TestOut

TestOut Ethical Hacker Pro – English 1.0.x

Objective Mappings:

TestOut Ethical Hacker Pro 1.0

EC-Council Certified Ethical Hacker v10 Exam Blueprint 3.0

Revised: 2020-05-19

Powered by LABSIM

Contents

This document contains four objective mappings. Click on a mapping to view its contents.

Objective Mapping: LabSim Section to TestOut Ethical Hacker Pro 1.0 Objectives

The TestOut Ethical Hacker Pro course covers the following TestOut Ethical Hacker Pro exam objectives:

Section	Title	Objectives
1.0	**Introduction to Ethical Hacking**	
1.1	Introduction	
2.0	**Introduction to Penetration Testing**	
2.1	Penetration Testing Process and Types	
2.2	Threat Actors	
2.3	Target Selection	
2.4	Assessment Types	
2.5	Legal and Ethical Compliance	
3.0	**Social Engineering and Physical Security**	
3.1	Social Engineering	2.1 Obtain login credentials Use Social Engineering
3.2	Physical Security	
3.3	Countermeasures and Prevention	5.2 Implement defensive systems

		Implement physical security countermeasures
4.0	**Reconnaissance**	
4.1	Reconnaissance Overview	1.1 Perform reconnaissance Perform reconnaissance with hacking tools
4.2	Reconnaissance Countermeasures	5.1 Defend systems and devices Hide a web server banner broadcast 5.2 Implement defensive systems Disable unnecessary services
5.0	**Scanning**	
5.1	Scanning Overview	1.2 Perform scanning Scan for network devices
5.2	Banner Grabbing	
6.0	**Enumeration**	
6.1	Enumeration Overview	1.2 Perform scanning Detect operating systems and applications 1.3 Perform enumeration Enumerate network resources

		Enumerate device information
6.2	Enumeration Countermeasures	5.2 Implement defensive systems Prevent DNS zone transfer
7.0	**Analyze Vulnerabilities**	
7.1	Vulnerability Assessment	
7.2	Vulnerability Management Life Cycle	
7.3	Vulnerability Scoring Systems	
7.4	Vulnerability Assessment Tools	1.2 Perform scanning Scan for vulnerabilities
8.0	**System Hacking**	
8.1	System Hacking	1.1 Perform reconnaissance Perform reconnaissance with operating system tools 2.1 Obtain login credentials Obtain credentials using tools 5.1 Defend systems and devices Configure account policies and account control
8.2	Privilege Escalation	2.2 Gain administrative access and escalate privileges

		Escalate privileges 5.1 Defend systems and devices Configure account policies and account control
8.3	Maintain Access	2.2 Gain administrative access and escalate privileges Gain access through a backdoor
8.4	Cover Your Tracks	4.1 Cover up access Disable auditing Clear logs Remove or hide files and folders
9.0	**Malware**	
9.1	Malware	
9.2	Combat Malware	1.2 Perform scanning Identify open ports 5.1 Defend systems and devices Use malware protection
10.0	**Sniffers, Session Hijacking, and Denial of Service**	

10.1	Sniffing	3.1 Perform passive online attacks Conduct a man-in-the-middle attack Perform passive sniffing 3.2 Perform active online attacks Perform active sniffing 4.1 Cover up access Change MAC address
10.2	Session Hijacking	2.2 Gain administrative access and escalate privileges Hijack a web session 3.1 Perform passive online attacks Examine hidden web form fields Conduct a man-in-the-middle attack
10.3	Denial of Service	3.2 Perform active online attacks Execute a DoS or DDoS attack
11.0	**IDS, Firewalls, and Honeypots**	
11.1	Intrusion Detection Systems	5.2 Implement defensive systems Implement an Intrusion Detection System (IDS)

11.2	Firewalls	3.3 Perform infrastructure attacks Evade firewalls, IDSs, and honeypots 5.2 Implement defensive systems Configure a perimeter firewall
11.3	Honeypots	5.2 Implement defensive systems Create a honeypot
12.0	**Web Servers, Web Applications, and SQL Injections**	
12.1	Web Servers	2.1 Obtain login credentials Obtain credentials using tools 3.3 Perform infrastructure attacks Attack a web server
12.2	Web Applications	
12.3	SQL Injections	3.2 Perform active online attacks Perform an SQL injection
13.0	**Wi-Fi, Bluetooth, and Mobile Devices**	

13.1	Wi-Fi	1.2 Perform scanning Discover wireless devices 2.2 Gain administrative access and escalate privileges Crack Wi-Fi devices 3.3 Perform infrastructure attacks Access wireless networks 5.1 Defend systems and devices Discover rogue hosts
13.2	Bluetooth Hacking	1.2 Perform scanning Discover wireless devices
13.3	Mobile Devices	5.1 Defend systems and devices Secure mobile devices
14.0	**Cloud Computing and Internet of Things**	
14.1	Cloud Computing	
14.2	Internet of Things	1.2 Perform scanning Scan for IoT devices
15.0	**Cryptography**	

15.1	Cryptography	5.1 Defend systems and devices Ensure file integrity
15.2	Public Key Infrastructure	
15.3	Cryptography Implementations	5.1 Defend systems and devices Implement drive encryption
15.4	Cryptanalysis and Cryptographic Attack Countermeasures	
A.0	**TestOut Ethical Hacker Pro - Practice Exams**	
A.1	Prepare for Certification	
A.2	TestOut Ethical Hacker Pro Domain Review	
B.0	**EC-Council Certified Ethical Hacker - Practice Exams**	
B.1	Prepare for Certification	
B.2	EC-Council CEH Practice Exams (20 Questions)	
B.3	EC-Council CEH Practice Exams (All Questions)	

Objective Mapping: TestOut Ethical Hacker Pro 1.0 Objectives to LabSim Section

The TestOut Ethical Hacker Pro course and certification exam cover the following TestOut Ethical Hacker Pro objectives:

#	Domain	Section
1.0	**Prepare**	
1.1	Perform reconnaissance Perform reconnaissance with operating system tools Perform reconnaissance with hacking tools	4.1 8.1
1.2	Perform scanning Scan for network devices Discover wireless devices Scan for IoT devices Detect operating systems and applications Identify open ports Scan for vulnerabilities	5.1 6.1 7.4 9.2 13.1, 13.2 14.2
1.3	Perform enumeration Enumerate network resources Enumerate device information	6.1
2.0	**Gain Access**	

2.1	Obtain login credentials Obtain credentials using tools Use Social Engineering	3.1 8.1 12.1
2.2	Gain administrative access and escalate privileges Gain access through a backdoor Escalate privileges Hijack a web session Crack Wi-Fi devices	8.2, 8.3 10.2 13.1
3.0	**Attack**	
3.1	Perform passive online attacks Examine hidden web form fields Conduct a man-in-the-middle attack Perform passive sniffing	10.1, 10.2
3.2	Perform active online attacks Perform an SQL injection Execute a DoS or DDoS attack Perform active sniffing	10.1, 10.3 12.3
3.3	Perform infrastructure attacks Attack a web server Access wireless networks Evade firewalls, IDSs, and honeypots	11.2 12.1 13.1
4.0	**Cover Up**	

4.1	Cover up access Disable auditing Clear logs Remove or hide files and folders Change MAC address	8.4 10.1
5.0	**Defend System**	
5.1	Defend systems and devices Hide a web server banner broadcast Discover rogue hosts Secure mobile devices Configure account policies and account control Ensure file integrity Implement drive encryption Use malware protection	4.2 8.1, 8.2 9.2 13.1, 13.3 15.1, 15.3
5.2	Implement defensive systems Implement an Intrusion Detection System (IDS) Create a honeypot Prevent DNS zone transfer Disable unnecessary services Implement physical security countermeasures Configure a perimeter firewall	3.3 4.2 6.2 11.1, 11.2, 11.3

Objective Mapping: LabSim Section to EC-Council Certified Ethical Hacker v10 Exam Blueprint 3.0 Objectives

The TestOut Ethical Hacker Pro course covers the following EC-Council Certified Ethical Hacker v10 Exam Blueprint 3.0 exam objectives:

Section	Title	Objectives
1.0	**Introduction to Ethical Hacking**	
1.1	Introduction	
2.0	**Introduction to Penetration Testing**	
2.1	Penetration Testing Process and Types	5. Procedures/Methodology Information Security Assessment Methodologies
2.2	Threat Actors	1. Background Information Security Threats and Attack Vector
2.3	Target Selection	1. Background Information Security Threats and Attack Vector
2.4	Assessment Types	2. Analysis/Assessment Information Security Assessment and Analysis Information Security Assessment Process

		5. Procedures/Methodology Information Security Procedures Information Security Assessment Methodologies
2.5	Legal and Ethical Compliance	6. Regulation/Policy Information Security Policies/Laws/Acts 7. Ethics Ethics of Information Security
3.0	**Social Engineering and Physical Security**	
3.1	Social Engineering	1. Background Information Security Threats and Attack Vector 3. Security Information Security Attack Detection 4. Tools/Systems/Programs Information Security Tools 5. Procedures/Methodology Information Security Assessment Methodologies
3.2	Physical Security	1. Background

		Information Security Threats and Attack Vector 3. Security Information Security Controls
3.3	Countermeasures and Prevention	1. Background Information Security Threats and Attack Vector 3. Security Information Security Attack Detection Information Security Attack Prevention
4.0	**Reconnaissance**	
4.1	Reconnaissance Overview	4. Tools/Systems/Programs Information Security Tools 5. Procedures/Methodology Information Security Procedures
4.2	Reconnaissance Countermeasures	3. Security Information Security Attack Prevention 4. Tools/Systems/Programs Information Security Systems

		Information Security Tools
5.0	**Scanning**	
5.1	Scanning Overview	3. Security Information Security Attack Prevention 4. Tools/Systems/Programs Information Security Tools 5. Procedures/Methodology Information Security Procedures
5.2	Banner Grabbing	3. Security Information Security Attack Detection Information Security Attack Prevention 4. Tools/Systems/Programs Information Security Tools
6.0	**Enumeration**	
6.1	Enumeration Overview	1. Background Network and Communication Technologies 3. Security

		Information Security Attack Detection 4. Tools/Systems/Programs Information Security Systems Information Security Tools 5. Procedures/Methodology Information Security Procedures
6.2	Enumeration Countermeasures	3. Security Information Security Attack Prevention 4. Tools/Systems/Programs Information Security Tools 5. Procedures/Methodology Information Security Procedures
7.0	**Analyze Vulnerabilities**	
7.1	Vulnerability Assessment	2. Analysis/Assessment Information Security Assessment and Analysis 5. Procedures/Methodology Information Security Procedures Information Security Assessment Methodologies

7.2	Vulnerability Management Life Cycle	2. Analysis/Assessment Information Security Assessment Process 5. Procedures/Methodology Information Security Procedures Information Security Assessment Methodologies
7.3	Vulnerability Scoring Systems	4. Tools/Systems/Programs Information Security Tools 5. Procedures/Methodology Information Security Assessment Methodologies
7.4	Vulnerability Assessment Tools	2. Analysis/Assessment Information Security Assessment and Analysis 4. Tools/Systems/Programs Information Security Tools
8.0	**System Hacking**	
8.1	System Hacking	1. Background Information Security Threats and Attack Vector 3. Security

		Information Security Attack Detection Information Security Attack Prevention 4. Tools/Systems/Programs Information Security Tools
8.2	Privilege Escalation	1. Background Information Security Threats and Attack Vector 3. Security Information Security Attack Prevention 4. Tools/Systems/Programs Information Security Tools 5. Procedures/Methodology Information Security Procedures
8.3	Maintain Access	4. Tools/Systems/Programs Information Security Tools 5. Procedures/Methodology Information Security Procedures
8.4	Cover Your Tracks	4. Tools/Systems/Programs

		Information Security Programs Information Security Tools 5. Procedures/Methodology Information Security Assessment Methodologies
9.0	**Malware**	
9.1	Malware	2. Analysis/Assessment Information Security Assessment and Analysis 3. Security Information Security Attack Detection Information Security Attack Prevention 4. Tools/Systems/Programs Information Security Tools 5. Procedures/Methodology Information Security Procedures 6. Regulation/Policy Information Security Policies/Laws/Acts
9.2	Combat Malware	3. Security Information Security Attack Prevention

		4. Tools/Systems/Programs Information Security Tools
10.0	**Sniffers, Session Hijacking, and Denial of Service**	
10.1	Sniffing	3. Security Information Security Attack Detection Information Security Attack Prevention 4. Tools/Systems/Programs Information Security Tools
10.2	Session Hijacking	3. Security Information Security Attack Detection Information Security Attack Prevention 4. Tools/Systems/Programs Information Security Tools
10.3	Denial of Service	3. Security Information Security Controls Information Security Attack Detection Information Security Attack Prevention 4. Tools/Systems/Programs

		Information Security Tools 5. Procedures/Methodology Information Security Procedures
11.0	**IDS, Firewalls, and Honeypots**	
11.1	Intrusion Detection Systems	1. Background Information Security Technologies 3. Security Information Security Attack Detection Information Security Attack Prevention 4. Tools/Systems/Programs Information Security Systems Information Security Tools 5. Procedures/Methodology Information Security Assessment Methodologies
11.2	Firewalls	1. Background Information Security Technologies 3. Security Information Security Attack Detection

		Information Security Attack Prevention 4. Tools/Systems/Programs Information Security Systems Information Security Tools 5. Procedures/Methodology Information Security Assessment Methodologies
11.3	Honeypots	1. Background Information Security Technologies 3. Security Information Security Attack Detection Information Security Attack Prevention 4. Tools/Systems/Programs Information Security Systems Information Security Programs Information Security Tools
12.0	**Web Servers, Web Applications, and SQL Injections**	
12.1	Web Servers	1. Background Information Security Technologies 3. Security

		Information Security Attack Detection Information Security Attack Prevention 4. Tools/Systems/Programs Information Security Tools 5. Procedures/Methodology Information Security Procedures
12.2	Web Applications	3. Security Information Security Attack Detection Information Security Attack Prevention 4. Tools/Systems/Programs Information Security Tools 5. Procedures/Methodology Information Security Procedures
12.3	SQL Injections	3. Security Information Security Attack Detection Information Security Attack Prevention 4. Tools/Systems/Programs Information Security Tools

13.0	Wi-Fi, Bluetooth, and Mobile Devices	
13.1	Wi-Fi	2. Analysis/Assessment Information Security Assessment and Analysis 3. Security Information Security Controls Information Security Attack Detection Information Security Attack Prevention 4. Tools/Systems/Programs Information Security Tools 5. Procedures/Methodology Information Security Procedures
13.2	Bluetooth Hacking	3. Security Information Security Attack Detection
13.3	Mobile Devices	1. Background Network and Communication Technologies Information Security Threats and Attack Vector Information Security Technologies 3. Security Information Security Attack Detection

		Information Security Attack Prevention 4. Tools/Systems/Programs Information Security Tools 5. Procedures/Methodology Information Security Procedures
14.0	**Cloud Computing and Internet of Things**	
14.1	Cloud Computing	1. Background Network and Communication Technologies Information Security Threats and Attack Vector Information Security Technologies 3. Security Information Security Controls 4. Tools/Systems/Programs Information Security Tools
14.2	Internet of Things	1. Background Network and Communication Technologies Information Security Threats and Attack Vector Information Security Technologies 4. Tools/Systems/Programs

		Information Security Tools 5. Procedures/Methodology Information Security Procedures
15.0	**Cryptography**	
15.1	Cryptography	3. Security Information Security Attack Prevention 4. Tools/Systems/Programs Information Security Tools 5. Procedures/Methodology Information Security Procedures
15.2	Public Key Infrastructure	5. Procedures/Methodology Information Security Procedures
15.3	Cryptography Implementations	3. Security Information Security Attack Prevention 4. Tools/Systems/Programs Information Security Tools

15.4	Cryptanalysis and Cryptographic Attack Countermeasures	3. Security Information Security Attack Detection Information Security Attack Prevention 4. Tools/Systems/Programs Information Security Programs Information Security Tools
A.0	**TestOut Ethical Hacker Pro - Practice Exams**	
A.1	Prepare for Certification	
A.2	TestOut Ethical Hacker Pro Domain Review	
B.0	**EC-Council Certified Ethical Hacker - Practice Exams**	
B.1	Prepare for Certification	
B.2	EC-Council CEH Practice Exams (20 Questions)	
B.3	EC-Council CEH Practice Exams (All Questions)	

Objective Mapping: EC-Council Certified Ethical Hacker v10 Exam Blueprint 3.0 Objectives to LabSim Section

The TestOut Ethical Hacker Pro course and certification exam cover the following EC-Council Certified Ethical Hacker v10 Exam Blueprint 3.0 objectives:

#	Domain	Section
1.	**Background**	
1.	Background Network and Communication Technologies Information Security Threats and Attack Vector Information Security Technologies	2.2, 2.3 3.1, 3.2, 3.3 6.1 8.1, 8.2 11.1, 11.2, 11.3 12.1 13.3 14.1, 14.2
2.	**Analysis/Assessment**	
2.	Analysis/Assessment Information Security Assessment and Analysis Information Security Assessment Process	2.4 7.1, 7.2, 7.4 9.1 13.1
3.	**Security**	
3.	Security Information Security Controls Information Security Attack Detection Information Security Attack Prevention	3.1, 3.2, 3.3 4.2 5.1, 5.2 6.1, 6.2 8.1, 8.2 9.1, 9.2 10.1, 10.2, 10.3 11.1, 11.2, 11.3

		12.1, 12.2, 12.3 13.1, 13.2, 13.3 14.1 15.1, 15.3, 15.4
4.	**Tools/Systems/Programs**	
4.	Tools/Systems/Programs Information Security Systems Information Security Programs Information Security Tools	3.1 4.1, 4.2 5.1, 5.2 6.1, 6.2 7.3, 7.4 8.1, 8.2, 8.3, 8.4 9.1, 9.2 10.1, 10.2, 10.3 11.1, 11.2, 11.3 12.1, 12.2, 12.3 13.1, 13.3 14.1, 14.2 15.1, 15.3, 15.4
5.	**Procedures/Methodology**	
5.	Procedures/Methodology Information Security Procedures Information Security Assessment Methodologies	2.1, 2.4 3.1 4.1 5.1 6.1, 6.2 7.1, 7.2, 7.3 8.2, 8.3, 8.4 9.1 10.3 11.1, 11.2 12.1, 12.2 13.1, 13.3 14.2 15.1, 15.2
6.	**Regulation/Policy**	

6.	Regulation/Policy Information Security Policies/Laws/Acts	2.5 9.1
7.	**Ethics**	
7.	Ethics Ethics of Information Security	2.5