Postgraduate Certificate in Network Security

Ethical Hacking

Ethical Hacking is a crucial aspect of cybersecurity that involves the authorized testing of computer systems and networks to identify and address potential vulnerabilities. It is a proactive approach to cybersecurity that helps organizations strengthen their security posture by simulating real-world cyber attacks. In this course, we will explore key terms and vocabulary related to Ethical Hacking to deepen your understanding of this field.

1. Ethical Hacking:
Ethical Hacking, also known as penetration testing or white-hat hacking, is the practice of identifying and exploiting vulnerabilities in a system or network with the permission of the owner. The goal of ethical hacking is to improve the security of the target system by identifying weaknesses that malicious hackers could exploit.

2. Penetration Testing:
Penetration testing is a controlled form of hacking where cybersecurity professionals simulate real-world attacks to assess the security of a system. It involves identifying vulnerabilities, exploiting them, and providing recommendations for remediation.

3. Vulnerability Assessment:
Vulnerability assessment is the process of identifying, quantifying, and prioritizing vulnerabilities in a system. It helps organizations understand their security risks and take appropriate measures to mitigate them.

4. Exploitation:
Exploitation refers to the act of taking advantage of a vulnerability to gain unauthorized access to a system or network. Ethical hackers use exploitation techniques to demonstrate the impact of vulnerabilities and help organizations improve their defenses.

5. Social Engineering:
Social engineering is a technique used by hackers to manipulate individuals into divulging confidential information or performing actions that compromise security. Ethical hackers often use social engineering to test the human element of cybersecurity defenses.

6. Phishing:
Phishing is a type of social engineering attack where attackers send deceptive emails or messages to trick recipients into revealing sensitive information, such as login credentials or financial data. Ethical hackers may use phishing simulations to assess an organization's susceptibility to such attacks.

7. Malware:
Malware is malicious software designed to infiltrate and damage a computer system. Ethical hackers study

malware to understand how it works and develop strategies to defend against it.

8. Backdoor:
A backdoor is a hidden entry point into a system that allows unauthorized access without going through normal authentication procedures. Ethical hackers often look for backdoors in systems to test their security controls.

9. Firewall:
A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Ethical hackers may test firewalls to identify misconfigurations or vulnerabilities that could be exploited by attackers.

10. Intrusion Detection System (IDS):
An Intrusion Detection System is a security tool that monitors network or system activities for malicious activities or policy violations. Ethical hackers may attempt to bypass IDS to test its effectiveness in detecting and responding to threats.

11. Cryptography:
Cryptography is the practice of securing communication by converting plain text into unintelligible ciphertext using algorithms. Ethical hackers study cryptography to understand how encryption works and assess the strength of cryptographic implementations.

12. Encryption:
Encryption is the process of encoding information to make it unreadable without the decryption key. Ethical hackers use encryption to protect sensitive data and test the security of encryption algorithms.

13. Digital Forensics:
Digital forensics is the process of collecting, preserving, and analyzing digital evidence to investigate cybercrimes or security incidents. Ethical hackers may use digital forensics techniques to gather evidence during penetration tests.

14. Zero-Day Vulnerability:
A zero-day vulnerability is a security flaw in a software or hardware that is unknown to the vendor and has no available patch. Ethical hackers may discover zero-day vulnerabilities and work with vendors to develop fixes before they are exploited by malicious actors.

15. Metasploit:
Metasploit is a popular penetration testing framework that provides tools for developing, testing, and executing exploit code against target systems. Ethical hackers use Metasploit to automate tasks and streamline the penetration testing process.

16. Port Scanning:
Port scanning is the process of scanning a computer or network for open ports to identify potential entry points for attackers. Ethical hackers use port scanning tools to assess the security of a system and identify vulnerabilities.

17. SQL Injection:
SQL Injection is a type of attack where malicious SQL code is inserted into a web application's input fields to manipulate the database. Ethical hackers test for SQL Injection vulnerabilities to prevent attackers from compromising sensitive data.

18. Cross-Site Scripting (XSS):
Cross-Site Scripting is a vulnerability that allows attackers to inject malicious scripts into web pages viewed by other users. Ethical hackers test for XSS vulnerabilities to prevent client-side attacks and protect user data.

19. Denial of Service (DoS) Attack:
A Denial of Service attack is a malicious attempt to disrupt the normal functioning of a network or website by overwhelming it with a high volume of traffic. Ethical hackers may conduct DoS attacks to test an organization's resilience against such threats.

20. Red Team vs. Blue Team:
In cybersecurity, the Red Team represents attackers, while the Blue Team represents defenders. Red Team exercises simulate real-world attacks, while Blue Team exercises focus on defending against them. Ethical hackers may play different roles in Red Team and Blue Team activities to enhance security preparedness.

By familiarizing yourself with these key terms and concepts in Ethical Hacking, you will be better equipped to navigate the challenges and opportunities in the field of network security. Ethical hacking plays a crucial role in protecting organizations from cyber threats and ensuring the confidentiality, integrity, and availability of their data and systems.