INTRODUCTORY ETHICAL HACKING COURSE FOR BEGINNERS:

Week 1: Introduction to Ethical Hacking

- What is ethical hacking?
- Understanding the different types of hackers
- Legal and ethical considerations in ethical hacking
- Overview of common security threats and vulnerabilities

Week 2: Footprinting and Reconnaissance

- Understanding the importance of reconnaissance
- Techniques for gathering information about a target
- Analyzing and organizing data

Week 3: Network Scanning and Enumeration

- Pre-scanning considerations
- Techniques for scanning networks
- Enumerating network services and vulnerabilities

Week 4: System Hacking

- Overview of password attacks
- Gaining access to systems
- Maintaining access with backdoors and rootkits

Week 5: Social Engineering

- Understanding social engineering attacks
- Techniques for phishing and pretexting
- Mitigating social engineering attacks

Week 6: Web Application Testing

- Understanding web vulnerabilities
- Testing for vulnerabilities in web applications
- Exploring web-based attack vectors

Week 7: Wireless Network Hacking

- Overview of wireless networks and attacks
- Hacking Wi-Fi networks
- Mitigating wireless network attacks

Week 8: Cryptography

- Introduction to cryptography
- Understanding encryption and decryption techniques
- Cryptanalysis: breaking codes and ciphers

Week 9: Ethical Hacking: Tools and Techniques

- Essential tools for ethical hacking
- Introduction to Kali Linux
- Configuring and using popular ethical hacking tools

Week 10: Final Project

Students will apply the knowledge and skills they have developed throughout the course to complete a final project, such as a penetration testing report or simulated security assessment.

Note: It is important to stress the legal and ethical considerations in ethical hacking throughout the course, as well as the

importance of obtaining permission before performing any type of security testing.