Postgraduate Certificate in Cybersecurity Risk Management

Ethical Hacking and Penetration Testing

Ethical Hacking and Penetration Testing are important concepts in the field of cybersecurity. In this explanation, we will cover key terms and vocabulary related to these concepts that are relevant to the Postgraduate Certificate in Cybersecurity Risk Management.

1. Ethical Hacking

Ethical Hacking, also known as White Hat Hacking, is the practice of penetrating a system or network with the permission of its owner to identify vulnerabilities and weaknesses that an attacker could exploit. Ethical hackers follow a code of ethics and are authorized to conduct their activities.

2. Penetration Testing

Penetration Testing, also known as Pen Testing, is the process of evaluating the security of a system or network by simulating an attack. Pen testing can be automated or manual and is used to identify vulnerabilities and weaknesses that an attacker could exploit.

3. Vulnerability

A vulnerability is a weakness in a system or network that could be exploited by an attacker to gain unauthorized access or perform unauthorized actions. Vulnerabilities can be caused by outdated software, misconfigured systems, or human error.

4. Exploit

An exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a vulnerability in a system or network to cause unintended or unanticipated behavior to occur. Exploits can be used to gain unauthorized access, escalate privileges, or perform other malicious actions.

5. Zero-Day Vulnerability

A zero-day vulnerability is a previously unknown vulnerability in a system or network that has not yet been patched. Zero-day vulnerabilities are particularly dangerous because attackers can exploit them before defenders have a chance to mitigate the risk.

6. Payload

A payload is the part of an exploit that performs the malicious action. For example, a payload might install malware, steal data, or delete files.

7. Social Engineering

Social engineering is the practice of manipulating people into performing actions or divulging confidential

information. Social engineering attacks can take many forms, including phishing emails, phone calls, and in-person interactions.

8. Phishing

Phishing is a type of social engineering attack that involves sending emails or messages that appear to be from a trusted source, such as a bank or a social media platform. The message typically contains a link that leads to a fake website, where the victim is tricked into entering their login credentials or other sensitive information.

9. Spear Phishing

Spear phishing is a more targeted form of phishing that involves tailoring the message to the victim. Spear phishing attacks often use personal information, such as the victim's name or job title, to make the message appear more legitimate.

10. Whaling

Whaling is a type of spear phishing attack that targets high-level executives or other high-value targets. Whaling attacks often use sophisticated tactics, such as spoofing email addresses or impersonating trusted colleagues.

11. Malware

Malware is short for malicious software. Malware is any software that is designed to harm a system or network, steal data, or perform other malicious actions. Examples of malware include viruses, worms, Trojans, and ransomware.

12. Ransomware

Ransomware is a type of malware that encrypts the victim's files and demands a ransom payment in exchange for the decryption key. Ransomware attacks can be devastating, resulting in the loss of critical data and significant downtime.

13. Denial of Service (DoS) Attack

A denial of service (DoS) attack is an attempt to make a system or network unavailable by overwhelming it with traffic or other requests. DoS attacks can be launched using a single computer or a network of compromised computers, known as a botnet.

14. Distributed Denial of Service (DDoS) Attack

A distributed denial of service (DDoS) attack is a type of DoS attack that uses a network of compromised computers to overwhelm the target system or network. DDoS attacks can generate massive amounts of traffic, making them difficult to mitigate.

15. Passive Reconnaissance

Passive reconnaissance is the process of gathering information about a target system or network without actively interacting with it. Passive reconnaissance techniques include searching public databases, social media profiles, and domain registration information.

16. Active Reconnaissance

Active reconnaissance is the process of gathering information about a target system or network by actively interacting with it. Active reconnaissance techniques include port scanning, ping sweeping, and vulnerability scanning.

17. Port Scanning

Port scanning is the process of probing a target system or network to identify open ports. Open ports can be used by attackers to gain unauthorized access or perform unauthorized actions.

18. Ping Sweeping

Ping sweeping is the process of sending ping requests to a range of IP addresses to identify which ones are alive and responding. Ping sweeping can be used to identify potential targets for further reconnaissance or attack.

19. Vulnerability Scanning

Vulnerability scanning is the process of using automated tools to identify vulnerabilities in a target system or network. Vulnerability scanning can help ethical hackers and penetration testers identify weaknesses that could be exploited by attackers.

20. Exploitation Framework

An exploitation framework is a tool that provides a structured approach to exploiting vulnerabilities in a target system or network. Exploitation frameworks typically include a library of exploits, payloads, and other tools that can be used to automate the exploitation process.

21. Metasploit

Metasploit is an open-source exploitation framework that is widely used by ethical hackers and penetration testers. Metasploit includes a large library of exploits and payloads, as well as tools for automating the exploitation process.

22. Burp Suite

Burp Suite is a popular penetration testing tool that includes a range of features for testing web applications. Burp Suite can be used to identify vulnerabilities, intercept and modify HTTP requests, and automate various aspects of the penetration testing process.

23. OWASP Top Ten

The OWASP Top Ten is a list of the ten most critical web application security risks, as identified by the Open Web Application Security Project (OWASP). The OWASP Top Ten includes risks such as injection attacks, broken authentication and session management, and cross-site scripting (XSS).

24. Common Vulnerability Scoring System (CVSS)

The Common Vulnerability Scoring System (CVSS) is a standardized framework for assessing the severity of vulnerabilities in software. CVSS scores are based on various factors, including the potential impact of the vulnerability, its ease of exploitation, and the availability of mitigations.

25. Certified Ethical Hacker (CEH)

The Certified Ethical Hacker (CEH) is a professional certification offered by the EC-Council. The CEH certification is designed to validate the skills and knowledge of ethical hackers and penetration testers.

Challenge:

Now that you have a better understanding of the key terms and vocabulary related to ethical hacking and penetration testing, try using them in a sentence or two. For example:

* During a recent penetration test, our team used a vulnerability scanning tool to identify potential weaknesses in the target system, and then used Metasploit to exploit those vulnerabilities and gain unauthorized access.
* To protect against social engineering attacks, it's important to educate employees about the risks of phishing emails and other common tactics used by attackers.
* The Common Vulnerability Scoring System (CVSS) is a valuable tool for assessing the severity of vulnerabilities and prioritizing remediation efforts.

Remember, ethical hacking and penetration testing are important skills in the field of cybersecurity. By understanding key terms and concepts, you can help protect systems and networks from attackers and keep sensitive data secure.