

CEH V10 EC-COUNCIL CERTIFIED ETHICAL HACKER

MOST DEMANDING COMPLETE HACKING GUIDE

EXAM: 312-50

CEH
Certified Ethical Hacker

"To beat a hacker, you need to think like a hacker"

MOST ADVANCED HACKING COURSE





Document Control

Proposal Name	:	CEH v10: EC-Council Certified Ethical Hacker Complete Training Guide with Practice Labs
Document Version	:	1.0
Document Release Date	:	14-May-18
Reference	:	Certified Ethical Hacking Workbook

Copyright © 2018 IPSpecialist LTD.

Registered in England and Wales

Company Registration No: 10883539

Registration Office at Office 32, 19-21 Crawford Street, London W1H 1PJ,
United Kingdom

www.ipspecialist.net

All rights reserved. No part of this book may be reproduced or transmitted in

any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from IPSpecialist LTD, except for the inclusion of brief quotations in a review.

Feedback:

If you have any comments regarding the quality of this book, or otherwise alter it to suit your needs better, you can contact us by email at info@ipspecialist.net

Please make sure to include the book title and ISBN in your message

About IPSpecialist

IPSPECIALIST LTD. IS COMMITTED TO EXCELLENCE AND DEDICATED TO YOUR SUCCESS.

Our philosophy is to treat our customers like family. We want you to succeed, and we are willing to do anything possible to help you make it happen. We have the proof to back up our claims. We strive to accelerate billions of careers with great courses, accessibility, and affordability. We believe that continuous learning and knowledge evolution are most important things to keep re-skilling and up-skilling the world.

Planning and creating a specific goal is where IPSpecialist helps. We can create a career track that suits your visions as well as develop the competencies you need to become a professional Network Engineer. We can also assist you with the execution and evaluation of proficiency level based on the career track you choose, as they are customized to fit your specific goals.

We help you STAND OUT from the crowd through our detailed IP training content packages.

Course Features:

- ***Self-Paced learning***
 - Learn at your own pace and in your own time
- ***Covers Complete Exam Blueprint***
 - Prep-up for the exam with confidence
- ***Case Study Based Learning***
 - Relate the content to real-life scenarios
- ***Subscriptions that suits you***
 - Get more pay less with IPS Subscriptions
- ***Career Advisory Services***
 - Let industry experts plan your career journey

- ***Virtual Labs to test your skills***
 - With IPS vRacks, you can testify your exam preparations
- ***Practice Questions***
 - Practice Questions to measure your preparation standards
- ***On Request Digital Certification***
 - On request, digital certification from IPSpecialist LTD.

About the Authors:

We compiled this workbook under the supervision of multiple professional engineers. These engineers specialize in different fields, i.e., Networking, Security, Cloud, Big Data, IoT, and so forth. Each engineer develops content in its specialized field that is compiled to form a comprehensive certification guide.

About the Technical Reviewers:

Nouman Ahmed Khan

AWS-Architect, CCDE, CCIEX5 (R&S, SP, Security, DC, Wireless), CISSP, CISA, CISM is a Solution Architect working with a major telecommunication provider in Qatar. He works with enterprises, mega-projects, and service providers to help them select the best-fit technology solutions. He also works closely with a consultant to understand customer business processes and helps select an appropriate technology strategy to support business goals. He has more than 14 years of experience working in Pakistan/Middle-East & UK. He holds a Bachelor of Engineering Degree from NED University, Pakistan, and M.Sc. in Computer Networks from the UK.

Abubakar Saeed

Abubakar Saeed has more than twenty-five years of experience, Managing, Consulting, Designing, and implementing large-scale technology projects,

extensive experience heading ISP operations, solutions integration, heading Product Development, Presales, and Solution Design. Emphasizing on adhering to Project timelines and delivering as per customer expectations, he always leads the project in the right direction with his innovative ideas and excellent management.

Muhammad Yousuf

Muhammad Yousuf is a professional technical content writer. He is Cisco Certified Network Associate in Routing and Switching, holding bachelor's degree in Telecommunication Engineering from Sir Syed University of Engineering and Technology. He has both technical knowledge and industry sounding information, which he uses perfectly in his career.

Table of Contents

Chapter 1: Introduction to Ethical Hacking

- Technology Brief

- Information Security Overview

 - Data Breach

 - Essential Terminology

 - Elements of Information Security

 - The Security, Functionality, and Usability Triangle

- Information Security Threats and Attack Vectors

 - Motives, Goals, and Objectives of Information Security Attacks

 - Top Information Security Attack Vectors

 - Information Security Threat Categories

 - Types of Attacks on a System

 - Information Warfare

- Hacking Concepts, Types, and Phases

 - Hacker

 - Hacking

 - Hacking Phases

- Ethical Hacking Concepts and Scope

 - Ethical Hacking

 - Why Ethical Hacking is Necessary

 - Scope and Limitations of Ethical Hacking

 - Phases of Ethical Hacking

 - Skills of an Ethical Hacker

- Information Security Controls

 - Information Assurance (IA)

 - Information Security Management Program

 - Threat Modeling

 - Enterprise Information Security Architecture (EISA)

- Network Security Zoning
- Information Security Policies
- Types of Security Policies
 - Implications for Security Policy Enforcement
- Physical Security
- Incident Management
 - Incident Management Process
 - Responsibilities of Incident Response Team
- Vulnerability Assessment
 - Types of Vulnerability Assessment
 - Network Vulnerability Assessment Methodology
- Penetration Testing
 - Technology Overview
 - Important for Penetration testing
 - Types of Penetration Testing
 - Phases of Penetration Testing
 - Security Testing Methodology
- Information Security Laws and Standards
 - Payment Card Industry Data Security Standard (PCI-DSS)
 - ISO/IEC 27001:2013
 - Health Insurance Portability and Accountability Act (HIPAA)
 - Sarbanes Oxley Act (SOX)
- Chapter 2: Footprinting & Reconnaissance
 - Technology Brief
 - Footprinting Concepts
 - Pseudonymous Footprinting
 - Internet Footprinting
 - Objectives of Footprinting
 - Footprinting Methodology
 - Footprinting through Search Engines
 - Footprinting using Advanced Google Hacking Techniques
 - Footprinting through Social Networking Sites
 - Website Footprinting
 - Email Footprinting
 - Competitive Intelligence

Monitoring Website Traffic of Target Company

WHOIS Footprinting

DNS Footprinting

Network Footprinting

Footprinting through Social Engineering

Footprinting Tool

Lab 02-1: Maltego Tool Overview

Lab 02-2: Recon-ng Overview

Lab 02-3: FOCA Tool Overview

Countermeasures of Footprinting

Lab 2-4: Gathering information using Windows Command Line Utilities

Lab 2-5: Downloading a Website using Website Copier tool (HTTrack)

Lab 2-6: Gathering information using Metasploit

Chapter 3: Scanning Networks

Technology Brief

Overview of Network Scanning

TCP Communication

Creating Custom Packet Using TCP Flags

Scanning Methodology

Checking for Live Systems

Check for Open Ports

Lab 3-1: Hping Commands:

Lab 3-2: Hping Commands:

Lab 3-3: Xmas Scanning

Scanning Beyond IDS

OS Fingerprinting & Banner Grabbing

Draw Network Diagrams

Lab 3-4: Creating Network Topology Map using Tool

Prepare Proxies

Chapter 4: Enumeration

Technology Brief

Enumeration Concepts

Enumeration

Techniques for Enumeration

Services and Ports to Enumerate

Lab 4-1: Services Enumeration using Nmap

NetBIOS Enumeration

NetBIOS Enumeration Tool

Lab 4-2: Enumeration using SuperScan Tool

Enumerating Shared Resources Using Net View

Lab 4-3: Enumeration using SoftPerfect Network Scanner Tool

SNMP Enumeration

SNMP Enumeration

Simple Network Management Protocol

LDAP Enumeration

Lightweight Directory Access Protocol (LDAP)

LDAP Enumeration Tool:

NTP Enumeration

Network Time Protocol (NTP)

SMTP Enumeration

Simple Mail Transfer Protocol (SMTP)

SMTP Enumeration Technique

DNS Zone Transfer Enumeration Using NSLookup

Enumeration Countermeasures

Chapter 5: Vulnerability Analysis

Technology Brief

Vulnerability Assessment Concept:

Vulnerability Assessment

Vulnerability Assessment Life-Cycle

Vulnerability Assessment Solutions

Vulnerability Scoring Systems

Vulnerability Scanning

Lab 5.1: Vulnerability Scanning using Nessus Vulnerability Scanning Tool

Chapter 6: System Hacking

Technology Brief

System Hacking

System Hacking Methodology

Password Cracking

Lab 6-1: Online tool for default passwords

Lab 6-2: Rainbow Table using Winrtgen tool

Lab 6-3: Password Cracking using Pwdump7 and Ophcrack tool.

Escalating Privileges

Executing Applications

Hiding Files

Lab 6-4: NTFS Stream Manipulation

Lab 6-5: Steganography

Lab 6-6: Image Steganography

Covering Tracks

Lab 6-7: Clearing Audit Policies on Windows

Lab 6-8: Clearing Logs on Windows

Lab 6-9: Clearing logs on Linux

Chapter 7: Malware Threats

Technology Brief

Malware

Trojan Concept

Trojan

Virus and Worms Concepts

Viruses

Virus Analysis and Detection Methods

Malware Reverse Engineering

Sheep Dipping

Malware Analysis

Lab 7-1: HTTP RAT Trojan

Lab 7-2: Monitoring TCP/IP connection using CurrPort tool

Chapter 8: Sniffing

Technology Brief

Sniffing Concepts

Introduction to Sniffing

Working of Sniffers

Types of Sniffing

Hardware Protocol Analyzer

SPAN Port

Wiretapping

MAC Attacks

MAC Address Table / CAM Table

- MAC Flooding

- Switch Port Stealing

- Defend against MAC Attacks

- DHCP Attacks

- Dynamic Host Configuration Protocol (DHCP) Operation

- DHCP Starvation Attack

- Rogue DHCP Server Attack

- Defending Against DHCP Starvation and Rogue Server Attack

- ARP Poisoning

- Address Resolution Protocol (ARP)

- ARP Spoofing Attack

- Defending ARP Poisoning

- Spoofing Attack

- MAC Spoofing/Duplicating

- Lab 8-1: Configuring locally administered MAC address

- DNS Poisoning

- DNS Poisoning Techniques

- How to Defend Against DNS Spoofing

- Sniffing Tools

- Wireshark

- Lab 8-2: Introduction to Wireshark

- Countermeasures

- Defending Against Sniffing

- Sniffing Detection Techniques

- Sniffer Detection Technique

- Promiscuous Detection Tool

- Chapter 9: Social Engineering

- Technology Brief

- Social Engineering Concepts

- Introduction to Social Engineering

- Phases of a Social Engineering Attack

- Social Engineering Techniques

- Types of Social Engineering

- Insider Attack

- Impersonation on Social Networking Sites

Social Engineering Through Impersonation on Social Networking Sites

Risks of Social Networking in a Corporate Networks

Identity Theft

Identify Theft Overview

The process of Identity theft

Social Engineering Countermeasures

Lab 09-1: Social Engineering using Kali Linux

Chapter 10: Denial-of-Services

Technology Brief

DoS/DDoS Concepts

Denial of Service (DoS)

Distributed Denial of Service (DDoS)

How Distributed Denial of Service Attacks Work

DoS/DDoS Attack Techniques

Basic Categories of DoS/DDoS Attacks

DoS/DDoS Attack Techniques

Botnets

Botnet Setup

Propagation of Malicious Codes

Botnet Trojan

DoS/DDoS Attack Tools

Pandora DDoS Bot Toolkit

Other DDoS Attack tools

DoS and DDoS Attack Tool for Mobile

Lab 10-1: SYN Flooding Attack using Metasploit

Lab 10-2: SYN Flooding Attack using Hping3

Counter-measures

Detection Techniques

DoS/DDoS Countermeasure Strategies

Techniques to Defend against Botnets

Enabling TCP Intercept on Cisco IOS Software

Chapter 11: Session Hijacking

Technology Brief

Session Hijacking

Session Hijacking Techniques

- Session Hijacking Process
- Types of Session Hijacking
- Session Hijacking in OSI Model
- Spoofing vs. Hijacking
- Application Level Session Hijacking
 - Application-Level Hijacking Concept
 - Compromising Session IDs Using Man-in-the-Middle Attack
 - Compromising Session IDs Using Man-in-the-Browser Attack
 - Compromising Session IDs Using Client-side Attacks
 - Session Replay Attack
 - Session Fixation
- Network-level Session Hijacking
 - The 3-Way Handshake
 - TCP/IP Hijacking
 - Source Routing
 - RST Hijacking
 - Blind Hijacking
 - Forged ICMP and ARP Spoofing
 - UDP Hijacking
- Countermeasures
 - Session Hijacking Countermeasures
 - IPSec
- Chapter 12: Evading IDS, Firewall and Honeypots
 - Technology Brief
 - IDS, Firewall and Honeypot Concepts
 - Intrusion Detection Systems (IDS)
 - Firewall
 - Honeypot
 - IDS, Firewall and Honeypot System
 - Intrusion Detection Tools
 - Evading IDS
 - Insertion Attack
 - Evasion
 - Denial-of-Service Attack (DoS)
 - Obfuscating

- False Positive Generation
- Session Splicing
- Unicode Evasion Technique
- Evading Firewalls
 - Firewall Identification
 - IP Address Spoofing
 - Source Routing
 - By passing Techniques
 - Bypassing through SSH Tunneling Method
 - Bypassing Firewall through External Systems
- IDS/Firewall Evasion Counter-measures
- Lab 12-1: Configuring Honeypot on Windows Server 2016
- Chapter 13: Hacking Web Servers
 - Technology Brief
 - Web server Concepts
 - Web Server Security Issue
 - Open Source Web server Architecture
 - IIS Web Server Architecture
 - Web server Attacks
 - DoS/DDoS Attacks
 - DNS Server Hijacking
 - DNS Amplification Attack
 - Directory Traversal Attacks
 - Man-in-the-Middle/Sniffing Attack
 - Phishing Attacks
 - Website Defacement
 - Web server Misconfiguration
 - HTTP Response Splitting Attack
 - Web Cache Poisoning Attack
 - SSH Brute-force Attack
 - Web Application Attacks
 - Attack Methodology
 - Information Gathering
 - Web server Footprinting
 - Lab 13-1: Web Server Footprinting using Tool

- Mirroring a Website
- Vulnerability Scanning
- Session Hijacking
- Hacking Web Passwords
- Countermeasures
 - Countermeasures
- Patch Management
 - Patches and Hotfixes
 - Patch Management
- Lab 13-2: Microsoft Baseline Security Analyzer (MBSA)
- Lab 13-3: Web server Security Tool
- Chapter 14: Hacking Web Applications
 - Technology Brief
 - Web Application Concepts
 - Server Administrator
 - Application Administrator
 - Client
 - How do Web Applications works?
 - Web 2.0
 - Web App Threats
 - Web App Hacking Methodology
 - Analyze Web Applications
 - Attack Authentication Mechanism
 - Authorization Attack Schemes
 - Session Management Attack
 - Perform Injection Attacks
 - Attack Data Connectivity
 - Countermeasures
 - Encoding Schemes
- Chapter 15: SQL Injection
 - Technology Brief
 - SQL Injection Concepts
 - SQL Injection
 - The scope of SQL Injection
 - How SQL Query works

- SQL Injection Tools
- Types of SQL Injection
 - In-Band SQL Injection
 - Inferential SQL Injection (Blind Injection)
 - Out-of-band SQL Injection
- SQL Injection Methodology
 - Information Gathering and SQL Injection Vulnerability Detection
 - Launch SQL Injection Attacks
 - Advanced SQL Injection
- Evasion Techniques
 - Evading IDS
 - Types of Signature Evasion Techniques
- Counter-measures
- Lab 15-1: Using IBM Security AppScan Standard
- Chapter 16: Hacking Wireless Networks
 - Technology Brief
 - Wireless Concepts
 - Wireless Networks
 - Wi-Fi Technology
 - Types of Wireless Antenna
 - Wireless Encryption
 - WEP Encryption
 - WPA Encryption
 - WPA2 Encryption
 - Wireless Threats
 - Access Control Attacks
 - Integrity and Confidentiality Attacks
 - Availability Attacks
 - Authentication Attacks
 - Rogue Access Point Attack
 - Client Mis-association
 - Misconfigured Access Point Attack
 - Unauthorized Association
 - Ad Hoc Connection Attack
 - Jamming Signal Attack

Wireless Hacking Methodology

- Wi-Fi Discovery

- GPS Mapping

- Wireless Traffic Analysis

- Launch Wireless Attacks

Bluetooth Hacking

- Bluetooth Attacks

- Bluetooth Countermeasures

Wireless Security Tools

- Wireless Intrusion Prevention Systems

- Wi-Fi Security Auditing Tool

Lab 16-1: Hacking Wi-Fi Protected Access Network using Aircrack-ng
Countermeasures

Chapter 17: Hacking Mobile Platforms

- Technology Brief

- Mobile Platform Attack Vectors

 - OWASP Top 10 Mobile Threats

 - Mobile Attack Vector

- Hacking Android OS

 - Introduction to Android Operating System

- Hacking iOS

 - iPhone Operating System

 - Jailbreaking iOS

- Hacking Windows Phone OS

 - Windows Phone

- Hacking BlackBerry

 - BlackBerry Operating System

 - BlackBerry Attack Vectors

- Mobile Device Management (MDM)

 - Mobile Device Management Concept

- Bring Your Own Device (BYOD)

 - BYOD Architecture Framework

- Mobile Security Guidelines

Chapter 18: IoT Hacking

- Technology Brief

Internet of Things (IoT) Concept

- How does the Internet of Things works?

- IoT Communication Models

Understanding IoT Attacks

- Challenges to IoT

- OWASP Top 10 IoT Vulnerabilities

- IoT Attack Areas

- IoT Attacks

IoT Hacking Methodology

- Information Gathering

- Vulnerability Scanning

- Launch Attack

- Gain Access

- Maintain Attack

Countermeasures:

Chapter 19: Cloud Computing

Introduction to Cloud Computing

- Types of Cloud Computing Services

- Cloud Deployment Models

- NIST Cloud Computing Reference Architecture

- Cloud Computing Benefits

- Understanding Virtualization

Cloud Computing Threats

- Data Loss/Breach

- Abusing Cloud Services

- Insecure Interface and APIs

Cloud Computing Attacks

- Service Hijacking using Social Engineering Attacks

- Service Hijacking using Network Sniffing

- Session Hijacking using XSS Attack

- Session Hijacking using Session Riding

- Domain Name System (DNS) Attacks

- Side Channel Attacks or Cross-guest VM Breaches

Cloud Security

- Cloud Security Control Layers

- Responsibilities in Cloud Security
- Cloud Computing Security Considerations
- Cloud Security Tools
 - Core CloudInspect
 - CloudPassage Halo
- Chapter 20: Cryptography
 - Technology Brief
 - Cryptography Concepts
 - Cryptography
 - Types of Cryptography
 - Government Access to Keys (GAK)
 - Encryption Algorithms
 - Ciphers
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
 - RC4, RC5, RC6 Algorithms
 - The DSA and Related Signature Schemes
 - RSA (Rivest Shamir Adleman)
 - Lab 20-1: Example of RSA Algorithm
 - Message Digest (One-way Hash) Functions
 - Secure Hashing Algorithm (SHA)
 - SSH (Secure Shell)
 - Cryptography Tools
 - MD5 Hash Calculators
 - Lab 20-2: Calculating MD5 using Tool
 - Hash Calculators for Mobile:
 - Cryptography Tool
 - Lab 20-3: Advanced Encryption Package 2014
 - Public Key Infrastructure(PKI)
 - Certification Authorities (CA)
 - Signed Certificate Vs. Self Signed Certificate
 - Email Encryption
 - Digital Signature
 - SSL (Secure Sockets Layer)
 - SSL and TLS for Secure Communication

Pretty Good Privacy (PGP)	
Disk Encryption	
Cryptography Attacks	
Code Breaking Methodologies	
References	
Chapter 1: Introduction to Ethical Hacking	22
Technology Brief	22
Information Security Overview	22
Data Breach	22
Essential Terminology	23
Elements of Information Security	24
The Security, Functionality, and Usability Triangle	26
Information Security Threats and Attack Vectors	27
Motives, Goals, and Objectives of Information Security Attacks	27
Top Information Security Attack Vectors	27
Information Security Threat Categories	30
Types of Attacks on a System	32
Information Warfare	33
Hacking Concepts, Types, and Phases	34
Hacker	34
Hacking	35
Hacking Phases	35
Ethical Hacking Concepts and Scope	36
Ethical Hacking	36
Why Ethical Hacking is Necessary	36
Scope and Limitations of Ethical Hacking	37
Phases of Ethical Hacking	37
Skills of an Ethical Hacker	38
Information Security Controls	39
Information Assurance (IA)	39
Information Security Management Program	39
Threat Modeling	40
Enterprise Information Security Architecture (EISA)	41
Network Security Zoning	41
Information Security Policies	42

Types of Security Policies	43	
Implications for Security Policy Enforcement		44
Physical Security	44	
Incident Management	45	
Incident Management Process	46	
Responsibilities of Incident Response Team		46
Vulnerability Assessment	47	
Types of Vulnerability Assessment	47	
Network Vulnerability Assessment Methodology		47
Penetration Testing	50	
Technology Overview	50	
Important for Penetration testing	50	
Types of Penetration Testing	51	
Phases of Penetration Testing	52	
Security Testing Methodology	52	
Information Security Laws and Standards	53	
Payment Card Industry Data Security Standard (PCI-DSS)		53
ISO/IEC 27001:2013	54	
Health Insurance Portability and Accountability Act (HIPAA)		54
Sarbanes Oxley Act (SOX)	54	
Chapter 2: Footprinting & Reconnaissance	57	
Technology Brief	57	
Footprinting Concepts	57	
Pseudonymous Footprinting	57	
Internet Footprinting	57	
Objectives of Footprinting	57	
Footprinting Methodology	58	
Footprinting through Search Engines	58	
Footprinting using Advanced Google Hacking Techniques		64
Footprinting through Social Networking Sites	66	
Website Footprinting	69	
Email Footprinting	79	
Competitive Intelligence	81	
Monitoring Website Traffic of Target Company		82
WHOIS Footprinting	86	

DNS Footprinting	92	
Network Footprinting	96	
Footprinting through Social Engineering		99
Footprinting Tool	101	
Lab 02-1: Maltego Tool Overview		101
Lab 02-2: Recon-ng Overview		104
Lab 02-3: FOCA Tool Overview		109
Countermeasures of Footprinting		111
Lab 2-4: Gathering information using Windows Command Line Utilities		112
Lab 2-5: Downloading a Website using Website Copier tool (HTTrack)		116
Lab 2-6: Gathering information using Metasploit		122
Chapter 3: Scanning Networks		138
Technology Brief		138
Overview of Network Scanning		138
TCP Communication		138
Creating Custom Packet Using TCP Flags		140
Scanning Methodology		142
Checking for Live Systems		142
Check for Open Ports		145
Lab 3-1: Hping Commands:		146
Lab 3-2: Hping Commands:		149
Lab 3-3: Xmas Scanning		155
Scanning Beyond IDS		165
OS Fingerprinting & Banner Grabbing		165
Draw Network Diagrams		167
Lab 3-4: Creating Network Topology Map using Tool		168
Prepare Proxies		170
Chapter 4: Enumeration		176
Technology Brief		176
Enumeration Concepts		176
Enumeration		176
Techniques for Enumeration		176
Services and Ports to Enumerate		177

Lab 4-1: Services Enumeration using Nmap	178
NetBIOS Enumeration	181
NetBIOS Enumeration Tool	183
Lab 4-2: Enumeration using SuperScan Tool	184
Enumerating Shared Resources Using Net View	187
Lab 4-3: Enumeration using SoftPerfect Network Scanner Tool	187
SNMP Enumeration	191
SNMP Enumeration	191
Simple Network Management Protocol	192
LDAP Enumeration	194
Lightweight Directory Access Protocol (LDAP)	194
LDAP Enumeration Tool:	194
NTP Enumeration	195
Network Time Protocol (NTP)	195
SMTP Enumeration	198
Simple Mail Transfer Protocol (SMTP)	198
SMTP Enumeration Technique	198
DNS Zone Transfer Enumeration Using NSLookup	199
Enumeration Countermeasures	200
Chapter 5: Vulnerability Analysis	202
Technology Brief	202
Vulnerability Assessment Concept:	202
Vulnerability Assessment	202
Vulnerability Assessment Life-Cycle	203
Vulnerability Assessment Solutions	204
Vulnerability Scoring Systems	205
Vulnerability Scanning	207
Lab 5.1: Vulnerability Scanning using Nessus Vulnerability Scanning Tool	211
Chapter 6: System Hacking	227
Technology Brief	227
System Hacking	227
System Hacking Methodology	228
Password Cracking	228
Lab 6-1: Online tool for default passwords	231

Lab 6-2: Rainbow Table using Winrtgen tool	234	
Lab 6-3: Password Cracking using Pwdump7 and Ophcrack tool.		244
Escalating Privileges	255	
Executing Applications	257	
Hiding Files	261	
Lab 6-4: NTFS Stream Manipulation	263	
Lab 6-5: Steganography	271	
Lab 6-6: Image Steganography	273	
Covering Tracks	277	
Lab 6-7: Clearing Audit Policies on Windows		278
Lab 6-8: Clearing Logs on Windows		281
Lab 6-9: Clearing logs on Linux		283
Chapter 7: Malware Threats	290	
Technology Brief	290	
Malware	290	
Trojan Concept	291	
Trojan	291	
Virus and Worms Concepts	297	
Viruses	297	
Virus Analysis & Detection Methods		301
Malware Reverse Engineering		302
Sheep Dipping	302	
Malware Analysis	302	
Lab 7-1: HTTP RAT Trojan	304	
Lab 7-2: Monitoring TCP/IP connection using CurrPort tool		313
Chapter 8: Sniffing	320	
Technology Brief	320	
Sniffing Concepts	320	
Introduction to Sniffing	320	
Working of Sniffers	320	
Types of Sniffing	321	
Hardware Protocol Analyzer		322
SPAN Port	323	
Wiretapping	324	
MAC Attacks	325	

MAC Address Table / CAM Table	325
MAC Flooding	327
Switch Port Stealing	327
Defend against MAC Attacks	327
DHCP Attacks	328
Dynamic Host Configuration Protocol (DHCP) Operation	328
DHCP Starvation Attack	329
Rogue DHCP Server Attack	330
Defending Against DHCP Starvation and Rogue Server Attack	330
ARP Poisoning	331
Address Resolution Protocol (ARP)	331
ARP Spoofing Attack	332
Defending ARP Poisoning	333
Spoofing Attack	336
MAC Spoofing/Duplicating	336
Lab 8-1: Configuring locally administered MAC address	336
DNS Poisoning	342
DNS Poisoning Techniques	342
How to Defend Against DNS Spoofing	343
Sniffing Tools	344
Wireshark	344
Lab 8-2: Introduction to Wireshark	344
Countermeasures	348
Defending Against Sniffing	348
Sniffing Detection Techniques	348
Sniffer Detection Technique	348
Promiscuous Detection Tool	349
Chapter 9: Social Engineering	350
Technology Brief	350
Social Engineering Concepts	350
Introduction to Social Engineering	350
Phases of a Social Engineering Attack	351
Social Engineering Techniques	351
Types of Social Engineering	351
Insider Attack	355

Impersonation on Social Networking Sites	355
Social Engineering Through Impersonation on Social Networking Sites	355
Risks of Social Networking in a Corporate Networks	356
Identity Theft	356
Identify Theft Overview	356
The process of Identity theft	356
Social Engineering Countermeasures	358
Lab 09-1: Social Engineering using Kali Linux	358
Chapter 10: Denial-of-Services	371
Technology Brief	371
DoS/DDoS Concepts	371
Denial of Service (DoS)	371
Distributed Denial of Service (DDoS)	372
How Distributed Denial of Service Attacks Work	372
DoS/DDoS Attack Techniques	372
Basic Categories of DoS/DDoS Attacks	372
DoS/DDoS Attack Techniques	373
Botnets	376
Botnet Setup	376
Propagation of Malicious Codes	378
Botnet Trojan	379
DoS/DDoS Attack Tools	379
Pandora DDoS Bot Toolkit	379
Other DDoS Attack tools	379
DoS and DDoS Attack Tool for Mobile	380
Lab 10-1: SYN Flooding Attack using Metasploit	380
Lab 10-2: SYN Flooding Attack using Hping3	386
Counter-measures	388
Detection Techniques	388
DoS/DDoS Countermeasure Strategies	388
Techniques to Defend against Botnets	388
Enabling TCP Intercept on Cisco IOS Software	389
Chapter 11: Session Hijacking	391
Technology Brief	391

Session Hijacking	391	
Session Hijacking Techniques	391	
Session Hijacking Process	392	
Types of Session Hijacking	393	
Session Hijacking in OSI Model	393	
Spoofing vs. Hijacking	394	
Application Level Session Hijacking	394	
Application-Level Hijacking Concept	394	
Compromising Session IDs Using Man-in-the-Middle Attack	395	
Compromising Session IDs Using Man-in-the-Browser Attack	395	
Compromising Session IDs Using Client-side Attacks	396	
Session Replay Attack	396	
Session Fixation	396	
Network-level Session Hijacking	397	
The 3-Way Handshake	397	
TCP/IP Hijacking	397	
Source Routing	398	
RST Hijacking	398	
Blind Hijacking	398	
Forged ICMP and ARP Spoofing	398	
UDP Hijacking	398	
Countermeasures	398	
Session Hijacking Countermeasures	398	
IPSec	399	
Chapter 12: Evading IDS, Firewall & Honeypots	403	
Technology Brief	403	
IDS, Firewall and Honeypot Concepts	403	
Intrusion Detection Systems (IDS)	403	
Firewall	408	
Honeypot	416	
IDS, Firewall and Honeypot System	416	
Intrusion Detection Tools	416	
Evading IDS	418	
Insertion Attack	418	
Evasion	419	

Denial-of-Service Attack (DoS)	420	
Obfuscating	420	
False Positive Generation	420	
Session Splicing	420	
Unicode Evasion Technique	420	
Evading Firewalls	421	
Firewall Identification	421	
IP Address Spoofing	422	
Source Routing	422	
By passing Techniques	422	
Bypassing through SSH Tunneling Method	423	
Bypassing Firewall through External Systems	423	
IDS/Firewall Evasion Counter-measures	423	
Lab 12-1: Configuring Honeypot on Windows Server 2016		424
Chapter 13: Hacking Web Servers	432	
Technology Brief	432	
Web server Concepts	432	
Web Server Security Issue	432	
Open Source Web server Architecture	432	
IIS Web Server Architecture	433	
Web server Attacks	434	
DoS/DDoS Attacks	434	
DNS Server Hijacking	435	
DNS Amplification Attack	435	
Directory Traversal Attacks	435	
Man-in-the-Middle/Sniffing Attack	435	
Phishing Attacks	435	
Website Defacement	435	
Web server Misconfiguration	435	
HTTP Response Splitting Attack	436	
Web Cache Poisoning Attack	436	
SSH Brute-force Attack	436	
Web Application Attacks	436	
Attack Methodology	436	
Information Gathering	436	

Web server Footprinting	437	
Lab 13-1: Web Server Footprinting using Tool		437
Mirroring a Website	438	
Vulnerability Scanning	439	
Session Hijacking	439	
Hacking Web Passwords	439	
Countermeasures	439	
Countermeasures	440	
Patch Management	440	
Patches and Hotfixes	440	
Patch Management	441	
Lab 13-2: Microsoft Baseline Security Analyzer (MBSA)		441
Lab 13-3: Web server Security Tool	448	
Chapter 14: Hacking Web Applications	452	
Technology Brief	452	
Web Application Concepts	452	
Server Administrator	452	
Application Administrator	453	
Client	453	
How Web Applications works?	453	
Web 2.0	454	
Web App Threats	454	
Web App Hacking Methodology	456	
Analyze Web Applications	456	
Attack Authentication Mechanism	456	
Authorization Attack Schemes	456	
Session Management Attack	456	
Perform Injection Attacks	456	
Attack Data Connectivity	457	
Countermeasures	458	
Encoding Schemes	458	
Chapter 15: SQL Injection	460	
Technology Brief	460	
SQL Injection Concepts	460	
SQL Injection	460	

The scope of SQL Injection	460	
How SQL Query works	460	
SQL Injection Tools	462	
Types of SQL Injection	462	
In-Band SQL Injection	462	
Inferential SQL Injection (Blind Injection)		463
Out-of-band SQL Injection	463	
SQL Injection Methodology	463	
Information Gathering and SQL Injection Vulnerability Detection	463	
Launch SQL Injection Attacks	464	
Advanced SQL Injection	464	
Evasion Techniques	464	
Evading IDS	464	
Types of Signature Evasion Techniques		464
Counter-measures	465	
Lab 15-1: Using IBM Security AppScan Standard		465
Chapter 16: Hacking Wireless Networks	472	
Technology Brief	472	
Wireless Concepts	472	
Wireless Networks	472	
Wi-Fi Technology	475	
Types of Wireless Antenna	480	
Wireless Encryption	481	
WEP Encryption	481	
WPA Encryption	482	
WPA2 Encryption	483	
Wireless Threats	484	
Access Control Attacks	484	
Integrity & Confidentiality Attacks		484
Availability Attacks	484	
Authentication Attacks	485	
Rogue Access Point Attack	485	
Client Mis-association	485	
Misconfigured Access Point Attack	485	

Unauthorized Association	485
Ad Hoc Connection Attack	485
Jamming Signal Attack	485
Wireless Hacking Methodology	486
Wi-Fi Discovery	486
GPS Mapping	486
Wireless Traffic Analysis	486
Launch Wireless Attacks	486
Bluetooth Hacking	487
Bluetooth Attacks	487
Bluetooth Countermeasures	487
Wireless Security Tools	488
Wireless Intrusion Prevention Systems	488
Wi-Fi Security Auditing Tool	488
Lab 16-1: Hacking Wi-Fi Protected Access Network using Aircrack-ng	489
Countermeasures	497
Chapter 17: Hacking Mobile Platforms	499
Technology Brief	499
Mobile Platform Attack Vectors	499
OWASP Top 10 Mobile Threats	499
Mobile Attack Vector	500
Hacking Android OS	501
Introduction to Android Operating System	501
Hacking iOS	504
iPhone Operating System	504
Jailbreaking iOS	504
Hacking Windows Phone OS	506
Windows Phone	506
Hacking BlackBerry	507
BlackBerry Operating System	507
BlackBerry Attack Vectors	507
Mobile Device Management (MDM)	508
Mobile Device Management Concept	508
Bring Your Own Device (BYOD)	511







BYOD Architecture Framework	512	
Mobile Security Guidelines	515	
Chapter 18: IoT Hacking	516	
Technology Brief	516	
Internet of Things (IoT) Concept	516	
How the Internet of Things works?	517	
IoT Communication Models	519	
Understanding IoT Attacks	522	
Challenges to IoT	522	
OWASP Top 10 IoT Vulnerabilities	522	
IoT Attack Areas	523	
IoT Attacks	523	
IoT Hacking Methodology	524	
Information Gathering	524	
Vulnerability Scanning	525	
Launch Attack	525	
Gain Access	525	
Maintain Attack	526	
Countermeasures:	526	
Chapter 19: Cloud Computing	527	
Introduction to Cloud Computing	527	
Types of Cloud Computing Services	527	
Cloud Deployment Models	528	
NIST Cloud Computing Reference Architecture	528	
Cloud Computing Benefits	529	
Understanding Virtualization	530	
Cloud Computing Threats	531	
Data Loss/Breach	531	
Abusing Cloud Services	531	
Insecure Interface and APIs	531	
Cloud Computing Attacks	532	
Service Hijacking using Social Engineering Attacks	532	
Service Hijacking using Network Sniffing	533	
Session Hijacking using XSS Attack	533	
Session Hijacking using Session Riding	533	

Domain Name System (DNS) Attacks	533	
Side Channel Attacks or Cross-guest VM Breaches		533
Cloud Security	534	
Cloud Security Control Layers	534	
Responsibilities in Cloud Security	535	
Cloud Computing Security Considerations		536
Cloud Security Tools	537	
Core CloudInspect	537	
CloudPassage Halo	537	
Chapter 20: Cryptography	540	
Technology Brief	540	
Cryptography Concepts	540	
Cryptography	540	
Types of Cryptography	540	
Government Access to Keys (GAK)	541	
Encryption Algorithms	541	
Ciphers	541	
Data Encryption Standard (DES)	542	
Advanced Encryption Standard (AES)	543	
RC4, RC5, RC6 Algorithms	545	
The DSA and Related Signature Schemes	546	
RSA (Rivest Shamir Adleman)	546	
Lab 20-1: Example of RSA Algorithm	547	
Message Digest (One-way Hash) Functions		548
Secure Hashing Algorithm (SHA)	549	
SSH (Secure Shell)	550	
Cryptography Tools	550	
MD5 Hash Calculators	550	
Lab 20-2: Calculating MD5 using Tool	551	
Hash Calculators for Mobile:	556	
Cryptography Tool	557	
Lab 20-3: Advanced Encryption Package 2014		557
Public Key Infrastructure(PKI)	562	
Certification Authorities (CA)	562	
Signed Certificate Vs. Self Signed Certificate		563

Email Encryption	564	
Digital Signature	564	
SSL (Secure Sockets Layer)	564	
SSL and TLS for Secure Communication		564
Pretty Good Privacy (PGP)	566	
Disk Encryption	566	
Cryptography Attacks	567	
Code Breaking Methodologies	568	
References	569	

About this Workbook

This workbook covers all the information you need to pass the EC-Council's Certified Ethical Hacking 312-50 exam. The workbook is designed to take a practical approach to learning with real-life examples and case studies.

-  Covers complete CEH blueprint
-  Summarized content
-  Case Study based approach
-  Ready to practice labs on VM
-  Pass guarantee
-  Mind maps

CEHv10 Update

CEH v10 covers new modules for the security of IoT devices, vulnerability analysis, focus on emerging attack vectors on the cloud, artificial intelligence, and machine learning including a complete malware analysis process. Our CEH workbook delivers a deep understanding of applications of the vulnerability analysis in a real-world environment.

EC-Council Certifications

The International Council of E-Commerce Consultants (EC-Council) is a member-based organization that certifies individuals in various e-business and information security skills. It is the owner and creator of the world famous Certified Ethical Hacker (CEH), Computer Hacking Forensics Investigator (CHFI) and EC-Council Certified Security Analyst (ECSA)/License Penetration Tester (LPT) certification, and as well as many others certification schemes, that are offered in over 87 countries globally.

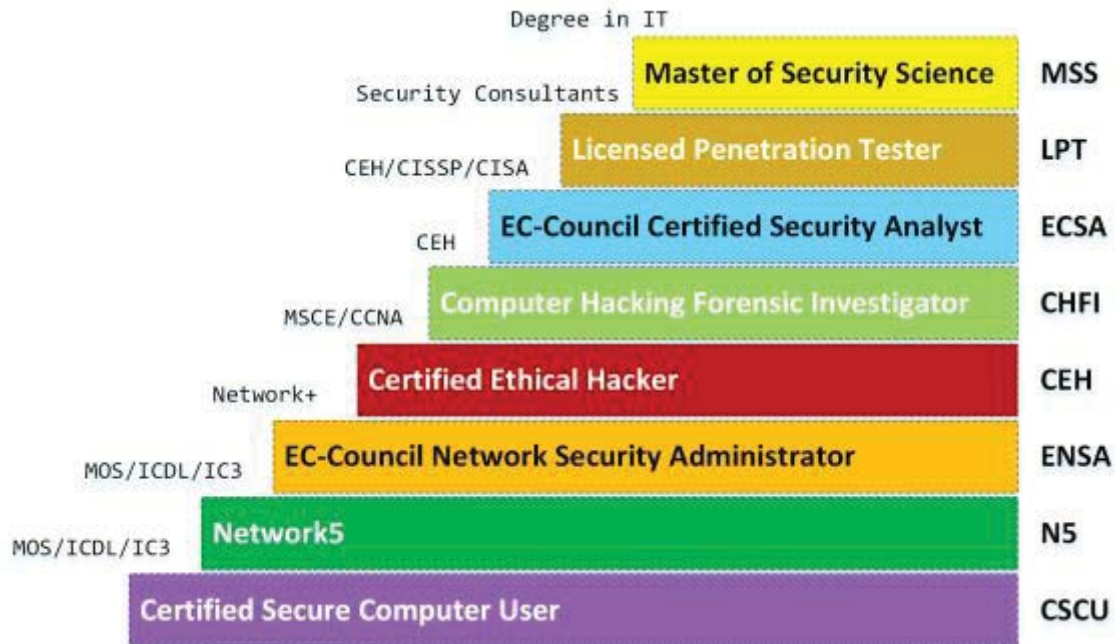


Figure 1 EC-Council Certifications Skill Matrix

EC-Council mission is to validate information security professionals having necessary skills and knowledge required in a specialized information security domain that helps them avert a cyber-war, should the need ever arise”. EC-Council is committed to withholding the highest level of impartiality and objectivity in its practices, decision making, and authority in all matters related to certification.

EC-Council Certification Tracks

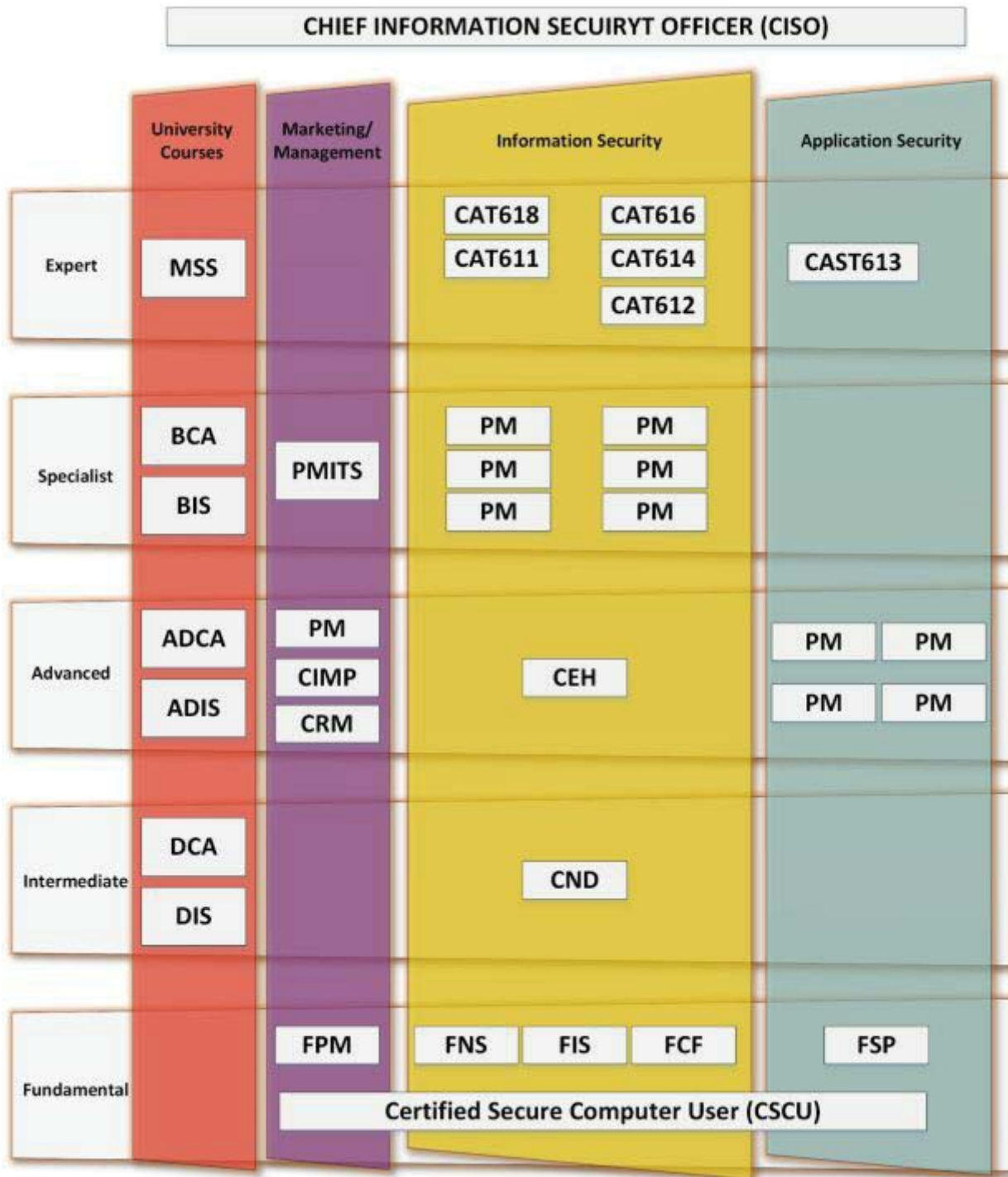


Figure 2 Cisco Certifications Track

How does CEH certification help?

The purpose of the CEH credential is to:

- ↗ Establish and govern minimum standards for credentialing professional information security specialists in ethical hacking measures.
- ↗ Inform the public that credentialed individuals meet or exceed the minimum standards.
- ↗ Reinforce ethical hacking as a unique and self-regulating profession.

About the CEH Exam

- ↗ **Number of Questions:** 125
- ↗ **Test Duration:** 4 Hours
- ↗ **Test Format:** Multiple Choice
- ↗ **Test Delivery:** ECC EXAM, VUE
- ↗ **Exam Prefix:** 312-50 (ECC EXAM), 312-50 (VUE)

A Certified Ethical Hacker is a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but lawfully and legitimately to assess the security posture of a target system(s). The CEH credential certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective.

↗	Background	04%	
↗	Analysis/Assessments		13%
↗	Security	25%	
↗	Tools/Systems/Programs		32%
↗	Procedures/Methodology		20%
↗	Regulation/Policy	04%	
↗	Ethics	02%	

Prerequisites

All the three programs, CEH, CHFI, and ECSA, require the candidate to have two years of work experience in the Information Security domain and should

be able to provide proof of the same as validated through the application process unless the candidate attends official training.