TestOut®

TestOut Ethical Hacker Pro - English 1.0.x

COURSE OUTLINE

Modified 2019-08-09

Powered by LABSIM

TestOut Ethical Hacker Pro Outline - English 1.0.x

- Videos: 88 (8:59:01)
- Demonstrations: 79 (6:29:22)
- Simulations: 65
- Fact Sheets: 96
- Exams: 63

CONTENTS:

- 2.4.2 Special Considerations (2:08)
- 2.4.3 Assessment Type Facts
- 2.4.4 Practice Questions

2.5 Legal and Ethical Compliance

- 2.5.1 Legal Compliance (5:54)
- 2.5.2 Ethics (2:37)
- 2.5.3 Authorization and Corporate Policies (3:52)
- 2.5.4 Legal and Ethical Compliance Facts
- 2.5.5 Engagement Contracts (4:18)
- 2.5.6 Engagement Contract Facts
- 2.5.7 Practice Questions

3.0 SOCIAL ENGINEERING AND PHYSICAL SECURITY

3.1 Social Engineering

- 3.1.1 Social Engineering Overview (4:46)
- 3.1.2 Social Engineering Overview Facts
- 3.1.3 Social Engineering Motivation (10:18)
- 3.1.4 Social Engineering Motivation Facts
- 3.1.5 Social Engineering Techniques (10:16)
- 3.1.6 Social Engineering Technique Facts
- 3.1.7 Phishing and Internet-Based Techniques (4:59)
- 3.1.8 Phishing and Internet-Based Technique Facts
- 3.1.9 Use the Social Engineer Toolkit (SET) (4:24)
- 3.1.10 Identify Social Engineering
- 3.1.11 Practice Questions

3.2 Physical Security

- 3.2.1 Physical Security Overview (11:25)
- 3.2.2 Physical Security Facts
- 3.2.3 Physical Security Attacks (6:32)
- 3.2.4 Physical Security Attack Facts
- 3.2.5 Practice Questions

3.3 Countermeasures and Prevention

- 3.3.1 Countermeasures and Prevention (8:13)
- 3.3.2 Countermeasures and Prevention Facts
- 3.3.3 Implement Physical Security Countermeasures
- 3.3.4 Practice Questions

4.0 RECONNAISSANCE

4.1 Reconnaissance Overview

- 4.1.1 Reconnaissance Processes (4:56)
- 4.1.2 Reconnaissance Process Facts
- 4.1.3 Reconnaissance Tool Facts
- 4.1.4 Google Hacking for Office Documents (4:19)
- 4.1.5 Perform Reconnaissance with theHarvester (4:51)
- 4.1.6 Perform Reconnaissance with Nmap (4:14)
- 4.1.7 Perform Reconnaissance with Nmap
- 4.1.8 Practice Questions

4.2 Reconnaissance Countermeasures

- 4.2.1 Reconnaissance Countermeasures (3:01)
- 4.2.2 View Windows Services (5:11)
- 4.2.3 Disable Windows Services
- 4.2.4 View Linux Services (4:14)
- 4.2.5 Manage Linux Services
- 4.2.6 Enable and Disable Linux Services
- 4.2.7 Reconnaissance Countermeasure Facts
- 4.2.8 Disable IIS Banner Broadcasting (1:47)
- 4.2.9 Hide the IIS Banner Broadcast
- 4.2.10 Practice Questions

5.0 SCANNING

5.1 Scanning Overview

- 5.1.1 Scanning Processes (5:54)
- 5.1.2 Scanning Process Facts
- 5.1.3 Scanning Tool Facts
- 5.1.4 Perform a Scan with Nmap (4:36)
- 5.1.5 Perform an Internal Scan
- 5.1.6 Perform an External Scan Using Zenmap
- 5.1.7 Perform a Scan with Nmap Scripts (4:36)
- 5.1.8 Scanning Considerations (5:38)
- 5.1.9 Scanning Considerations Facts
- 5.1.10 Practice Questions

5.2 Banner Grabbing

- 5.2.1 Banner Grabbing (4:19)
- 5.2.2 Banner Grabbing Facts

- 5.2.3 Practice Questions

6.0 ENUMERATION

6.1 Enumeration Overview

- 6.1.1 Enumeration (5:11)
- 6.1.2 Enumerate a Windows System (4:00)
- 6.1.3 Enumerate Windows (4:09)
- 6.1.4 Enumerate a Linux System (6:55)
- 6.1.5 Enumeration Facts
- 6.1.6 Enumerate with SuperScan (4:41)
- 6.1.7 Enumerate with NetBIOS Enumerator (2:52)
- 6.1.8 Enumerate Ports and Services Facts
- 6.1.9 Perform Enumeration with Nmap
- 6.1.10 Enumerate with SoftPerfect (3:50)
- 6.1.11 Perform Enumeration with Metasploit
- 6.1.12 Perform Enumeration of MSSQL with Metasploit
- 6.1.13 Practice Questions

6.2 Enumeration Countermeasures

- 6.2.1 Enumeration Countermeasures (1:53)
- 6.2.2 Enumeration Countermeasure Facts
- 6.2.3 Disable DNS Zone Transfers (5:07)
- 6.2.4 Prevent Zone Transfer
- 6.2.5 Practice Questions

7.0 ANALYZE VULNERABILITIES

7.1 Vulnerability Assessment

- 7.1.1 Vulnerability Assessment (8:41)
- 7.1.2 Vulnerability Assessment Facts
- 7.1.3 Conduct Vulnerability Scans (4:01)
- 7.1.4 Practice Questions

7.2 Vulnerability Management Life Cycle

- 7.2.1 Vulnerability Management Life Cycle (6:20)
- 7.2.2 Vulnerability Management Life Cycle Facts
- 7.2.3 Vulnerability Solutions (2:20)
- 7.2.4 Vulnerability Solution Facts
- 7.2.5 Practice Questions

7.3 Vulnerability Scoring Systems

- 7.3.1 Vulnerability Scoring Systems (5:41)
- 7.3.2 Vulnerability Scoring System Facts
- 7.3.3 Practice Questions

7.4 Vulnerability Assessment Tools

- 7.4.1 Vulnerability Assessment Tools (4:52)
- 7.4.2 Vulnerability Assessment Tool Facts
- 7.4.3 Scan a Network with Retina (7:16)
- 7.4.4 Scan a Network with Nessus (3:16)
- 7.4.5 Scan for Vulnerabilities on a Windows Workstation
- 7.4.6 Scan for Vulnerabilities on a Linux Server
- 7.4.7 Scan for Vulnerabilities on a Domain Controller
- 7.4.8 Scan for Vulnerabilities on a Security Appliance
- 7.4.9 Scan for Vulnerabilities on a WAP
- 7.4.10 Practice Questions

8.0 SYSTEM HACKING

8.1 System Hacking

- 8.1.1 Introduction to Hacking (7:05)
- 8.1.2 Introduction to Hacking Facts
- 8.1.3 Keylogger Attack (5:18)
- 8.1.4 Analyze a USB Keylogger Attack
- 8.1.5 Analyze a USB Keylogger Attack 2
- 8.1.6 Use Rainbow Tables (3:33)
- 8.1.7 Crack a Password with Rainbow Tables
- 8.1.8 Crack Passwords (8:02)
- 8.1.9 Crack Password Protected Files (3:22)
- 8.1.10 Crack a Password with John the Ripper
- 8.1.11 Crack a Router Password (6:35)
- 8.1.12 Use L0phtCrack to Audit Passwords (2:46)
- 8.1.13 Configure Password Policies (10:41)
- 8.1.14 Configure Account Password Policies
- 8.1.15 Practice Questions

8.2 Privilege Escalation

- 8.2.1 Privilege Escalation in Windows (7:15)
- 8.2.2 Use Bootable Media to Modify User Accounts (6:29)
- 8.2.3 Crack the SAM Database (4:17)
- 8.2.4 Change a Windows Password (3:03)

- 8.2.5 Privilege Escalation in Windows Facts
- 8.2.6 Crack the SAM Database with John the Ripper
- 8.2.7 Configure User Account Control (6:57)
- 8.2.8 Enforce User Account Control
- 8.2.9 Practice Questions

8.3 Maintain Access

- 8.3.1 Exploit Systems to Maintain Access (4:01)
- 8.3.2 Establish an Unauthorized SSH Connection (4:20)
- 8.3.3 Create a Backdoor with Metasploit (5:22)
- 8.3.4 Create a Backdoor with Metasploit
- 8.3.5 Exploit Systems to Maintain Access Facts
- 8.3.6 Create a Backdoor with Netcat
- 8.3.7 Practice Questions

8.4 Cover Your Tracks

- 8.4.1 Cover Your Tracks (4:57)
- 8.4.2 Clear Logs In Windows (3:01)
- 8.4.3 Use CCleaner to Hide Tracks (4:41)
- 8.4.4 Cover Your Tracks Facts
- 8.4.5 Clear Windows Log Files on Server 2016
- 8.4.6 Clear Audit Policies
- 8.4.7 Hide Programs (7:48)
- 8.4.8 Use NTFS Data Stream to Hide Files (3:14)
- 8.4.9 Use Steganography to Hide a File (3:20)
- 8.4.10 Hide Programs Facts
- 8.4.11 Hide Files with OpenStego
- 8.4.12 Practice Questions

9.0 MALWARE

9.1 Malware

- 9.1.1 Malware Overview (9:40)
- 9.1.2 Malware Overview Facts
- 9.1.3 Trojans and Backdoors (5:36)
- 9.1.4 Trojan and Backdoor Facts
- 9.1.5 Malware Concerns (3:51)
- 9.1.6 Malware Concern Facts
- 9.1.7 Malware Analysis (4:25)
- 9.1.8 Malware Analysis Facts

- 9.1.9 Create a Virus (2:34)
- 9.1.10 Create a HTTP Trojan (3:12)
- 9.1.11 Use ProRat to Create a Trojan (3:14)
- 9.1.12 Practice Questions

9.2 Combat Malware

- 9.2.1 Anti-Malware Software (5:04)
- 9.2.2 Scan for Open Ports with Netstat (3:09)
- 9.2.3 Track Port Usage with TCPView (2:31)
- 9.2.4 Anti-Malware Software Facts
- 9.2.5 Detect Open Ports with Nmap
- 9.2.6 View Open Ports with netstat
- 9.2.7 Scan for Open Ports from a Remote Computer
- 9.2.8 Counter Malware with Windows Defender
- 9.2.9 Practice Questions

10.0 SNIFFERS, SESSION HIJACKING, AND DENIAL OF SERVICE

10.1 Sniffing

- 10.1.1 Sniffing (6:38)
- 10.1.2 Sniffer Facts
- 10.1.3 Sniff Network Traffic with Wireshark (6:49)
- 10.1.4 Capture Traffic with TCPDump (5:40)
- 10.1.5 Use SMAC to Spoof MAC Addresses (3:45)
- 10.1.6 Spoof MAC Addresses with SMAC
- 10.1.7 Poison ARP (5:13)
- 10.1.8 Poison ARP and Analyze with Wireshark
- 10.1.9 Poison DNS (6:17)
- 10.1.10 Poison DNS
- 10.1.11 Filter and Analyze Traffic with Wireshark
- 10.1.12 Analyze Email Traffic for Sensitive Data
- 10.1.13 Analyze Email Traffic for Sensitive Data 2
- 10.1.14 Sniffing Countermeasures and Detection (2:54)
- 10.1.15 Detect Promiscuous Mode (3:16)
- 10.1.16 Sniffing Countermeasure and Detection Facts
- 10.1.17 Practice Questions

10.2 Session Hijacking

- 10.2.1 Session Hijacking Overview (2:36)
- 10.2.2 Session Hijacking Facts

- 10.2.3 Client-Side and Network Attacks (8:02)
- 10.2.4 Client-Side and Network Attack Facts
- 10.2.5 Perform a Man-in-the-Middle DHCP Attack (6:55)
- 10.2.6 Perform a DHCP Spoofing Man-in-the-Middle Attack
- 10.2.7 Perform an MITM Attack from a Remote Computer
- 10.2.8 Capture HTTP POST Packets with Wireshark
- 10.2.9 Use Burp Suite (5:36)
- 10.2.10 Hijack a Web Session (3:33)
- 10.2.11 Hijack a Web Session
- 10.2.12 Session Hijacking Countermeasures (3:56)
- 10.2.13 Session Hijacking Countermeasure Facts
- 10.2.14 Practice Questions

10.3 Denial of Service

- 10.3.1 Denial of Service (DoS) Overview (6:44)
- 10.3.2 Denial of Service (DoS) Facts
- 10.3.3 DoS Attack Types (5:12)
- 10.3.4 DoS Attack Type Facts
- 10.3.5 Perform a SYN Flood (6:18)
- 10.3.6 Perform and Analyze a SYN Flood Attack
- 10.3.7 Analyze ICMP Traffic in Wireshark
- 10.3.8 Launch a DoS and DDoS Attack (5:42)
- 10.3.9 Perform a DoS Attack
- 10.3.10 Analyze a DDoS Attack
- 10.3.11 DoS Countermeasures (3:42)
- 10.3.12 DoS Countermeasure Facts
- 10.3.13 Practice Questions

11.0 IDS, FIREWALLS, AND HONEYPOTS

11.1 Intrusion Detection Systems

- 11.1.1 Intrusion Detection Systems (5:15)
- 11.1.2 Intrusion Detection System Facts
- 11.1.3 Avoid IDS Detection (9:36)
- 11.1.4 Avoid IDS Detection Facts
- 11.1.5 Evade IDS (11:25)
- 11.1.6 Evade IDS Facts
- 11.1.7 IDS Penetration Testing Facts
- 11.1.8 Detect IDS Intrusion with Snort (9:16)

- 11.1.9 Implement Intrusion Detection (5:58)
- 11.1.10 Implement Intrusion Detection
- 11.1.11 Practice Questions

11.2 Firewalls

- 11.2.1 Firewalls (10:07)
- 11.2.2 Firewall Facts
- 11.2.3 Evade Firewalls (6:38)
- 11.2.4 Evade Firewalls Facts
- 11.2.5 Firewall Penetration Testing Facts
- 11.2.6 Configure a Perimeter Firewall (7:53)
- 11.2.7 Configure a Perimeter Firewall
- 11.2.8 Avoid Firewall Detection (5:26)
- 11.2.9 Perform a Decoy Scan
- 11.2.10 Perform a Decoy Scan with Zenmap
- 11.2.11 Bypass Windows Firewall with Metasploit (3:45)
- 11.2.12 Bypass Windows Firewall with Metasploit
- 11.2.13 Practice Questions

11.3 Honeypots

- 11.3.1 Honeypots (4:36)
- 11.3.2 Honeypot Facts
- 11.3.3 Evade Honeypots (4:35)
- 11.3.4 Evade Honeypots Facts
- 11.3.5 Detect Malicious Network Traffic with a Honeypot (3:23)
- 11.3.6 Create a Honeypot with Pentbox
- 11.3.7 Practice Questions

12.0 WEB SERVERS, WEB APPLICATIONS, AND SQL INJECTIONS

12.1 Web Servers

- 12.1.1 Web Server Hacking (3:38)
- 12.1.2 Web Server Hacking Facts
- 12.1.3 Web Server Attacks (5:05)
- 12.1.4 Web Server Attack Facts
- 12.1.5 Mirror a Website with HTTrack (2:13)
- 12.1.6 Extract Web Server Information (4:30)
- 12.1.7 Extract Web Server Information with Nmap
- 12.1.8 Crack FTP Credentials with Wireshark
- 12.1.9 Web Server Countermeasures (4:58)

- 12.1.10 Web Server Countermeasures Facts
- 12.1.11 Practice Questions

12.2 Web Applications

- 12.2.1 Web Applications (4:39)
- 12.2.2 Web Application Facts
- 12.2.3 Web Application Hacking (5:32)
- 12.2.4 Web Application Hacking Facts
- 12.2.5 Hidden Field Manipulation Attacks (2:36)
- 12.2.6 Exploit Cross-Site Scripting Vulnerabilities (2:57)
- 12.2.7 Web Application Countermeasures (6:43)
- 12.2.8 Scan a Website with Acunetix (4:17)
- 12.2.9 Web Application Countermeasure Facts
- 12.2.10 Practice Questions

12.3 SQL Injections

- 12.3.1 SQL Injection (5:52)
- 12.3.2 SQL Injection Facts
- 12.3.3 SQL Injection Attack Types (4:32)
- 12.3.4 SQL Injection Attack Facts
- 12.3.5 Exploit SQL on a Web Page (3:57)
- 12.3.6 Perform an SQL Injection Attack
- 12.3.7 SQL Injection Countermeasures (2:26)
- 12.3.8 SQL Injection Countermeasure Facts
- 12.3.9 Practice Questions

13.0 WI-FI, BLUETOOTH, AND MOBILE DEVICES

13.1 Wi-Fi

- 13.1.1 Wireless Overview (9:31)
- 13.1.2 Wireless Facts
- 13.1.3 Wireless Encryption and Authentication (8:56)
- 13.1.4 Wireless Encryption and Authentication Facts
- 13.1.5 Wireless Hacking (10:51)
- 13.1.6 Wireless Hacking Facts
- 13.1.7 Wi-Fi Packet Analysis (5:33)
- 13.1.8 Crack Wi-Fi Encryption with Aircrack-ng (5:40)
- 13.1.9 Discover a Hidden Network
- 13.1.10 Wireless Hacking Countermeasure Tools (11:12)
- 13.1.11 Wireless Hacking Countermeasures Tool Facts

- 13.1.12 Detect a Rogue Device (5:53)
- 13.1.13 Discover a Rogue DHCP Server
- 13.1.14 Locate a Rogue Wireless Access Point
- 13.1.15 Practice Questions

13.2 Bluetooth Hacking

- 13.2.1 Bluetooth Hacking (6:45)
- 13.2.2 Bluetooth Hacking Facts
- 13.2.3 Discover Vulnerable Bluetooth Devices (3:28)
- 13.2.4 Discover Bluetooth Devices
- 13.2.5 Practice Questions

13.3 Mobile Devices

- 13.3.1 Mobile Device Attacks (7:52)
- 13.3.2 Mobile Device Attack Facts
- 13.3.3 Mobile Device Operating Systems (8:58)
- 13.3.4 Mobile Device Operating System Facts
- 13.3.5 Secure a Device (5:43)
- 13.3.6 Secure a Mobile Device
- 13.3.7 Mobile Device Hacking (7:54)
- 13.3.8 Hack Android with Binary Payloads (7:18)
- 13.3.9 Mobile Device Hacking Facts
- 13.3.10 Mobile Device Management (6:00)
- 13.3.11 Mobile Device Management Facts
- 13.3.12 Practice Questions

14.0 CLOUD COMPUTING AND INTERNET OF THINGS

14.1 Cloud Computing

- 14.1.1 Cloud Computing (13:06)
- 14.1.2 Cloud Computing Facts
- 14.1.3 Cloud Computing Threats (6:13)
- 14.1.4 Cloud Threats Facts
- 14.1.5 Cloud Computing Attacks (9:04)
- 14.1.6 Cloud Attacks Facts
- 14.1.7 Cloud Security (6:40)
- 14.1.8 Cloud Security Facts
- 14.1.9 Secure Files in the Cloud (3:52)
- 14.1.10 Practice Questions

14.2 Internet of Things

- 14.2.1 Internet of Things (6:40)
- 14.2.2 Internet of Things Facts
- 14.2.3 IoT Technologies and Protocols (8:37)
- 14.2.4 IoT Technologies and Protocols Facts
- 14.2.5 IoT Security Challenges (7:17)
- 14.2.6 IoT Security Challenge Facts
- 14.2.7 IoT Hacking (6:14)
- 14.2.8 IoT Hacking Facts
- 14.2.9 Search for IoT with Shodan (4:38)
- 14.2.10 Scan for IoT with Nmap (3:23)
- 14.2.11 Scan for IoT Devices
- 14.2.12 Practice Questions

15.0 CRYPTOGRAPHY

15.1 Cryptography

- 15.1.1 Cryptography (5:22)
- 15.1.2 Cryptography Facts
- 15.1.3 Symmetric Encryption (4:11)
- 15.1.4 Symmetric Encryption Facts
- 15.1.5 Asymmetric Encryption (5:40)
- 15.1.6 Asymmetric Encryption Facts
- 15.1.7 Verify MD5 Hash Integrity (2:50)
- 15.1.8 Compare an MD5 Hash
- 15.1.9 Practice Questions

15.2 Public Key Infrastructure

- 15.2.1 Public Key Infrastructure (6:49)
- 15.2.2 Public Key Infrastructure Facts
- 15.2.3 Practice Questions

15.3 Cryptography Implementations

- 15.3.1 Disk and Email Encryption (5:58)
- 15.3.2 PGP and GPG (4:22)
- 15.3.3 Disk and Email Encryption Facts
- 15.3.4 Encrypt Files with GPG (5:46)
- 15.3.5 Encrypt a Hard Disk (6:01)
- 15.3.6 Encrypt a Hard Drive
- 15.3.7 Practice Questions

15.4 Cryptanalysis and Cryptographic Attack Countermeasures

- 15.4.1 Cryptanalysis and Cryptographic Attack Countermeasures (5:56)
- 15.4.2 Cryptanalysis and Cryptographic Attack Countermeasures Facts
- 15.4.3 Data Encryption (4:31)
- 15.4.4 Practice Questions

A.0 TESTOUT ETHICAL HACKER PRO - PRACTICE EXAMS

A.1 Prepare for Certification

- A.1.1 TestOut Ethical Hacker Pro Exam Objectives
- A.1.2 TestOut Ethical Hacker Pro Objectives by Course Section
- A.1.3 How to Take the Certification Exam
- A.1.4 Certification FAQs

A.2 TestOut Ethical Hacker Pro Domain Review

- A.2.1 Domain 1: Prepare
- A.2.2 Domain 2: Gain Access
- A.2.3 Domain 3: Attack
- A.2.4 Domain 4: Cover Up
- A.2.5 Domain 5: Defend a System

A.3 TestOut Ethical Hacker Pro Certification Practice Exam

B.0 EC-COUNCIL CERTIFIED ETHICAL HACKER - PRACTICE EXAMS

B.1 Prepare for Certification

- B.1.1 EC-Council EH Objectives
- B.1.2 EC-Council EH Objectives by Course Section
- B.1.3 How to Register for an Exam
- B.1.4 Exam FAQs
- B.1.5 Exam-Taking Hints and Tips

B.2 EC-Council CEH Practice Exams (20 Questions)

- B.2.1 EC-Council CEH Domain 1: Background
- B.2.2 EC-Council CEH Domain 2: Analysis/Assessment
- B.2.3 EC-Council CEH Domain 3: Security
- B.2.4 EC-Council CEH Domain 4: Tools/Systems/Programs
- B.2.5 EC-Council CEH Domain 5: Procedures/Methodology
- B.2.6 EC-Council CEH Domain 6: Regulation/Policy
- B.2.7 EC-Council CEH Domain 7: Ethics

B.3 EC-Council CEH Practice Exams (All Questions)

- B.3.1 EC-Council CEH Domain 1: Background
- B.3.2 EC-Council CEH Domain 2: Analysis/Assessment

- B.3.3 EC-Council CEH Domain 3: Security
- B.3.4 EC-Council CEH Domain 4: Tools/Systems/Programs
- B.3.5 EC-Council CEH Domain 5: Procedures/Methodology
- B.3.6 EC-Council CEH Domain 6: Regulation/Policy
- B.3.7 EC-Council CEH Domain 7: Ethics

- B.4 EC-Council CEH Practice Exam