ϟ ETHICAL HACKING s CYBERSECURITY COURSE SYLLABUS

Module 1: Introduction to Ethical Hacking s Cybersecurity

1. What is Cybersecurity
2. What is Hacking (Theory Awareness)
3. Who are Hackers (Classification Awareness)
4. Skills required in Cybersecurity
5. Common motives behind cyber attacks
6. Who is at risk of cyber threats
7. Information Security Principles: Confidentiality, Integrity C Availability
8. What is Ethical Hacking
9. Need and Importance of Ethical Hacking C Cybersecurity
10. Scope C Legal Boundaries of Ethical Hacking C Cybersecurity
11. Introduction to Penetration Testing
12. Setting up Virtual Machines and Kali Linux (Lab Environment Only)
13. Case studies on cybersecurity incidents
14. Security importance in digital world
15. Cybersecurity as a Career
16. Top Cybersecurity Certifications
17. Popular cybersecurity job roles, requirements C salary expectations
18. History of major cybersecurity events

Module 2: Basics of Networking

19. Introduction to Internet Protocol
20. Types of IP (Public, Private, Static, Dynamic)
21. Ports and Services
22. Understanding Protocols
23. Operating Systems for different platforms

24. Key cybersecurity terms (Vulnerability, Exploit)
25. Programming languages used in cybersecurity
26. What are Networks and the concept of Networking
27. Network Topologies
28. Networking Devices (Hub, Switch, Router)
29. How networking devices communicate
30. Building secure testing environments
31. Basic Windows/Linux commands
32. Introduction to Kali Linux
33. CIA Triad

Module 3: Footprinting (Information Gathering)

34. What is Footprinting
35. Objectives of Footprinting
36. Public OSINT methods for gathering organization details
37. Domain and WHOIS lookup
38. Identifying public URLs and subdomains
39. Understanding server information (Public data only)
40. DNS information gathering
41. Identifying publicly listed services
42. Approximate geolocation awareness of servers
43. Email tracking awareness
44. Legal OSINT C footprinting tools

Module 4: Network Scanning (Lab Simulation)

45. What is Network Scanning
46. Objectives of scanning
47. Identifying active systems (Lab-based demonstration)

48. Identifying open ports (Theory + Simulation)
49. Identifying running services
50. Nmap overview
51. Zen map overview
52. Metasploit framework introduction
53. OS fingerprinting awareness
54. Vulnerability scanning concepts
55. Nessus vulnerability assessment tool
56. Understanding vulnerability reports

Module 5: Network Sniffing (Security Monitoring Awareness)

57. What is Packet Sniffing
58. How sniffing works
59. Types of sniffing (Active vs Passive)
60. Wireshark introduction
61. Common network monitoring tools like Driftnet C Darkstat
62. Ethical use cases in audits

Module 6: Malware Awareness

63. What is Malware
64. Categories of Malware
65. What is a Computer Virus (Awareness only)
66. Malware behaviour and propagation
67. Types of computer viruses
68. Malware prevention techniques
69. What is a worm
70. What is a Trojan
71. Spyware awareness

72. What are Rootkits
73. Defending against malware threats

Module 7: Denial of Service (DoS) Awareness

74. What is DoS
75. What is DDoS
76. Signs of DDoS attacks
77. Awareness of common attack patterns (Theory only)
78. Botnet concept
79. Preventing and mitigating DoS/DDoS attacks
80. Safe simulated demonstration tools

Module 8: Hardware-Based Cybersecurity (Awareness Overview)

81. Introduction to hardware used in cybersecurity labs
    a. OMG Cable
    b. Flipper Zero
    c. Card Cloners
    d. USB Rubber Ducky
    e. Raspberry Pi
    f. Hack-RF
    g. Wifi Jammer
    h. Blade RF
    i. Skimmer
82. Wireless security devices (awareness only)
83. Signal auditing concepts
84. Microcomputer platforms for cybersecurity education
85. Radio-frequency testing awareness

Module G: Social Engineering Awareness

86. What is Social Engineering
87. Phishing awareness
88. How victims are manipulated
89. Safe phishing simulation tools (Training environment only)
90. Difference between fake and genuine webpages
91. Prevention techniques and best practices

Module 10: Web Application Security

92. Introduction to Web Application Security
93. OWASP Top 10 Vulnerabilities
94. OWASP ZAP Overview
95. Burp Suite Overview
96. Safe vulnerable environments (DVWA / OWASP BWA)

Module 11: Cryptography s Steganography

97. Introduction to Cryptography
98. Hashing Algorithms
99. Hash Functions
100. Encryption techniques
101. Secure email concepts
102. What is Steganography
103. Data hiding demonstration awareness
104. Use of EXIF metadata tools

Module 12: IDS, IPS, Cloud s IoT Overview

105. What is IDS
106. What is IPS

107. IAAS, PAAS, SAAS models in cloud computing

108. Introduction to IoT C related cybersecurity challenges

Module 13: Web Server Security

109. Web Server Fundamentals

110. Robots.txt

111. Web Server Vulnerability Assessment by nikto

112. Web server bruteforcing for directory listing issues

113. Dirb & Dirbuster tool in kali Linux for webserver Pen testing