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)

Aspect	OSI Model	TCP/IP Model
Layers	7 layers	4 layers
Layer Names	Physical, Data Link, Network, Transport, Session, Presentation, Application	Network Interface, Internet, Transport, Application
Granularity	More detailed, each layer has specific functions	Less detailed, layers encompass broader functions
Origins	Developed by the ISO (International Organization for Standardization)	Evolved from the ARPANET project
Adoption	Less commonly referenced in practice	Widely used as the basis for the internet's architecture
Significance	Provides a theoretical framework, helpful for understanding concepts and layer interactions	More directly reflects the structure of internet protocols and communication

Understanding these models helps in comprehending network communication by providing a structured way to conceptualize the various processes and protocols involved. While the OSI model is a theoretical model that aids in understanding how different layers interact, the TCP/IP model is a practical framework used to build and operate the internet. Both models offer valuable insights into network communication, albeit with varying levels of granularity and practical relevance.

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)**

Aspect	Vulnerability Assessment	Penetration Testing
Purpose	Identifies vulnerabilities in a system	Simulates real-world attacks to exploit vulnerabilities
Focus	Scans and identifies potential weaknesses	Actively exploits vulnerabilities to assess real-world impact
Depth	Less intrusive, identifies vulnerabilities	More aggressive, tests how vulnerabilities can be exploited
Example Tools	Nessus, OpenVAS, Qualys	Metasploit, Nmap, Burp Suite
Outcome	Provides a list of vulnerabilities	Evaluates the system's defense and response mechanisms
Frequency	Regular scans to monitor for changes	Occasional tests to evaluate preparedness

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 information (2)	Limited major topics with minor details are presented(3)	All major topics with minor 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)				