Ethical Hacking Supported Labs

Lab	Title	Certified Ethical Hacking (CEH) Domain
1	Using Active and Passive Techniques to Enumerate Network Hosts	• Introduction to Ethical Hacking • Scanning Networks • Enumeration • Sniffers
2	Conducting Active and Passive Reconnaissance Against a Target	• Introduction to Ethical Hacking • Footprinting and Reconnaissance • Scanning Networks • Social Engineering
3	Using the SYSTEM account	• System Hacking
4	Poison Ivy – Remote Access Trojan	• System Hacking • Trojans and Backdoors • Viruses and Worms
5	Using the SHARK Remote Administration Tool	• System Hacking • Trojans and Backdoors • Viruses and Worms
6	Utilizing Malware - Dark Comet	• System Hacking • Trojans and Backdoors • Viruses and Worms
7	Breaking Windows Passwords	• System Hacking
8	Using John the Ripper to Crack Linux Passwords	• System Hacking
9	Using Spear Phishing to Target an Organization	• System Hacking • Social Engineering • Session Hijacking
10	Breaking WEP and WPA Encryption	• Hacking Wireless Networks
11	Using Metasploit to Attack a Remote System	• Scanning Networks • Enumeration • Sniffers

Lab	Title	Certified Ethical Hacking (CEH) Domain
		• Evading IDS, Firewalls, and Honeypots
12	Using Armitage to Attack the Network	• Introduction to Ethical Hacking • Footprinting and Reconnaissance • Scanning Networks • System Hacking • Penetration Testing
13	Exploitation with IPv6	• System Hacking
14	Creating MSFPAYLOADS	• System Hacking • Trojans and Backdoors • Viruses and Worms • Penetration Testing
15	Abusing SYSTEMS	• Denial of Service
16	SQL Injection	• Hacking Webservers • Hacking Web Applications • SQL Injection
17	Launching a Buffer Overflow	• System Hacking • Buffer Overflow
18	Intrusion Detection	• Evading IDS, Firewalls, and Honeypots
19	Using Certificates to Encrypt Email	• Cryptography