Authentication (MFA):** Encourage the use of MFA for access to systems and data. MFA adds an extra layer of security, making it harder for attackers to gain unauthorized access, even if they have some login credentials.

4. **Policies and Procedures:** Develop and enforce clear security policies and procedures related to information sharing, access control, and employee verification. Ensure that employees are aware of these policies.

5. **Verification Protocols:** Implement protocols for verifying the identity of individuals requesting sensitive information or actions. Employees should be cautious when responding to unsolicited requests, especially if they involve sharing sensitive data.

6. **Incident Reporting:** Establish a clear and user-friendly process for reporting suspicious activities or potential security incidents. Encourage employees to report anything they find unusual or suspicious.

7. **Regular Updates and Patch Management:** Keep software and systems up-to-date to reduce the risk of attackers exploiting known vulnerabilities. Educate employees on the importance of applying updates promptly.

8. **Security Culture:** Foster a security-aware culture within the organization where employees understand the significance of their role in safeguarding company information.

9. **Testing and Evaluation:** Regularly assess the effectiveness of security awareness programs and adjust them based on feedback and emerging threats.

Preventing social engineering attacks requires a combination of technological safeguards and an informed and vigilant workforce. Educating employees on these threats and promoting a security-conscious culture is essential for reducing the risk of falling victim to social engineering attacks.

->

Viruses:
- A computer virus is a type of malware that attaches itself to legitimate programs or files. When the infected program is executed, the virus replicates and spreads to other programs or files. Viruses are often spread through infected email attachments, downloads, or sharing infected files.
- Impact on Network Security: Viruses can severely impact network security by corrupting or deleting files, stealing sensitive data, and disrupting network operations. They can also spread rapidly and infect multiple devices within a network if not detected and contained.

Worms:
- Worms are self-replicating malware that don't need a host program to spread. They exploit vulnerabilities in network protocols or operating systems to propagate. Worms can spread quickly across networks and the internet.
- Impact on Network Security: Worms can congest network traffic, consume bandwidth, and overwhelm servers. They may also carry payloads that can cause data breaches or damage to networked devices, making them a significant threat to network security.

Trojans (or Trojan Horses):
- Trojans are malware that disguise themselves as legitimate software or files to deceive users into running them. Once activated, Trojans can carry out malicious activities, such as data theft, remote access, or installing additional malware.
- Impact on Network Security: Trojans can provide unauthorized access to network resources, enabling attackers to compromise the network's integrity and confidentiality. They often serve as entry points for more extensive attacks.

Ransomware:
- Ransomware is a type of malware that encrypts a victim's files and demands a ransom in exchange for a decryption key. It can spread through malicious email attachments, infected downloads, or vulnerabilities in networked systems.
- Impact on Network Security: Ransomware can lead to data loss, financial losses, and significant downtime. It can affect not only individual devices but also network file shares, crippling an organization's ability to operate.

Spyware and Adware:

- Spyware is designed to collect sensitive information or monitor a user's activities without their knowledge or consent. Adware, on the other hand, bombards users with unwanted advertisements.
- Impact on Network Security: These types of malware can compromise user privacy and slow down network performance. Spyware may lead to data leaks, while adware can disrupt user productivity.

Botnets:
- Botnets are networks of compromised computers (bots) controlled by a single entity (the botmaster). These bots can be used for various malicious activities, such as launching DDoS attacks, sending spam, or stealing information.
- Impact on Network Security: Botnets can perform coordinated attacks on network infrastructure, leading to service disruption or data theft. They are challenging to detect and dismantle due to their distributed nature.

Rootkits:
- Rootkits are a type of malware that hides their presence and activities on an infected system. They often gain deep access to the operating system, making them challenging to detect and remove.
- Impact on Network Security: Rootkits can undermine the network's security by granting attackers persistent and privileged access to systems. This access can be exploited for data exfiltration, further malware deployment, or surveillance.

The impact of these malware threats on network security can be devastating. They can lead to data breaches, financial losses, legal consequences, and damage to an organization's reputation. To mitigate these risks, organizations must employ robust cybersecurity measures, including antivirus software, intrusion detection systems, regular patching, user education, and network monitoring.