Certified Ethical Hacker (CEH v13), Videos & Skill Labs Set

Course Specifications

Course Number: ACI77-013VL_rev1.0
Video and Lab Length: Approximately 31 hours, 23 minutes

Course Introduction

Progressing across the CEH domains while incorporating Ai assisted techniques for reconnaissance, vulnerability analysis, exploitation concepts, web attacks, cloud concepts, and cryptography—this lab set is ideal for CEH-aligned skill-building.

Video Enhanced Learning

(15h 23m * 21 Modules * 139 Episodes)

We've enhanced select lab sets with targeted video content to strengthen student readiness and improve lab success. With focused video learning, students get reinforcement of core concepts before they enter the lab, giving them the confidence and context needed to apply skills effectively. Support diverse learning styles, improve lab readiness, and drive stronger outcomes across today's most in-demand skills.

Video Topics

1. Certified Ethical Hacker Overview
2. Introduction to Ethical Hacking
3. Attacker Motives and Goals
4. Attack Classifications
5. Information Warfare
6. Cyber Kill Chain
7. Tactics Techniques and Procedures
8. Common Attack Patterns
9. Threat Hunting Concepts
10. Risk and Risk Management
11. Cyber Threat Intelligence
12. Threat Modeling
13. Incident Management and Response

14. ML and AI
15. Standards and Regulations
16. CEH Hacking Methodology
17. MITRE ATT&CK Framework
18. Diamond Model of Intrusion Analysis
19. Footprinting Concepts
20. Google Dorks
21. Shodan and Censys
22. Sub-Domain Enumeration
23. Social Networking Recon
24. Job Board Recon
25. Deep-Dark Web Recon
26. Email Tracking
27. WHOIS and DNS Recon
28. Social Engineering Recon
29. Other Footprinting Tools
30. Footprinting and Recon Countermeasures
31. Network Scanning Types
32. Network Scanning Tools
33. Host Discovery
34. Port and Service Scanning
35. TCP Connect Scan
36. Stealth Scan
37. Inverse TCP XMAS and Maimon Scans
38. ACK Scan
39. IDLE IPID Scan
40. UDP Scan
41. SCTP INIT and COOKIE ECHO Scans
42. Scan Optimizations
43. Target OS Identification Techniques
44. IDS and Firewall Evasion
45. NetBIOS and SMB Enumeration
46. SMTP Enumeration
47. LDAP Enumeration

48. NTP Enumeration
49. NFS Enumeration
50. SNMP Enumeration
51. Vulnerability Assessment Concepts and Resources
52. Vulnerability Management Life-Cycle
53. Vulnerability Classification
54. Vulnerability Assessment Types
55. Vulnerability Assessment Models and Tools
56. Vulnerability Assessment Reports
57. CEH Hacking Methodology and Goals
58. Windows Authentication
59. Password Attacks - Basic Concepts
60. Password Extraction and Cracking
61. Password Attacks Cracking Enhancement Techniques
62. Buffer Overflows
63. Privilege Escalation
64. Maintaining Access
65. Steganography
66. Covering Tracks
67. AD Enumeration
68. Mimikatz
69. Pivoting
70. Malware Concepts and Components
71. APT
72. Trojans
73. Viruses and Worms
74. Fileless Malware
75. Malware Analysis
76. Malware Countermeasures
77. Network Sniffing Basics
78. DHCP Sniffing Attacks
79. ARP Poisoning
80. DNS Poisoning
81. Sniffing Defenses

82. Social Engineering Concepts and Attacks
83. Insider Threats
84. Identity Theft
85. DoS and DDoS Attacks
86. Volumetric Attacks
87. Protocol Attacks
88. Application Layer Attacks
89. Botnets
90. DoS and DDoS Countermeasures
91. Session Hijacking Concepts
92. Network Level Session Hijacking
93. Application Level Session Hijacking
94. Session Hijacking Countermeasures
95. IDS and IPS
96. Firewalls
97. Honeypots
98. Web Server Basics
99. Web Server Attacks
100. Web Server Hacking Methodology
101. Web App Basics
102. OWASP Top 10 Web Application Attacks 2021
103. Web App Hacking Methodology
104. Unvalidated Redirects and Forwards
105. XSS and CSRF
106. Input Filtering Evasion
107. IDOR
108. Local File Inclusion and Remote File Inclusion
109. IoT Attacks Tools and Countermeasures
110. APIs and Webhooks
111. SQL Injection to System Access
112. SQL Injection Concepts
113. Error-Based SQL Injection Attacks
114. Blind-Based SQL Injection Attacks
115. SQLMap

116. Wireless Basics
117. Wireless Threats
118. Wireless Hacking Tools
119. Wireless Hacking
120. Wireless Hacking Countermeasures
121. Mobile Security Basics: App and Network Vulnerabilities
122. Mobile Security Basics: Device, Proximity, and Operational
123. Android Security
124. iOS Security
125. Mobile Device Management and BYOD
126. IoT Basics
127. IoT Threats and Vulnerabilities
128. Operational Technology Basics
129. OT Attacks Tools and Countermeasures
130. Cloud Computing Basics
131. Container Basics
132. Hacking Cloud Services
133. Cloud Security Controls
134. Cryptography Basics
135. Crypto Algorithms and Implementations
136. Cryptography Tools
137. Public Key Infrastructure
138. Cryptanalysis
139. Crypto-Attack Countermeasures

Skill Labs

(16h * 16 Labs)

A **skills lab** is a guided, hands-on learning environment that allows students to practice real-world tasks in a safe, virtual setting. Instead of simply reading or watching videos, learners actively do the work—navigating realistic scenarios, applying concepts, troubleshooting issues, and building confidence through practical experience. This ensures that theory becomes usable skill. Skill labs are essential for developing true workplace readiness because they mirror real systems, tools, and challenges, helping learners bridge the gap between knowledge and performance. By completing a skills lab, students gain the hands-on competence employers expect and are better prepared for both assessments and real job responsibilities.

Skill Labs Topics

1. Introduction to AI in Ethical Hacking (CEHv13)
2. Footprinting and Reconnaissance Techniques with AI (CEHv13)
3. Network Reconnaissance Techniques with AI (CEHv13)
4. Enumeration Reconnaissance Techniques with AI (CEHv13)
5. Vulnerability Analysis Tools & Techniques with AI (CEHv13)
6. System Hacking Methodologies with AI (CEHv13)
7. Malware Threat Concepts with AI (CEHv13)
8. Network Sniffing Techniques with AI (CEHv13)
9. Social Engineering Techniques and Exploits with AI (CEHv13)
10. Denial-of-Service Attacks w/AI (CEHv13)
11. Session Hijacking Concepts with AI (CEHv13)
12. Compromising Web Servers with AI (CEHv13)
13. Web Application Hacking with AI (CEHv13)
14. SQL Injection Methodologies with AI (CEHv13)
15. Introduction to Cloud Computing with AI (CEHv13)
16. Cryptography Techniques with AI (CEHv13)