CEH Complete Course

Duration: 30 days
Class Duration: 1.5 hours per day
Structure:

- **Covers all 20 CEH modules**
- **Each module approximately 1 to 1.5 hours with practical demos and Q&A**
- **Includes hands-on labs spread throughout the course**
- **Final days dedicated to revision and practice tests**

1. Introduction to Ethical Hacking

Overview of ethical hacking, its goals, legal implications, and the different types of hackers (white hat, black hat, gray hat). Understanding the hacking process and methodology.

2. Footprinting and Reconnaissance

Techniques for gathering information about a target system or organization, such as DNS queries, WHOIS lookups, and social engineering, to build a profile for attacks.

3. Scanning Networks

Methods to discover active devices, open ports, and services on a network using tools like Nmap and Netcat. Identifying live hosts and potential vulnerabilities.

4. Enumeration

Extracting detailed information such as usernames, machine names, and shares from systems to identify potential points of attack.

5. Vulnerability Analysis

Identifying weaknesses in systems and networks using automated tools and manual techniques to assess potential security gaps.

6. System Hacking

Steps hackers use to gain unauthorized access, escalate privileges, maintain access, and cover tracks on compromised systems.

7. Malware Threats

Understanding different types of malware (viruses, worms, Trojans, ransomware), their propagation methods, and how to detect and prevent them.

8. Sniffing

Capturing and analyzing network traffic to intercept sensitive information using tools like Wireshark and tcpdump.

9. Social Engineering

Psychological manipulation techniques used to trick users into revealing confidential information or granting access.

10. Denial-of-Service (DoS)

Attacks designed to overwhelm and disrupt services, including flood attacks and methods to detect and mitigate DoS attacks.

11. Session Hijacking

Techniques to take over active sessions between a user and a service, including stealing session tokens and cookies.

12. Evading IDS, Firewalls, and Honeypots

Methods attackers use to bypass security measures such as Intrusion Detection Systems and firewalls to avoid detection.

13. Hacking Web Servers

Exploiting vulnerabilities in web servers to gain unauthorized access or cause disruption.

14. Hacking Web Applications

Attacking web applications through flaws like cross-site scripting (XSS), SQL injection, and others.

15. SQL Injection

A specific attack targeting databases by injecting malicious SQL code to manipulate or retrieve data.

16. Hacking Wireless Networks

Techniques to attack Wi-Fi networks, crack encryption, and exploit weaknesses in wireless protocols.

17. Hacking Mobile Platforms

Security issues and attack methods related to smartphones and tablets, including app vulnerabilities and OS exploits.

18. IoT Hacking

Understanding vulnerabilities in Internet of Things devices and how to exploit or protect them.

19. Cloud Computing

Security challenges unique to cloud environments and techniques to protect cloud resources.

20. Cryptography

Basics of encryption, hashing, digital signatures, and how cryptography is used to secure data.