SOMAIYA VIDYAVIHAR UNIVERSITY

Semester: Jan 2025-April 2025 **Maximum Marks: 30** **Examination: Lab CA Examination** **Duration :1 Hr.**		
Programme code: **Programme:**	**Class:** SY	**Semester:**IV
Name of the Constituent College: **K. J. Somaiya College of Engineering**	**Name of the department:** COMP/ETRX/EXTC/IT/MECH	
Course Code:	**Name of the Course:VAPT**	

Question No.		Max. Marks
Q1	Discuss in detail steps to exploit the client-side vulnerability to gain access to the target machine.	5
Q2	A company's cybersecurity team wants to train employees on the dangers of using weak passwords. Give a detailed plan to the company's cybersecurity team for mentioned training.	5
Q3	Discuss the role of Kali Linux in phases of penetration testing.	5
Q4	Write down steps to identify a known vulnerability in a target system, such as an outdated version of a service using nmap.	5
Q5	If hashed passwords are found, list John Reaper's steps.	5

Roll No : 16010423076

Batch : SY-IT(B3)

Answers

1) To exploit a client-side vulnerability, the below steps are followed in a sequential manner

Scanning : Properly define the target assets and conduct a preliminary research about the factors which would be involved in the attack.

Reconnaisance : In military terms the word Reconnaisance means to conduct a physical survey of the target locations before launching an offensive attack. But in digital terms it purely refers to conducting a deep scan of the target devices and its assets. This has two types :

1) Passive Reconnaisance : In this type of recon, the attacker does not interact with the target directly. The objectives of active recon are to gather all publicly available information about the target using dorking, social media scans, etc.

2) Active Reconnaisance : Here the attacker engages with the target directly. The objectives of active recon are to find open ports, services, etc using tools such as nmap, netcat etc.

Exploitation : This is the stage where the payload is delivered to the target to exploit the known vulnerabilities from the previous scanning stages.

Gaining access : In this stage, the access to the target machines, servers, applications is gained. Privilege escalation is also involved in this stage of exploitation.

Maintaining access : Once the access is gained, it needs to be maintained for easy futures access or daisy chaining attacks. This includes covering the attack trails and also creating backdoor channels for further access.

2)

Weak passwords are a big threat to security.

Strong passwords : One must use a combination of letters, numbers and special characters and not keep the password plain in either of the three formats.

Multi-factor authentication : Even if someone obtains your password and tries to log into your accounts they are stopped at this stage and the system is not compromised.

Non-reuable passwords : If a person needs to change their passwords, they need to change it completely and not repeat using any of the passwords which they have used previously.

Fixed time period to change passwords : All the passwords need to be changed mandatorily after a certain time period to improve hygiene.

Being aware of threats : Various threats such as keyloggers, Social engineering etc

3) Kali-linux is a debian based operating system which is developed and maintained by Offensive Security group. It is widely used in the field of cybersecurity at various stages of penetration testing.

Reconnaissance: Kali Linux provides various pre installed tools such as nmap and netcat which are used in recon. In military terms the word Reconnaisance means to conduct a physical survey of the target locations before launching an offensive attack. But in digital terms it purely refers to conducting a deep scan of the target devices and its assets.

Scanning and Enumeration : Scanning is the process of gathering information and enumeration is the process of listing all the available services about a given target. Kali provides a series of tools in the process of Scanning and enumeration.

Exploitation: When a vulnerability is found out, it is used to gain access to the target machine and this process is called exploitation.

Post-Exploitation: After a system is exploited, there are a few steps which follow the exploitabtion and these steps include privilege escalation and maintain access, this can be performed using Kali by making use of backdoor channels or rootkits.

Reporting: In Vulnerability assessment and Penetration testing, reporting is one of the most crucial aspects. Any security test which is performed by Cyber security professionals is performed after taking due permission and hence it becomes very important to document and report

everything. Kali also provides various tools which help in visualizing and document all the information about a pen-test.

4) To identify a known vulnerability in a target system nmap or network mapper tool is used as it provides a series of scans which can be used to identify open ports, vulnerabilities, application versions, operating systems, etc.

The below two commands are used to identify a vulnerability related to outdated version of a service :

- Command : nmap -sV {targetipaddr}
- Command : nmap --script=vuln {targetipaddr}

5) The passwords which we use for our various online accounts are not stored as they are, but security measures are installed in place to protect those accounts from being used by unauthorized people. These passwords are ofter hashed (md5, sha-1, etc), salted, etc before being stored in databases or other storage devices. Password Cracking is the method of decrypting these hashes to obtain the original passwords as they were kept. Sofwares such as John the Reaper and Hydra are used for this purpose.

If hashed passwords are obtained, they can be cracked using the below steps.

- Download the zip file of John the Reaper from its website.
- Extract that zip file of John the Reaper.
- Open terminal
- Command prompt for example
- Run the command : john
- to check if the software has been installed properly
- Create a file containing the hashed md5 passwords and save it in '.txt' format.
- Run Command : john.exe --format=raw-md5 CompleteFileDirectory\example.txt
- The decrypted plaintext password of the given hash will be displayed

1. A hacker uses nc -zv 192.168.1.5 1-1000 to check open ports. What steps must the hacker have executed?

- Identified the target and its IP address.
- Defined target ports to scan
- They have installed netcat
- It will scan the ports to perform active reconnaissance and find vulnerabilitie
- The ports which it will scan are 1-1000