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)
2. Explain the process of IP addressing and routing in a computer network. How does routing protocol help in efficient data transmission? (L2, CO1)
3. Outline the key steps involved in ethical hacking and describe how these steps contribute to securing computer systems. (L2, CO1)
4. Compare and contrast the OSI model and the TCP/IP model, highlighting their significance in understanding network communication. (L2, CO1)
5. Explain the process of information gathering and reconnaissance in the context of network security. How can attackers exploit this phase? (L3, CO2)
6. Differentiate between vulnerability assessment and penetration testing. Provide examples of tools used for each of these processes. (L2, CO2)
7. Describe the key characteristics of social engineering attacks and discuss how organizations can educate their employees to prevent such attacks. (L2, CO2)
8. Investigate the different types of malware threats, such as viruses, worms, and Trojans, and explain their impact on network security. (L2, CO2)

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)				

Lisa Gonsalves 9607 TE CompsB
FR. CONCEICAO RODRIGUES COLLEGE OF ENGINEERING

CYBER SECURITY: ASSIGNMENT-1.

1)→ The TCP/IP protocol stack consists of several layers which have their responsibilities. They are as follows:

1. Application layer:- This layer is where user applications interact with the network.
   - Protocols like http FTP, SMTP & DNS operate here.
   - It provides a way for applications to communicate over the network.
2. Transport layer: This layer manages end-to-end communicat-ion and data flow control.
   - TCP ensures reliable, ordered and error-checked delivery of data.
   - UDP provides faster but less reliable communication.
3. Internet layer: - Also know as network layer, this layer handle the addressing and routing of data packet across interconnected networks.
   - IP is a key protocol here.
4. Link layer: This layer deals with the physical connection between devices on the same network.

- It encompasses protocols that handle hardware addressing (MAC addressing), frame creation & error detection.
- All these layers contribute to network functioning by breaking down complex tasks into manageable components.
- Each layer provides specific services while abstracting the complexities of lower layers, ensuring data transmission across diverse systems.

2] → • IP addressing and routing are crucial processes in computer networking that enable data to travel from a source to destination across interconnected networks.
- IP Addressing: In this an unique numerical label is assigned to devices on a network.
- Routing: Routing is the process of determining the best path for data packets travel from source to destination.
- When a data packet is sent from a source device, it contains the source and destination IP addresses.
- As the packet travels through routers, each router examines destination IP address and forwards it.
- This continues until the packet reaches the destination network.
- ~~These~~ Routing protocols help in efficient transmission in several ways like:
Dynamic Adaptation, Load Balancing, Redundancy & Reliability, Scalibility & Fast convergence.

3] → Steps of ethical hacking are as follows:

1. Reconnaissance: In this initial phase, ethical hackers gather as much ~~as~~ information as possible about the target system or organization. This includes identifying IP addresses, domain names, network topology, potential entry points, and other publicly available information.

2. Scanning: In this step, ethical hackers use various tools and techniques to scan the target system for open ports, services and vulnerabilities.

3. Enumeration: During this phase, the ethical hacker further probes the target system to obtain detailed information about users, shares & services.

4. Vulnerability Assessment: In this step, the ethical hackers analyzes the information collected during scanning and enumeration to identify potential vulnerabilities & weakness in the target system.

5. Gaining access: Once potential

vulnerabilities are identified, ethical hackers attempt to exploit them to gain unauthorized access to the target system.

6. Maintaining Access: After gaining initial access, ethical hackers work to maintain a foothold in the target system.

7. Covering tracks: In the ethical hacking process, the goal is to leave no traces behind to avoid detection by the target organization.

8. Reporting: After completing the assesment, ethical hackers compile a comprehensive report detailing their findings, including identified vulnerabilities, potential risks and recomended remediation steps.

9. Post-Mortem Analysis: This step involves conducting a debriefing session with the organization to discuss the result of the ethical hacking engagement.

4) →

OSI Model	TCP/IP Model
• Consist of seven layers, providing a detailed breakdown of network functionality.	• Compromises four layers, offering a more streamlined approach to network communication.
• Has 3 distinct layers that correspondence to TCP/IP Application layers.	• Combine functionalities of these 3 OSI layers into its Application layers.
• Developed by the ISO as a universal reference model, with a more theoretical approach.	• Originated from the architecture of ARPANE and is the foundation of the internet's structu
• Less commonly used as a practical framework for networking, mainly used for conceptual teaching.	• Widely used in networking implementat--ions and closely align with how the internet function.

5) → • Information gathering and reconnaissance, also known as the initial phase of a cyberatt--acks, involve the collection of data about a target network or system to identify vulnerabilities and potential entry points.

- This phase aids attackers in crafting a well-informed strategy for subsequent attacks.

The process typically entails:

1. Passive Data collection: Attackers gather publicly available information, such as domain names, IP addresses, and organizational details, using tools like search engines and social media.
2. Network Mapping: Attackers identify active devices, open ports, and services using tools like Nmap, aiding in understanding the network's layout and potential weakness.
3. DNS Enumeration: Attackers ~~identify active~~ extract domain-related information through DNS queries, revealing potential subdomains and mail server details.
4. WHOIS Lookup: Attackers use WHOIS database to acquire ownership and contact information for domains, which might help in social engineering attacks.
5. Social Engineering: Attackers leverage public sources to craft convincing phishing emails or craft tailored attacks that exploit personal information.

- Attackers exploit this phase by combining collected data to craft precise attack strategies.
- For instance, using gathered emails addresses and organization details, attackers might send spear-phishing emails loaded with malware.

- By identifying outdated software versions, attackers can focus on exploiting known vulnerabilities.
- Furthermore, the reconnaissance phase might expose weak points, allowing attackers to manipulate human psychology through social engineering.
- Ultimately, the information gathered serves as a blueprint, for attackers, enabling them to plan attacks that are more targeted, successful and difficult to detect.

6) → • Vulnerability Assessment and Penetration Testing are key elements in cybersecurity.

• VULNERABILITY ASSESSMENT :

- The purpose of this process is to identify vulnerabilities and weakness in system networks or applications.
- It scans and analyzes for known vulnerabilities and misconfigurations.
- It provides a report highlighting the severities.
- This process is conducted regularly to maintain security readiness.
- Eg. of tools : Nessus, OpenVAS, Qualys, Nexpos

PENETRATION TESTING:

- This process simulates real-world attacks to evaluate system resistance.
- It exploits vulnerabilities to assess impact & extent of compromise.
- It produces a detailed report with exploited vulnerabilities and outcomes.
- This process is conducted periodically or after significant changes
- Eg of tools: Metasploit, Nmap, BurpSuite.

- In a vulnerability assesment, outdated software on a web server might be found, while in penetration testing, the testor would exploit it to showcase potential consequence, highlighting the differing scope of these practices.
- Both processes are crucial for robust security.

7) → • Social engineering attacks are manipulative tactics used by malicious actors to deceive individuals into divulging confidential information or granting access.
- Key characteristics include exploiting human psychology, leveraging trust and relying on manipulation rather than technical exploits.
- To prevent such attacks organization can implement effective employee education. Strategies:

1. Awareness Program: Regularly conduct training session to raise awareness about common social engineering tactics, such as phishing and pretexting.
2. Simulated Attacks: Run mock social engineering campaigns to expose employees to real life scenarios without actual risks, helping them recognize suspicious behaviors.
3. Phishing Training: Teach employees to identify phishing emails by scrutinizing sender details, URLs and attachments.
4. Multi-Factor Authentication: Promote the use of MFA for accessing sensitive systems, reducing the effectiveness of stolen credentials.
5. Clear Policies: Develop and communicate clear security policies, emphasizing the importance of not sharing sensitive information.

8) → • Viruses are malicious programs that attach themselves to legitimate files or software.
• They spread when infected files are executed.
• Worms are self-replicating malware that spread over networks, exploiting vulnerabilities to infect other systems.

- Unlike viruses, they don't need a host file to propagate
- Trojans are disguised as legitimate software but contain malicious code.
- Trojans often rely on social engineering to trick users into installing them.
- These impact network security in the following ways:

1- Data can be breached as malware can steal sensitive data which can lead to privacy violation.

2. Malware can disrupt network services and operations, causing downtime and loss.

3- Worms can rapidly spread across networks, overwhelming systems and clogging network traffic.

4. Malware can lead to financial theft, fraud, etc impacting both individuals & organizations

5. Some malware can corrupt/delete data causing permanent loss and impacting productivity.