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

HCSC501 .1: **Articulate the fundamentals of Computer Networks, IP Routing and core concepts of ethical hacking in real world scenarios.**

HCSC501 .2: Apply the knowledge of information gathering to perform penetration testing and social engineering attacks.

Questions :

1. What are the core components of the TCP/IP protocol stack and how do they contribute to the functioning of computer networks? (L2, CO1)

The core components of the TCP/IP protocol stack:

Application Layer: It includes programs and services that let you do things like sending emails (SMTP), browsing websites (HTTP), and chatting (FTP). It helps you decide what kind of communication you want to do.

Transport Layer: It manages the actual sending and receiving of data between your computer and the other one. There are two popular "waiters" here: TCP and UDP. TCP makes sure the data arrives in order and completes, like assembling a puzzle. UDP is faster but doesn't check if all pieces of the puzzle arrived.

Internet Layer: It uses IP addresses to locate your computer and the one you want to talk to. Just like your home address helps the delivery person find you, IP addresses help data find its way across the internet.

Link Layer: It deals with physical connections, like Wi-Fi or Ethernet cables. It makes sure that the data packets travel safely across these connections.

Physical Layer: It's the physical hardware like wires, radio waves, and other technology that physically transfers the data.

2. Explain the process of IP addressing and routing in a computer network. How does routing protocol help in efficient data transmission? (L2, CO1)

IP Addressing:

Assigns unique numerical labels (IP addresses) to devices on a network. Identifies and locates devices for communication. Facilitates communication between devices on the network.

Routing:

Selects paths for data to travel from source to destination. Data is divided into packets with destination IP addresses. Routers determine best paths for packets based on destinations.

Routers:

Specialized network devices for routing data. Use routing tables and protocols for routing decisions.

Routing Tables:

Stores information about network destinations and paths. Contains data needed to make routing decisions.

Routing Protocols:

Used by routers to exchange destination info. Dynamically updates routing tables based on network changes.

Efficient Data Transmission:

Routing protocols help routers choose optimal paths. Adjust routing based on changing network conditions. Ensures quick and efficient data transmission.

3. Outline the key steps involved in ethical hacking and describe how these steps contribute to securing computer systems. (L2, CO1)

1. Planning and Reconnaissance:
   - Understand the target system and its components.
   - Gather information about potential vulnerabilities and weaknesses.

2. Scanning:
   - Use various tools to actively scan the target for vulnerabilities.
   - Identify open ports, services, and potential attack vectors.

3. Gaining Access:
   - Attempt to exploit vulnerabilities to gain access.
   - Mimic real-world attacks to uncover weaknesses.

4. Maintaining Access
   - Once access is achieved, maintain control to analyze the extent of compromise.
   - Mimics how attackers could stay undetected over time.
5. Analysis and Reporting:
- Evaluate the results of the ethical hacking tests.
- Document identified vulnerabilities and potential impacts.
- Provide recommendations to fix and strengthen security measures.

These steps contribute to securing computer systems by:

- Realistic Testing: It mirrors real-world attacks, providing insights into actual system weaknesses and helping improve defenses.
- Risk Reduction: By addressing identified vulnerabilities, the risk of successful cyberattacks is reduced, enhancing overall system security.
- Enhanced Preparedness Ethical hacking prepares organizations to respond effectively to potential breaches, minimizing potential damages.
- Continuous Improvement: Ethical hacking is an ongoing process that promotes the continuous enhancement of security measures based on evolving threats.

4. Compare and contrast the OSI model and the TCP/IP model, highlighting their significance in understanding network communication. (L2, CO1)

The OSI (Open Systems Interconnection) model and the TCP/IP (Transmission Control Protocol/Internet Protocol) model are both conceptual frameworks that describe how different networking protocols work together to enable network communication. They provide a structured way to understand the layers of network communication. Here's a comparison and contrast of these two models, highlighting their significance in understanding network communication:

1. Number of Layers:

-OSI Model:The OSI model consists of seven layers, which are Application, Presentation, Session, Transport, Network, Data Link, and Physical, from top to bottom.

- TCP/IP Model: The TCP/IP model has four layers, which are Application, Transport, Internet (Network), and Link, from top to bottom. The TCP/IP model combines the Presentation and Session layers into the Application layer of the OSI model.

2. Significance:

- OSI Model: The OSI model provides a more comprehensive and detailed framework, making it a useful tool for theoretical understanding of networking concepts. It separates functions and services into individual layers, making it easier to identify and troubleshoot network issues.

- TCP/IP Model: The TCP/IP model is more closely aligned with the actual implementation of the Internet. It is used to describe how the internet and most modern networks operate. While it lacks some of the detail of the OSI model, it is more practical and directly applicable.

3. Protocols and Standards:

- OSI Model: The OSI model is not directly tied to any specific set of protocols, and it is more of a theoretical guideline for understanding network communication. Various protocols fit into its framework, but it is not as commonly used as the TCP/IP model for practical networking.

- TCP/IP Model: The TCP/IP model is directly associated with the suite of protocols and standards that are used in the Internet. The layers in the TCP/IP model align closely with specific protocols, such as HTTP, FTP, TCP, IP, and Ethernet.

4. Layer Descriptions:

- OSI Model: Each layer of the OSI model has specific responsibilities. For example, the Network layer handles routing, while the Data Link layer deals with error detection and correction. These responsibilities are more clearly defined and separated.

- TCP/IP Model: The TCP/IP model provides more generalized descriptions of its layers. For instance, the Transport layer is responsible for end-to-end communication, and the Internet layer handles routing, but it does not define specific services as rigidly as the OSI model.

5. Real-World Application:

- OSI Model: While the OSI model is not as commonly used in practice, it is valuable for teaching and understanding network concepts in a structured way.

- TCP/IP Model: The TCP/IP model is the de facto standard for describing network protocols and is used extensively in real-world networking scenarios. It is the model you are likely to encounter when configuring and troubleshooting networks.

In summary, the OSI model is more comprehensive and theoretical, serving as a framework for understanding networking concepts, while the TCP/IP model is more practical and directly applicable to real-world networking, especially in the context of the Internet. Understanding both models can provide a well-rounded knowledge of network communication.

5. **Explain the process of information gathering and reconnaissance in the context of network security. How can attackers exploit this phase? (L3, CO2)**

Info Gathering & Recon in Security Assessment:
- Essential in security checks, exposing vulnerabilities.
- Ethical hacking's reconnaissance phase collects data for attack paths. - Data includes network info, aiding multiple attack vectors.

Footprinting: Passive & Active:
- Passive: Gather public data (websites, news).
- Active: Intrusive methods (hacking, social engineering).

Recon Objectives:
- Attackers choose vulnerable targets, explore exploits.
- Any org member can be the initial target.
- Single entry point is enough to begin.
- Targeted phishing emails for malware spread.
- Focus: understand target, personnel, relationships, and public data.

Exploiting Recon Data:

- Data used for targeted attacks, social engineering.
- Vulnerabilities found exploited for unauthorized access.

Preventing Recon Attacks:
- Strong security policies, controls needed.
- Regular network monitoring is crucial.
- Educate employees on spotting social engineering.

Understanding the initial phase is vital for prevention and early detection.

6. **Differentiate between vulnerability assessment and penetration testing. Provide examples of tools used for each of these processes. (L2, CO2)**

Vulnerability assessment and penetration testing are both essential components of a comprehensive cybersecurity strategy, but they serve different purposes and have distinct methodologies. Here's a differentiation between vulnerability assessment and penetration testing:

1. Purpose:

- Vulnerability Assessment: The primary purpose of a vulnerability assessment is to identify and prioritize security vulnerabilities within a network, system, or application. It focuses on finding weaknesses, misconfigurations, and potential entry points for attackers. The emphasis is on evaluating the overall security posture and understanding where vulnerabilities exist.

- Penetration Testing: Penetration testing, often referred to as "pen testing," is conducted to simulate real-world cyberattacks. The primary goal is to actively exploit identified vulnerabilities to assess the effectiveness of an organization's security defenses. Pen testing goes beyond identifying weaknesses and aims to determine the extent to which an attacker could compromise a system or network.

2. Approach:

- Vulnerability Assessment: Vulnerability assessments are typically automated or semi-automated processes that use scanning tools to identify vulnerabilities in a systematic and comprehensive manner. These assessments are less intrusive and don't involve actively attempting to exploit vulnerabilities.

- Penetration Testing: Penetration testing is a manual and highly controlled process performed by ethical hackers who actively attempt to exploit vulnerabilities. The approach is more aggressive and resembles an actual cyberattack to gauge an organization's response capabilities.

3. Scope:

- Vulnerability Assessment: Vulnerability assessments are broader in scope and are often used for regular security audits and compliance checks. They help organizations identify weaknesses and compliance issues across their entire network.

- Penetration Testing: Penetration tests have a narrower scope. They focus on specific systems, applications, or components, and they aim to provide a deeper understanding of how a determined attacker might exploit identified vulnerabilities.

4. Reporting:

- Vulnerability Assessment:Vulnerability assessments typically provide a list of identified vulnerabilities along with their severity ratings and recommendations for remediation. The emphasis is on providing actionable information to improve security.

- Penetration Testing: Penetration testing reports go beyond vulnerability lists. They describe how vulnerabilities were exploited, the extent of potential damage, and the impact of a successful attack. They also provide recommendations for addressing vulnerabilities and improving security.

5. Frequency:

- Vulnerability Assessment: Vulnerability assessments are often conducted regularly, such as on a monthly or quarterly basis, to continuously monitor and improve security.

- Penetration Testing: Penetration testing is usually conducted periodically, such as annually or on an as-needed basis, to evaluate the security posture more comprehensively and to test the organization's response to attacks.

In summary, vulnerability assessments are primarily focused on identifying and prioritizing vulnerabilities for the purpose of improving overall security, while penetration testing involves actively trying to exploit those vulnerabilities to assess an organization's readiness to defend against real-world attacks. Both are important tools in the cybersecurity toolkit, and they are often used together to strengthen an organization's security posture.

Example Tools for Vulnerability Assessment:

- Nessus: A widely used vulnerability scanner that identifies and reports vulnerabilities. - OpenVAS: An open-source vulnerability scanner that detects security issues in systems and networks.
- Qualys: A cloud-based platform that performs vulnerability assessments on various assets.

Example Tools for Penetration Testing:

- Metasploit: A versatile penetration testing tool that aids in exploiting vulnerabilities.
- Nmap: A network scanning tool often used to discover open ports and services.
- Burp Suite: A web vulnerability scanner and proxy tool to test web applications.

7. Describe the key characteristics of social engineering attacks and discuss how organizations can educate their employees to prevent such attacks. (L2, CO2)

Key Characteristics of Social Engineering Attacks:

Manipulation of Human Psychology: Social engineering attacks exploit human emotions and behaviors, such as trust, fear, curiosity, and authority, to manipulate individuals into taking actions that benefit the attacker.

Pretexting: Attackers create fabricated scenarios or pretexts to deceive victims into divulging sensitive information or performing actions they wouldn't normally do.

Impersonation: Attackers impersonate legitimate individuals or entities, often using fake emails, phone calls, or websites to gain trust and credibility.

Urgency: Attackers create a sense of urgency to pressure victims into making hasty decisions, bypassing normal security protocols.

Scarcity: By creating a perception of limited availability, attackers entice victims to act quickly without careful consideration.

Baiting: Attackers offer something enticing (like a free software download) that contains malware, tricking victims into compromising their security.

Tailgating: Attackers physically follow authorized personnel into restricted areas by pretending to be part of the organization.

Phishing: Attackers send fraudulent emails or messages that appear legitimate, enticing recipients to click on malicious links or share sensitive information.

8. Investigate the different types of malware threats, such as viruses, worms, and Trojans, and explain their impact on network security. (L2, CO2)

Malware stands for malicious software designed to exploit devices, networks, or services. It includes viruses, worms, and Trojans.

Viruses:
Replicates by modifying other programs and inserting its own code. Successful replication results in "infection" of the affected areas. Can harm computers by deleting files, reformatting drives, or using up memory.

Worms:
Independent malware program that self-replicates to spread to other computers. Spreads through computer networks, capitalizing on security flaws. Doesn't need to attach to existing programs.
Typically causes harm to the network, consuming bandwidth.

Trojan Horses (Trojans):
Misleads users about its true intent. Named after the deceptive Trojan Horse from Greek mythology.
Spread through social engineering, tricking users into executing disguised attachments.

Impact and Risks:
Malware can steal sensitive data, disrupt networks, and damage or destroy data.

Protection Measures:

Implement strong security measures, such as firewalls and antivirus software. Regularly update systems and software to patch vulnerabilities. Educate employees on safe computing practices.

Each point provides a concise overview of the mentioned topics.

Rubrics :

Indicator	Average	Good	Excellent	Marks
Organization (2)	Readable with some mistakes and structured (1)	Readable with some mistakes and structured (1)	Very well written and structured (2)	
Level of content(4)	Minimal topics are covered with	Limited major topics with minor	All major topics with minor	

	limited information (2)	details are presented(3)	details are covered (4)	
Depth and breadth of discussion(4)	Minimal points with missing information (1)	Relatively more points with information (2)	All points with in depth information(4)	
Total Marks(10)				