Duration: 2 Months

ADVANCE ETHICAL HACKING

Overview:

The Advance Ethical Hacking program is the most desired information security training program for any information security professional or cyber security enthusiast will ever want to be in. To master the hacking technologies, you will need to become one, but an ethical one. The course provides the advanced hacking tools and techniques used by hackers and information security professionals alike to break into an organization. As we put it, “To beat a hacker, you need to think like a hacker”.

What you’ll learn

➢In Advanced Ethical Hacking, you will delve into sophisticated techniques used by ethical hackers to uncover and exploit security vulnerabilities in systems and networks.

➢ This includes mastering advanced penetration testing methodologies, evasion techniques, and post-exploitation strategies.

➢Additionally, you will learn about the latest tools and tactics employed by attackers, enabling you to develop robust defensive measures to safeguard against cyber threats effectively.

➢To simulate real-world cyberattacks and strengthen defensive capabilities.

Benifits

➢**Hands-on practical:** Engage in real-world exercises to apply theoretical knowledge directly.

➢**Internship opportunity:** Gain practical experience through internships to enhance skills and build a professional network.

➢**Expert trainers:** Receive guidance and instruction from seasoned professionals with extensive experience in the field.

➢**Job assistance:** Access support and resources to secure employment opportunities aligned with acquired skills. and expertise.

You can reach us at:

www.cyberous.in
info@cyberous.in
cyberous_
cyberous

Course Outline:

Module 01: Ethical Hacking Fundamentals

- Ethical concepts
- Legal considerations
- Distinction from malicious hacking

Module 02: Footprinting and Reconnaissance

- Information gathering
- OSINT tools
- Footprinting methodologies

Module 03: Scanning Networks

- Port scanning
- Network mapping
- Vulnerability scanning

Module 04: Enumeration

- Service enumeration
- User enumeration
- SNMP enumeration

Module 05: System Hacking

- Exploiting vulnerabilities
- Privilege escalation
- Password cracking

Module 06: Malware Threats

- Types of malware
- Malware analysis
- Antivirus evasion

Module 07: Sniffing and Spoofing

- Packet sniffing
- ARP/DNS spoofing
- Sniffing tools

Module 08: Social Engineering

- Psychological manipulation
- Phishing
- Social engineering toolkits

Module 09: Web Application Hacking

- SQL injection
- XSS
- Session hijacking

Module 10: Wireless Network Hacking

- WLAN security
- Cracking keys
- Rogue APs

Module 11: Evading IDS, Firewalls, Honeypots

- IDS evasion
- Firewall evasion
- Honeypot detection

Module 12: Cryptography

- Encryption algorithms
- Cryptanalysis
- Steganography

Module 13: Penetration Testing Methodologies

- Planning
- Execution
- Reporting

Module 14: Post-Exploitation Techniques

- Maintaining access
- Covering tracks
- Pivoting

Module 15: IoT Hacking

- Device vulnerabilities
- Exploitation.
- Penetration testing

Module 16: Cloud Computing Security

- Cloud infrastructure flaws
- AWS/Azure/GCP security
- Cloud pen testing

Module 17: Mobile Application Hacking

- Android/iOS security
- Reverse engineering
- Exploiting vulnerabilities

Module 18: Physical Security

- Social engineering attacks
- Lock picking
- Physical security audits

Module 19: Red Team Operations

- Simulating attacks
- Covert ops
- Adversarial tactics

Module 20: Ethical Hacking Best Practices

- Responsible disclosure
- Continuous learning
- Upholding ethical standards