Ethical Hacking Advanced

Module 1: Introduction to Ethical Hacking

- **Overview:** What is ethical hacking, and why is it important?
- **Ethics and Legality:** Understanding the ethical and legal implications of hacking.
- **Setting Up the Hacking Environment:** Installing necessary software like Kali Linux, configuring virtual machines, and ensuring a safe practice environment.

Module 2: Network Scanning and Reconnaissance

- **Tools Featured:** Nmap, Zenmap
- **Objectives:** Learn to identify live hosts, open ports, and services running on servers.
- **Practical Lab:** Scanning a network to map out the network structure.

Module 3: Vulnerability Assessment

- **Tools Featured:** Nessus, OpenVAS
- **Objectives:** Understanding vulnerability scanning concepts and interpreting scan results.
- **Practical Lab:** Conducting scans to identify and report vulnerabilities.

Module 4: Web Application Security

- **Tools Featured:** OWASP ZAP, sqlmap, Nikto
- **Objectives:** Testing web applications for vulnerabilities such as SQL injection, XSS, and CSRF.
- **Practical Lab:** Attacking a dummy web application to practice web exploits.

Module 5: System Hacking

- **Tools Featured:** Metasploit, John the Ripper
- **Objectives:** Gaining access to systems and escalating privileges.
- **Practical Lab:** Using Metasploit to exploit known vulnerabilities and crack passwords.

www.urbancode.in

Module 6: Network Traffic Analysis

- **Tools Featured:** Wireshark, Tcpdump
- **Objectives:** Capturing and analyzing network packets.
- **Practical Lab:** Monitoring network traffic to detect malicious activities.

Module 7: Wireless Security

- **Tools Featured:** Aircrack-ng, Reaver, Wifiphisher
- **Objectives:** Understanding Wi-Fi security protocols and breaking WEP/WPA2.
- **Practical Lab:** Cracking a Wi-Fi password and setting up an Evil Twin attack.

Module 8: Social Engineering and Phishing Attacks

- **Tools Featured:** Social-Engineer Toolkit (SET), GoPhish
- **Objectives:** Crafting effective social engineering campaigns and phishing attacks.
- **Practical Lab:** Setting up a phishing page and conducting a mock phishing attack.

Module 9: Anonymity and Privacy

- **Tools Featured:** Tor, Proxychains, VPNs
- **Objectives:** Techniques to maintain anonymity online.
- **Practical Lab:** Configuring Tor and VPNs to anonymize your digital footprint.

Module 10: Forensics and Incident Response

- **Tools Featured:** Autopsy, GRR
- **Objectives:** Basic concepts of digital forensics and conducting an incident response.
- **Practical Lab:** Analyzing forensic images and responding to a data breach simulation.

www.urbancode.in