

TestOut[®]

TestOut Ethical Hacker Pro - English 1.0.x

LESSON PLAN

Table of Contents

| | |
|--|----|
| Table of Contents | 2 |
| 1.1: Introduction | 3 |
| 2.1: Penetration Testing Process and Types | 5 |
| 2.2: Threat Actors | 6 |
| 2.3: Target Selection | 8 |
| 2.4: Assessment Types | 9 |
| 2.5: Legal and Ethical Compliance | 11 |
| 3.1: Social Engineering | 13 |
| 3.2: Physical Security | 16 |
| 3.3: Countermeasures and Prevention | 18 |
| 4.1: Reconnaissance Overview | 20 |
| 4.2: Reconnaissance Countermeasures | 22 |
| 5.1: Scanning Overview | 24 |
| 5.2: Banner Grabbing | 26 |
| 6.1: Enumeration Overview | 27 |
| 6.2: Enumeration Countermeasures | 29 |
| 7.1: Vulnerability Assessment | 31 |
| 7.2: Vulnerability Management Life Cycle | 33 |
| 7.3: Vulnerability Scoring Systems | 35 |
| 7.4: Vulnerability Assessment Tools | 37 |
| 8.1: System Hacking | 39 |
| 8.2: Privilege Escalation | 42 |
| 8.3: Maintain Access | 44 |
| 8.4: Cover Your Tracks | 46 |
| 9.1: Malware | 48 |
| 9.2: Combat Malware | 50 |
| 10.1: Sniffing | 52 |
| 10.2: Session Hijacking | 54 |
| 10.3: Denial of Service | 56 |
| 11.1: Intrusion Detection Systems | 58 |
| 11.2: Firewalls | 61 |
| 11.3: Honeypots | 64 |
| 12.1: Web Servers | 66 |
| 12.2: Web Applications | 68 |
| 12.3: SQL Injections | 70 |
| 13.1: Wi-Fi | 72 |
| 13.2: Bluetooth Hacking | 76 |
| 13.3: Mobile Devices | 78 |
| 14.1: Cloud Computing | 81 |
| 14.2: Internet of Things | 85 |
| 15.1: Cryptography | 89 |
| 15.2: Public Key Infrastructure | 93 |
| 15.3: Cryptography Implementations | 94 |
| 15.4: Cryptanalysis and Cryptographic Attack Countermeasures | 96 |
| Practice Exams | 98 |
| Appendix A: Approximate Time for the Course | 99 |

1.1: Introduction

Summary

This course is designed to prepare you to pass the TestOut Ethical Hacker Pro and EC-Council Certified Ethical Hacker certifications. This certification measures not just what you know, but what you can do to evaluate a system's security and make recommendations to make the system more secure.

This section introduction covers the following topics:

- Course purpose
- Course prerequisites
- Certifications

Course Purpose

The purpose of this course is to allow students and IT professionals to move into the cybersecurity field. The course covers the five phases of ethical hacking:

- Reconnaissance: also known as the preparatory phase, the reconnaissance phase is the phase in which the hacker gathers information about a target before launching an attack. This task is completed in phases prior to exploiting system vulnerabilities.
- Scanning: in the scanning phase, the hacker identifies a quick way to gain access to the network and look for information.
- Gain access: hackers gain access to the system, applications, and network, and then escalate user privileges to take control of systems.
- Maintain access: the hacker continues accessing the organization's systems to launch additional attacks on the network.
- Cover your tracks: after the hacker gains access, it is necessary to cover evidence of the system having been hacked to avoid being detected by security personnel.

Course Prerequisites

Although there are no official prerequisites, we've created this course with the expectation that you already know the following:




- What a network is
- How a network functions
- IP addressing
- Subnetting
- DNS
- DHCP
- Basic security practices

Certifications

This course meets the specifications for two industry certification programs:

| Certification | Definition |
|-------------------------------------|--|
| TestOut Ethical Hacker Pro | <p>The TestOut Ethical Hacker Pro certification measures how much you know and what you can do. The Ethical Hacker Pro certification validates that you have the equivalent knowledge of two years of work experience in the cybersecurity field. The exam focuses on the basics of penetration testing and ethical hacking. It also helps the student be aware of network attack strategies and common countermeasures. It prepares students to use various testing tools to analyze networks for vulnerabilities. Knowledge of these vulnerabilities also helps students understand how to counter these vulnerabilities and improve network security. To get your Ethical Hacker Pro certification, you'll perform real-world tasks in a simulated environment.</p> |
| EC-Council Certified Ethical Hacker | <p>The Certified Ethical Hacker (CEH) is a qualification obtained from EC-Council. EC-Council states that 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 in a lawful and legitimate manner to assess the security posture of a target system. This knowledge is assessed by answering multiple-choice questions regarding various ethical hacking techniques and tools.</p> <p>The code for the current CEH exam is 312-50. To take the exam, a candidate must have two years of work experience in the information security domain and pay a \$100 fee with their application. The current cost of the exam is \$1199 if it's taken at a Pearson VUE test center or \$950 if it's taken through EC-Council. This exam fee is in addition to the \$100 application fee. For the latest requirements, check the EC-Council website at www.eccouncil.org.</p> |

Video/Demo

-  1.1.1 Introduction to Ethical Hacker Pro
-  1.1.2 Use the Simulator
-  1.1.3 Explore the New Lab Features

Time

5:13

14:55

10:17

Total Video Time

30:25

Total Time

About 31 minutes

2.1: Penetration Testing Process and Types

Lecture Focus Questions:

- What is penetration testing and ethical hacking?
- What are the differences between penetration testing and ethical hacking?
- Who performs a penetration test?
- What are the different types of penetration tests?

Key terms for this section include the following:

| Term | Definition |
|---------------------|---|
| Ethical hacking | Perpetrating exploits against a system with the intent to find vulnerabilities so that security weaknesses can be addressed and the system can be made more secure. |
| Penetration testing | The practice of finding vulnerabilities and risks with the purpose of securing the computer or network system. |
| Red team | An offensive security team that attempts to discover vulnerabilities in a network or computer system. |
| Blue team | A defensive security team that attempts to close vulnerabilities and stop the red team. |
| Purple team | A mixture of both red and blue teams. |

This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|------------|---|
| EC-Council | 5. Procedures/Methodology <ul style="list-style-type: none"> • Information Security Assessment Methodologies |

Video/Demo

- 📺 2.1.1 Penetration Test Process and Types

Total Video Time

Time

4:42

4:42

Fact Sheets

- 📄 2.1.2 Penetration Test Process and Types Facts

Number of Exam Questions

8 questions

Total Time

About 18 minutes

2.2: Threat Actors

Lecture Focus Questions:

- What are the different categories of hackers?
- What are common motivations for a hacker?
- What separates a hacker from a script kiddie?
- Do today's hackers need as much technical knowledge as previous hackers?

Key terms for this section include the following:

| Term | Definition |
|----------------------------------|---|
| Advanced persistent threat (APT) | A stealthy computer network attack in which a person or group gains unauthorized access to a network and remains undetected for an extended period. |
| Threat modeling | The process of analyzing the security of the organization and determine security holes. |
| White hat | A skilled hacker who uses skills and knowledge for defensive purposes only. The white hat hacker interacts only with systems for which express access permission has been given. |
| Black hat | A skilled hacker who uses skills and knowledge for illegal or malicious purposes. |
| Gray hat | A skilled hacker who falls in the middle of the white hat and black hat hackers. The gray hat may cross the line of what is ethical, but usually has good intentions and isn't malicious like a black hat hacker. |
| Suicide hacker | A hacker who is concerned only with taking down the target for a cause. |
| Cyber terrorist | A hacker motivated by religious or political beliefs who wants to create severe disruption or widespread fear. |
| State-sponsored hacker | A hacker who works for a government and attempts to gain top-secret information by hacking other governments. |
| Hactivist | A hacker whose main purpose is to protest an event or situation and draw attention to their own views and opinions. |
| Script kiddie | An extremely unskilled person who uses tools and scripts developed by real hackers. |

This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|------------|--|
| EC-Council | 1. Background <ul style="list-style-type: none"> • Information Security Threats and Attack Vector |

Video/Demo 2.2.1 Threat Actor Types**Total Video Time****Time**6:35**6:35****Fact Sheets** 2.2.2 Threat Actor Type Facts**Number of Exam Questions**

5 questions

Total Time*About 17 minutes*

2.3: Target Selection

Lecture Focus Questions:



- What is the scope of work? What does it include?
- What are the rules of engagement?
- What is the difference between an internal target and an external target?

Key terms for this section include the following:

| Term | Definition |
|---------------------|--|
| Scope of work | A scope of work (SOW) defines exactly what a project will entail. It is also known as a statement of work. |
| Rules of engagement | A rules of engagement (ROE) defines how the penetration test will be carried out. |

This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|------------|--|
| EC-Council | 1. Background <ul style="list-style-type: none"> • Information Security Threats and Attack Vector |

| Video/Demo | Time |
|---|-------------|
|  2.3.1 Choose a Target | 3:41 |
|  2.3.2 Additional Scoping Considerations | <u>5:05</u> |
| Total Video Time | 8:46 |

Fact Sheets

-  2.3.3 Target Selection Facts

Number of Exam Questions

15 questions

Total Time

About 29 minutes

2.4: Assessment Types

Lecture Focus Questions:

- What are the different types of penetration tests?
- How does being part of a supply chain affect a penetration test?
- Why would a penetration test be performed before a merger of two organizations?
- What are the main laws and regulations a penetration tester needs to be aware of?

Key terms for this section include the following:

| Term | Definition |
|---|--|
| Payment Card Industry Data Security Standards (PCI-DSS) | Security standards for any organization that handles cardholder information for debit cards, credit cards, prepaid cards, and other types of payment cards. |
| Health Insurance Portability and Accountability Act (HIPAA) | A set of standards that ensures a person's health information is kept safe and shared only with the patient and medical professionals who need it. |
| ISO/IEC 27001 | A set of processes and requirements for an organization's information security management systems. |
| Sarbanes Oxley Act (SOX) | Federal regulation enacted in 2002 with the goal of implementing accounting and disclosure requirements that would increase transparency in corporate governance and financial reporting and formalize a system of internal checks and balances. |
| Digital Millennium Copyright Act (DMCA) | A federal regulation enacted in 1998 that is designed to protect copyrighted works. |
| Federal Information Security Management Act (FISMA) | A federal regulation that defines how federal government data, operations, and assets are handled. |

This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|------------|--|
| EC-Council | 2. Analysis/Assessment <ul style="list-style-type: none"> • Information Security Assessment and Analysis • Information Security Assessment Process |
| | 5. Procedures/Methodology <ul style="list-style-type: none"> • Information Security Procedures |

- Information Security Assessment Methodologies

| Video/Demo | Time |
|--------------------------------|-------------|
| ▣ 2.4.1 Assessment Types | 4:49 |
| ▣ 2.4.2 Special Considerations | <u>2:08</u> |
| Total Video Time | 6:57 |

Fact Sheets

- ▣ 2.4.3 Assessment Type Facts

Number of Exam Questions

13 questions

Total Time

About 25 minutes

2.5: Legal and Ethical Compliance

Lecture Focus Questions:

- What laws and regulations does the penetration tester need to be aware of?
- What special considerations are needed when performing a penetration test on a cloud-based service?
- How are local laws and regulations handled when the penetration tester and client are in different states?
- How can corporate policies affect the penetration test?
- What documents should be included in a penetration test contract?

Key terms for this section include the following:

| Term | Definition |
|--------------------------------|--|
| Wassenaar Arrangement | An agreement between 41 countries to hold similar export controls on weapons, including banning some and requiring licensing for others, like intrusion software. |
| Bring your own device (BYOD) | Policies that govern an organization's rules and regulations regarding support of employee-owned smart phones, tablets, and similar devices. |
| Scope of work (SoW) | A very detailed document that defines exactly what is going to be included in the penetration test. This document is also referred to as the statement of work. |
| Rules of engagement (RoE) | A document that defines exactly how the work will be carried out. |
| Master service agreement (MSA) | A contract where parties agree to the terms that will govern future actions. This makes future services and contracts easier to handle and define. |
| Non-disclosure agreement (NDA) | A common legal contract that outlines confidential material or information that will be shared during a security assessment and what restrictions are placed on information. |
| Permission to test | A document that explains what the penetration tester is doing and that their work is authorized. This document is sometimes referred to as the Get Out Of Jail Free Card. |

This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|------------|---|
| EC-Council | 6. Regulation/Policy |
| | • Information Security Policies/Laws/Acts |
| | 7. Ethics |

- Ethics of Information Security

| Video/Demo | Time |
|--|--------------|
| 📺 2.5.1 Legal Compliance | 5:54 |
| 📺 2.5.2 Ethics | 2:37 |
| 📺 2.5.3 Authorization and Corporate Policies | 3:52 |
| 📺 2.5.5 Engagement Contracts | <u>4:18</u> |
| Total Video Time | 16:41 |

Fact Sheets

- 📄 2.5.4 Legal and Ethical Compliance Facts
- 📄 2.5.6 Engagement Contract Facts

Number of Exam Questions

15 questions

Total Time

About 42 minutes

3.1: Social Engineering

Lecture Focus Questions:

- What is social engineering?
- What are the phases of a social engineering attack?
- What is pretexting? How is it used in social engineering?
- What are some of the most common social engineering techniques?
- How are attackers different in their motivations and approaches?
- How are motivation techniques effective in convincing targets to comply with a hacker's desires?
- What are elicitation techniques? How are they effective for social engineering?
- How do hackers use interview and interrogation techniques for social engineering?

In this section, you will learn to:

- Identify social engineering






Key terms for this section include the following:

| Term | Definition |
|--------------------|--|
| Social engineering | Social engineering is an attack involving human interaction. |
| Footprinting | Footprinting is similar to stalking, but in a social engineering context. |
| Pretexting | Pretexting is a fictitious scenario to persuade someone to perform an action or give information. |
| Elicitation | Elicitation is a technique to extract information from a target without arousing suspicion. |
| Preloading | Preloading is influencing a target's thoughts, opinions, and emotions before something happens. |
| SMiShing | SMiShing is doing phishing through SMS. |
| Impersonation | Impersonation is pretending to be somebody else and approaching a target to extract information. |
| Spim | Spim is similar to spam, but the malicious link is sent to the target over instant messaging instead of email. |
| Hoax | A hoax is a type of malicious email with some type of urgent or alarming message to deceive the target. |
| Hacktivist | A hacktivist is a hacker with a political motive. |
| Script kiddie | A script kiddie is a hacker who uses scripts written by much more talented individuals. |
| White hat hacker | A white hat hacker is a professional who helps companies see the vulnerabilities in their security. |

| | |
|---------------|---|
| Cybercriminal | A cybercriminal is a hacker willing to take more risks because the payoff is higher. Cybercriminals are often associated with large organized crime syndicates such as the mafia. |
|---------------|---|

This section helps you prepare for the following certification exam objectives:





| Exam | Objective |
|----------------------------|---|
| TestOut Ethical Hacker Pro | 2.1 Obtain login credentials <ul style="list-style-type: none"> • Use Social Engineering |
| | 1. Background <ul style="list-style-type: none"> • Information Security Threats and Attack Vector |
| EC-Council | 3. Security <ul style="list-style-type: none"> • Information Security Attack Detection |
| | 4. Tools/Systems/Programs <ul style="list-style-type: none"> • Information Security Tools |
| | 5. Procedures/Methodology <ul style="list-style-type: none"> • Information Security Assessment Methodologies |

| Video/Demo | Time |
|--|--------------|
|  3.1.1 Social Engineering Overview | 4:46 |
|  3.1.3 Social Engineering Motivation | 10:18 |
|  3.1.5 Social Engineering Techniques | 10:16 |
|  3.1.7 Phishing and Internet-Based Techniques | 4:59 |
|  3.1.9 Use the Social Engineer Toolkit | <u>4:24</u> |
| Total Video Time | 34:43 |

Lab/Activity

-  3.1.10 Identify Social Engineering

Fact Sheets

-  3.1.2 Social Engineering Overview Facts
-  3.1.4 Social Engineering Motivation Facts
-  3.1.6 Social Engineering Technique Facts
-  3.1.8 Phishing and Internet-Based Technique Facts

Number of Exam Questions

12 questions

Total Time

About 79 minutes

3.2: Physical Security

Lecture Focus Questions:

- What kinds of natural disasters can affect a company's physical assets?
- What are some basic tools and methods for lock picking?
- How do hackers clone an ID badge?
- What are some of the most common physical attacks a company needs to protect itself against?
- Which agency in the U.S. Department of Commerce helps determine the controls that are helpful for physical security?

Key terms for this section include the following:

| Term | Definition |
|---|---|
| National Institute of Standards and Technology (NIST) | NIST is an institute that publishes and standardizes the security controls and assessment procedures to protect the integrity of information systems. |
| Bump key | A bump key is cut to the number nine position with some of the front and shank removed. |
| Scrubbing | A lock picking method that involves running a pick over all the pins with carefully calculated pressure. |
| Lock shim | A lock shim is a thin and stiff piece of metal used to open a padlock. |

This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|------------|--|
| EC-Council | 1. Background |
| | <ul style="list-style-type: none"> • Information Security Threats and Attack Vector |
| | 3. Security |
| | <ul style="list-style-type: none"> • Information Security Controls |

Video/Demo

 3.2.1 Physical Security Overview

Time

11:25

 3.2.3 Physical Security Attacks

6:32

Total Video Time

17:57

Fact Sheets

 3.2.2 Physical Security Facts

 3.2.4 Physical Security Attack Facts

Number of Exam Questions

11 questions

Total Time

About 39 minutes

3.3: Countermeasures and Prevention

Lecture Focus Questions:

- What kinds of policies and procedures deter social engineers from attacking a company?
- What kind of employee awareness training should a company implement?
- How can the HR department help prevent attacks through its hiring and termination process?
- How should the help desk handle requests over the phone and in person?
- How do you dispose of documents or any piece of paper that could contain sensitive information?
- What kind of backup should a company implement?

In this section, you will learn to:

- Implement physical security countermeasures

Key terms for this section include the following:

| Term | Definition |
|---------------------|--|
| Bollard | A physical barrier to deter aggressive intruders. |
| Strip-cut shredder | A device that cuts paper into long, thin strips. |
| Crosscut shredder | A device that cuts paper both vertically and horizontally, turning the paper into confetti. |
| Full backup | A process that backs up every piece of an organization's data. |
| Incremental backup | A process that backs up every file that's changed since the last full or incremental backup. |
| Differential backup | A process that backs every file that's changed since the last full backup. |

This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|------------|---|
| EC-Council | 1. Background <ul style="list-style-type: none"> • Information Security Threats and Attack Vector |
| | 3. Security <ul style="list-style-type: none"> • Information Security Attack Detection • Information Security Attack Prevention |

Video/Demo

- 3.3.1 Countermeasures and Prevention

Total Video Time**Time**8:13**8:13****Lab/Activity**

- 3.3.3 Implement Physical Security Countermeasures

Fact Sheets

- 3.3.2 Countermeasures and Prevention Facts

Number of Exam Questions

5 questions

Total Time*About 31 minutes*

4.1: Reconnaissance Overview

Lecture Focus Questions:

- What is reconnaissance?
- Why is it important to gain information about your target before you start an active attack?
- Which tools you use to gather information?
- What type of information can be gathered during the reconnaissance phase?
- How can social networking, Google hacking, and search engines be used to gather information?

In this section, you will learn to:

- Perform reconnaissance with nmap

Key terms for this section include the following:

| Term | Definition |
|-------------------------------|---|
| Reconnaissance | Reconnaissance is a systematic attempt to locate, gather, identify, and record information about a target. |
| Passive information gathering | Passive information gathering is a method of indirectly collecting details about a target. It does not involve direct engagement with the target, so the chance of detection is very low. |
| Active information gathering | Active information gathering is a method of directly collecting details about a target. It involves direct engagement with the target, so the chance of detection is higher. |

This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|----------------------------|---|
| | 1.1 Perform reconnaissance |
| TestOut Ethical Hacker Pro | <ul style="list-style-type: none"> • Perform reconnaissance with hacking tools |
| | 4. Tools/Systems/Programs |
| | <ul style="list-style-type: none"> • Information Security Tools |
| EC-Council | 5. Procedures/Methodology |
| | <ul style="list-style-type: none"> • Information Security Procedures |

Video/Demo

 4.1.1 Reconnaissance Processes

Time

4:56

| | |
|---|-------------|
| 🖥️ 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 | <u>4:14</u> |

Total Video Time**18:20****Lab/Activity**

- 🔗 4.1.7 Perform Reconnaissance with Nmap

Fact Sheets

- 📄 4.1.2 Reconnaissance Process Facts
- 📄 4.1.3 Reconnaissance Tool Facts

Number of Exam Questions

12 questions

Total Time*About 53 minutes*

4.2: Reconnaissance Countermeasures

Lecture Focus Questions:





- How can companies limit the types of information hackers can gather about them?
- What can you do to keep DNS servers up-to-date?
- What types of information should you include in your information sharing policies?

In this section, you will learn to:

- Disable Windows services (IIS)
- Manage Linux services
- Enable and disable Linux services
- Hide the IIS banner broadcast

This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|----------------------------|--|
| TestOut Ethical Hacker Pro | 5.1 Defend systems and devices <ul style="list-style-type: none"> • Hide a web server banner broadcast |
| | 5.2 Implement defensive systems <ul style="list-style-type: none"> • Disable unnecessary services |
| | 3. Security <ul style="list-style-type: none"> • Information Security Attack Prevention |
| EC-Council | 4. Tools/Systems/Programs <ul style="list-style-type: none"> • Information Security Systems • Information Security Tools |

| Video/Demo | Time |
|---|--------------|
|  4.2.1 Reconnaissance Countermeasures | 3:01 |
|  4.2.2 View Windows Services | 5:11 |
|  4.2.4 View Linux Services | 4:14 |
|  4.2.8 Disable IIS Banner Broadcasting | <u>1:47</u> |
| Total Video Time | 14:13 |

Lab/Activity

- 🔗 4.2.3 Disable Windows Services
- 🔗 4.2.5 Manage Linux Services
- 🔗 4.2.6 Enable and Disable Linux Services
- 🔗 4.2.9 Hide the IIS Banner Broadcast

Fact Sheets

- 📄 4.2.7 Reconnaissance Countermeasure Facts

Number of Exam Questions

5 questions

Total Time

About 73 minutes

5.1: Scanning Overview

Lecture Focus Questions:

- What is scanning?
- Which types of scanning are used to gather information about a target?
- Which tools can be used for scanning?
- What type of information can be gathered with scanning?
- How can organizations protect themselves against scanning attempts?

In this section, you will learn to:

- Perform a scan
- Perform a decoy scan

Key terms for this section include the following:

| Term | Definition |
|--------------------|---|
| Scanning | Scanning is the process of actively engaging with a target in an attempt to gather information about a network. |
| Port scan | A port scan probes a server or host for open ports. |
| Network scan | Network scans are used to find live computers on a network. |
| Vulnerability scan | Vulnerability scans are used to find system weaknesses such as open ports and access points. |

This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|----------------------------|---|
| TestOut Ethical Hacker Pro | 1.2 Perform scanning <ul style="list-style-type: none"> • Scan for network devices |
| | 3. Security <ul style="list-style-type: none"> • Information Security Attack Prevention |
| EC-Council | 4. Tools/Systems/Programs <ul style="list-style-type: none"> • Information Security Tools |
| | 5. Procedures/Methodology <ul style="list-style-type: none"> • Information Security Procedures |

Video/Demo

Time

| | |
|--|--------------|
| 📺 5.1.1 Scanning Processes | 5:54 |
| 🖥 5.1.4 Perform a Scan with Nmap | 4:36 |
| 🖥 5.1.7 Perform a Scan with Nmap Scripts | 4:36 |
| 📺 5.1.8 Scanning Considerations | <u>5:38</u> |
| Total Video Time | 20:44 |

Lab/Activity

- 🔗 5.1.5 Perform an Internal Scan
- 🔗 5.1.6 Perform an External Scan Using Zenmap

Fact Sheets

- 📄 5.1.2 Scanning Process Facts
- 📄 5.1.3 Scanning Tool Facts
- 📄 5.1.9 Scanning Considerations Facts

Number of Exam Questions

14 questions

Total Time

About 74 minutes

5.2: Banner Grabbing

Lecture Focus Questions:

- What is banner grabbing?
- Which tools can be used to grab a banner?
- What information is included in a banner?

Key terms for this section include the following:

| Term | Definition |
|-----------------|---|
| Banner grabbing | Banner grabbing is a technique hackers use to obtain information about the services running on a target system. |

This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|------------|---|
| EC-Council | 3. Security <ul style="list-style-type: none"> • Information Security Attack Detection • Information Security Attack Prevention |
| | 4. Tools/Systems/Programs <ul style="list-style-type: none"> • Information Security Tools |

Video/Demo

 5.2.1 Banner Grabbing

Total Video Time

Time

4:19

4:19

Fact Sheets

 5.2.2 Banner Grabbing Facts

Number of Exam Questions

5 questions

Total Time

About 15 minutes

6.1: Enumeration Overview

Lecture Focus Questions:

- What is enumeration?
- How is enumeration used to gather information about a target?
- Which tools can be used for enumeration?
- Which type of information can be gathered with enumeration?
- How can companies protect themselves against enumeration attempts?

In this section, you will learn to:

- Perform enumeration with nmap
- Perform enumeration with Metasploit

Key terms for this section include the following:


| Term | Definition |
|-------------|--|
| Enumeration | Enumeration is a method of gathering information from a system to learn more about its configurations, software, and services. |

This section helps you prepare for the following certification exam objectives:




| Exam | Objective |
|----------------------------|--|
| | 1.2 Perform scanning <ul style="list-style-type: none"> • Detect operating systems and applications |
| TestOut Ethical Hacker Pro | 1.3 Perform enumeration <ul style="list-style-type: none"> • Enumerate network resources • Enumerate device information |
| | 1. Background <ul style="list-style-type: none"> • Network and Communication Technologies |
| | 3. Security <ul style="list-style-type: none"> • Information Security Attack Detection |
| EC-Council | 4. Tools/Systems/Programs <ul style="list-style-type: none"> • Information Security Systems • Information Security Tools |

5. Procedures/Methodology

- Information Security Procedures

| Video/Demo | Time |
|---|--------------|
|  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 |
|  6.1.6 Enumerate with Metasploit | 6:35 |
|  6.1.7 Enumerate with NetBIOS Enumerator | 2:52 |
|  6.1.10 Enumerate with SoftPerfect | <u>3:50</u> |
| Total Video Time | 33:32 |

Lab/Activity

-  6.1.9 Perform Enumeration with Nmap
-  6.1.11 Perform Enumeration with Metasploit
-  6.1.12 Perform Enumeration of MSSQL with Metasploit

Fact Sheets

-  6.1.5 Enumeration Facts
-  6.1.8 Enumerate Ports and Services Facts

Number of Exam Questions

12 questions

Total Time

About 90 minutes

6.2: Enumeration Countermeasures

Lecture Focus Questions:

- How can companies protect themselves against enumeration attempts?
- What can you do to prevent SNMP exploitation?
- What is the best way to secure LDAP?


In this section, you will learn to:

- Prevent zone transfer

This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|----------------------------|---|
| TestOut Ethical Hacker Pro | 5.2 Implement defensive systems <ul style="list-style-type: none"> • Prevent DNS zone transfer |
| | 3. Security <ul style="list-style-type: none"> • Information Security Attack Prevention |
| EC-Council | 4. Tools/Systems/Programs <ul style="list-style-type: none"> • Information Security Tools |
| | 5. Procedures/Methodology <ul style="list-style-type: none"> • Information Security Procedures |

Video/Demo

-  6.2.1 Enumeration Countermeasures
-  6.2.3 Disable DNS Zone Transfers

Time

1:53

5:07

Total Video Time

7:00

Lab/Activity

-  6.2.4 Prevent Zone Transfer

Fact Sheets

-  6.2.2 Enumeration Countermeasure Facts

Number of Exam Questions

5 questions

Total Time
About 29 minutes

7.1: Vulnerability Assessment

Lecture Focus Questions:

- Why is vulnerability assessment important?
- What are the limitations of scans?
- What are seven types of assessments?
- What are the top nine areas to research when conducting an assessment?

In this section, you will learn to:

- Conduct vulnerability scans

Key terms for this section include the following:

| Term | Definition |
|---------------------|---|
| Active assessment | A network evaluation that is obtained by actively testing the network for weaknesses. |
| Passive assessment | A network evaluation that is obtained by looking for weaknesses through observation with no direct network interaction. |
| External assessment | A network evaluation that is obtained by testing external systems and testing from outside the network. |
| Internal assessment | A network evaluation that is obtained by testing and analyzing processes and systems inside the network. |

This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|------------|--|
| EC-Council | 2. Analysis/Assessment <ul style="list-style-type: none"> • Information Security Assessment and Analysis |
| | 5. Procedures/Methodology <ul style="list-style-type: none"> • Information Security Procedures • Information Security Assessment Methodologies |

Video/Demo

- 📺 7.1.1 Vulnerability Assessment
- 📺 7.1.3 Conduct Vulnerability Scans

Total Video Time

Time

8:41

4:01

12:42

Fact Sheets

7.1.2 Vulnerability Assessment Facts

Number of Exam Questions

8 questions

Total Time

About 26 minutes

7.2: Vulnerability Management Life Cycle

Lecture Focus Questions:

- Why is it important to create a baseline before testing begins?
- How important is the vulnerability assessment phase to the rest of the cycle?
- Why should you take the time to evaluate the threat levels of the results of your penetration testing?
- Which phase includes fixing weaknesses that are found?
- Why would you retest the system after remediation?
- Why is ongoing monitoring a valuable practice?

Key terms for this section include the following:

| Term | Definition |
|--------------------------|--|
| Vulnerability assessment | A phase of testing the network for vulnerabilities. |
| Risk assessment | A phase of evaluating the found vulnerabilities for threat level. |
| Remediation | A phase of patching, hardening, and correcting weaknesses. |
| Verification | A phase of retesting the system to verify that patching and hardening was effective. |
| Monitoring | A phase where continuous monitoring of systems is implemented. |

This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|------------|--|
| EC-Council | 2. Analysis/Assessment <ul style="list-style-type: none"> • Information Security Assessment Process |
| | 5. Procedures/Methodology <ul style="list-style-type: none"> • Information Security Procedures • Information Security Assessment Methodologies |

Video/Demo

- 📺 7.2.1 Vulnerability Management Life Cycle
- 📺 7.2.3 Vulnerability Solutions

Total Video Time

Time

6:20

2:20**8:40**

Fact Sheets

- 📄 7.2.2 Vulnerability Management Life Cycle Facts
- 📄 7.2.4 Vulnerability Solution Facts

Number of Exam Questions

8 questions

Total Time

About 27 minutes

7.3: Vulnerability Scoring Systems

Lecture Focus Questions:

- What are the three metrics used to determine a CVSS score?
- What is the value of a CVSS score to an ethical hacker?
- What are five helpful government-sponsored resources?
- Why is it helpful to use tools based on known vulnerability databases?

Key terms for this section include the following:

| Term | Definition |
|---|---|
| Common Vulnerability Scoring System (CVSS) | A system that categorizes vulnerabilities by threat level. |
| CVSS calculator | A calculator for determining risk level of vulnerabilities based on base, temporal, and environmental metrics. |
| Cybersecurity and Infrastructure Security Agency (CISA) | A large government-sponsored organization that provides many resources for cyber security. |
| National Vulnerability Database (NVD) | A government-sponsored, detailed database of known vulnerabilities. |
| Full disclosure | A public, vendor-neutral forum for the discussion of vulnerabilities and threats that often has the newest information. It also has tools, papers, news, and events related to vulnerabilities and threats. |

This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|------------|---|
| EC-Council | 4. Tools/Systems/Programs <ul style="list-style-type: none"> • Information Security Tools |
| | 5. Procedures/Methodology <ul style="list-style-type: none"> • Information Security Assessment Methodologies |

Video/Demo

 7.3.1 Vulnerability Scoring Systems

Time

5:41

Total Video Time

5:41

Fact Sheets

 7.3.2 Vulnerability Scoring System Facts

Number of Exam Questions

7 questions

Total Time

About 18 minutes

7.4: Vulnerability Assessment Tools

Lecture Focus Questions:

- Why is it important to be familiar with assessment tools?
- What are the top assessment tools for networks and mobile devices?
- Why is it important to include mobile devices in your assessment testing?
- What information can you expect from vulnerability reports?

In this section, you will learn to:

- Scan for vulnerabilities on a Windows workstation
- Scan for vulnerabilities on a Linux server
- Scan for vulnerabilities on a domain controller
- Scan for vulnerabilities on a security appliance
- Scan for vulnerabilities on a WAP

Key terms for this section include the following:




| Term | Definition |
|-------------------------------|--|
| Vulnerability assessment tool | A service or program that tests systems and devices for weaknesses that could be exploited. |
| Open source tool | A tool that is free to use and can be modified and shared. |
| Vulnerability report | A report generated by a vulnerability assessment tool that gives information such as weak passwords, open ports, and lack of encryption. It also provides suggestions for remediation. |
| Remediation | The actions taken to patch, repair, fix, or harden weaknesses in a network. |

This section helps you prepare for the following certification exam objectives:






| Exam | Objective |
|----------------------------|---|
| TestOut Ethical Hacker Pro | 1.2 Perform scanning <ul style="list-style-type: none"> • Scan for vulnerabilities |
| | 2. Analysis/Assessment <ul style="list-style-type: none"> • Information Security Assessment and Analysis |
| EC-Council | 4. Tools/Systems/Programs <ul style="list-style-type: none"> • Information Security Tools |

Video/Demo

Time

| | |
|--|-------------|
|  7.4.1 Vulnerability Assessment Tools | 4:52 |
|  7.4.3 Scan a Network with Retina | 7:16 |
|  7.4.4 Scan a Network with Nessus | <u>3:16</u> |

Total Video Time**15:24****Lab/Activity**

-  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

Fact Sheets

-  7.4.2 Vulnerability Assessment Tool Facts

Number of Exam Questions

7 questions

Total Time*About 88 minutes*

8.1: System Hacking

Lecture Focus Questions:

- What non-technical password attacks do organizations need to guard themselves against?
- What are the main types of technical password attacks?
- What are rainbow table attacks?
- What is password salting?
- What can an organization do to protect passwords?

In this section, you will learn to:

- Spoof MAC addresses with SMAC
- Analyze USB keylogger attacks
- Crack a password with rainbow tables
- Crack a password with John the Ripper
- Configure account password policies









Key terms for this section include the following:

| Term | Definition |
|--------------------|---|
| Brute force attack | A password cracking technique that tests every possible keystroke for each character in a password until the correct one is found. |
| Rainbow attack | A password hash cracking technique that uses pre-computed word lists and their hashes in tables for quick comparison using the cracked hashes for authentication. |
| Dictionary attack | A password cracking technique that tests for words from a dictionary, but can include additional common password phrases and symbol substitutions that are added to the database. |
| Password salting | Adding random bits of data to a password before it is stored as a hash to make password cracking much more difficult. |
| Keylogger | Hardware or software that captures every keystroke on the computer. |






This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|----------------------------|---|
| TestOut Ethical Hacker Pro | 1.1 Perform reconnaissance <ul style="list-style-type: none"> • Perform reconnaissance with operating system tools |
| | 2.1 Obtain login credentials <ul style="list-style-type: none"> • Crack passwords |
| | 4.1 Cover up access |

| | |
|------------|---|
| | <ul style="list-style-type: none"> • Change MAC address |
| | 5.1 Defend systems and devices |
| | <ul style="list-style-type: none"> • Configure account policies and account control |
| | 1. Background |
| | <ul style="list-style-type: none"> • Information Security Threats and Attack Vector |
| | 3. Security |
| EC-Council | <ul style="list-style-type: none"> • Information Security Attack Detection • Information Security Attack Prevention |
| | 4. Tools/Systems/Programs |
| | <ul style="list-style-type: none"> • Information Security Tools |

| Video/Demo | Time |
|--|--------------|
|  8.1.1 Introduction to Hacking | 7:05 |
|  8.1.3 Keylogger Attack | 5:18 |
|  8.1.6 Use Rainbow Tables | 3:33 |
|  8.1.8 Crack Passwords | 8:02 |
|  8.1.9 Crack Password Protected Files | 3:22 |
|  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 | <u>10:41</u> |
| Total Video Time | 47:22 |

Lab/Activity

-  8.1.4 Analyze a USB Keylogger Attack
-  8.1.5 Analyze a USB Keylogger Attack 2
-  8.1.7 Crack a Password with Rainbow Tables
-  8.1.10 Crack a Password with John the Ripper
-  8.1.14 Configure Account Password Policies

Fact Sheets

-  8.1.2 Introduction to Hacking Facts

Number of Exam Questions

11 questions

Total Time

About 124 minutes

8.2: Privilege Escalation

Lecture Focus Questions:

- What is privilege escalation?
- How do attackers escalate privileges?
- What are escalation tools?
- How can you protect against privilege escalation?

In this section, you will learn to:

- Crack the SAM database with John the Ripper
- Enforce user account control

Key terms for this section include the following:






| Term | Definition |
|--|--|
| Kerberoasting | An offline brute force to crack a Kerberos ticket to reveal the service account password in plain text. There is no risk of detection and no need for escalated privileges, and the attack is easy to perform. |
| DLL hijacking | Loading a malicious DLL in the application directory so that when the application executes, it will choose the malicious DLL. |
| cPasswords | The attribute that stores passwords in a Windows group policy preference item. This attribute can be exploited because Microsoft publishes a public key for the account credentials. |
| Security Account Manager (SAM) database | The database that authenticates local and remote users. In Windows, this database stores user passwords as an LM hash or an NTLM hash. |
| Local Security Authority Subsystem Service (LSASS) | The Local Security Authority Subsystem Service is a Windows service that performs the system's security protocol. |

This section helps you prepare for the following certification exam objectives:



| Exam | Objective |
|----------------------------|--|
| TestOut Ethical Hacker Pro | 2.2 Gain administrative access and escalate privileges <ul style="list-style-type: none"> • Escalate privileges |
| | 5.1 Defend systems and devices |

EC-Council

- Configure account policies and account control
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

| Video/Demo | Time |
|--|--------------|
|  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 |
|  8.2.7 Configure User Account Control | <u>6:57</u> |
| Total Video Time | 28:01 |

Lab/Activity

-  8.2.6 Crack the SAM Database with John the Ripper
-  8.2.8 Enforce User Account Control

Fact Sheets

-  8.2.5 Privilege Escalation in Windows Facts

Number of Exam Questions

9 questions

Total Time

About 67 minutes

8.3: Maintain Access

Lecture Focus Questions:

- How do hackers maintain access to the systems they exploit?
- What are writable services?
- How do hackers leave the back door open for themselves?

In this section, you will learn to:

- Create a backdoor with Metasploit
- Create a backdoor with Netcat

Key terms for this section include the following:

| Term | Definition |
|-------------------|--|
| Path interception | When a malicious file name is added to a service path without quotation marks and includes spaces in the code. |
| Backdoor | An installed program that grants continued access to a previously hacked system. |
| Spyware | Malware that works by stealth to capture information and send it to a hacker to help them gain remote access. |
| Crackers | Software programs that crack code and passwords to gain unauthorized access to a system. |
| Writable services | A service with permissions that allow anyone to change the service's execution. |

This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|----------------------------|--|
| TestOut Ethical Hacker Pro | Gain administrative access and escalate privileges <ul style="list-style-type: none"> • Gain access through a backdoor |
| EC-Council | 4. Tools/Systems/Programs <ul style="list-style-type: none"> • Information Security Tools 5. Procedures/Methodology <ul style="list-style-type: none"> • Information Security Procedures |

Video/Demo

 8.3.1 Exploit Systems to Maintain Access

Time

4:01

| | |
|---|--------------|
| 🖥️ 8.3.2 Establish an Unauthorized SSH Connection | 4:20 |
| 🖥️ 8.3.3 Create a Backdoor with Metasploit | <u>5:22</u> |
| Total Video Time | 13:43 |

Lab/Activity

- 🔗 8.3.4 Create a Backdoor with Metasploit
- 🔗 8.3.6 Create a Backdoor with Netcat

Fact Sheets

- 📄 8.3.5 Exploit Systems to Maintain Access Facts

Number of Exam Questions

5 questions

Total Time

About 48 minutes

8.4: Cover Your Tracks

Lecture Focus Questions:

- How can an attacker prevent being detected?
- How is evidence such as files, data, and programs hidden?
- What are rootkits? How can you detect them? And how can you protect systems from them?
- What is steganography? Why is it so difficult to detect?

In this section, you will learn to:

- Clear Windows log files on Server 2016
- Clear audit policies
- Hide files with OpenStego







Key terms for this section include the following:

| Term | Definition |
|-------------------|--|
| Rootkit | A software program that attackers use to establish root-level privileges to a system. |
| Steganography | A method of embedding data into legitimate files like graphics, music, video, and plain text messages to hide it from everyone except the intended receiver. |
| NTFS data streams | One data stream stores the attributes, another stores the data. Additional data streams, which can be hidden, are allowed. |
| Slack space | The unused portion of an existing file that has been defined. |
| System file logs | Files that are continuously recording when files are created, accessed, or modified. |




This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|----------------------------|--|
| TestOut Ethical Hacker Pro | 4.1 Cover up access <ul style="list-style-type: none"> • Disable auditing • Clear logs • Remove or hide files and folders |
| | 4. Tools/Systems/Programs |
| EC-Council | <ul style="list-style-type: none"> • Information Security Programs • Information Security Tools |
| | 5. Procedures/Methodology |



- Information Security Assessment Methodologies

| Video/Demo | Time |
|--|--------------|
|  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 |
|  8.4.7 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 | <u>3:20</u> |
| Total Video Time | 27:01 |

Lab/Activity

-  8.4.5 Clear Windows Log Files on Server 2016
-  8.4.6 Clear Audit Policies
-  8.4.11 Hide Files with OpenStego

Fact Sheets

-  8.4.4 Cover Your Tracks Facts
-  8.4.10 Hide Programs Facts

Number of Exam Questions

13 questions

Total Time

About 87 minutes

9.1: Malware

Lecture Focus Questions:

- What are the different types of malware?
- Which component of malware actually causes damage?
- What is the purpose of a Trojan horse?
- What are some ways malware can infect a system?
- What is the best way to analyze malware?

In this section, you will learn to:

- Create a virus
- Create a HTTP Trojan
- Use ProRat to create a Trojan

Key terms for this section include the following:

| Term | Definition |
|----------------------------------|---|
| Malware | Any software that is designed to perform malicious and disruptive actions. |
| The Computer Fraud and Abuse Act | This law was originally passed to address federal computer-related offenses and the cracking of computer systems. |
| The Patriot Act | This act expanded on the powers already included in the Computer Fraud and Abuse Act. |
| CAN-SPAM Act | This law was designed to thwart the spread of spam. |
| Crypter | Software that protects the malware code from being analyzed and reverse engineered. It also helps prevent detection from anti-virus software. |
| Exploit | The act of taking advantage of a bug or vulnerability to execute malware. |
| Injector | A program that injects malware into vulnerable running processes. |
| Obfuscator | The act of concealing malware through different techniques. |
| Packer | The act of compressing malware to help hide it. |
| Payload | The main piece of malware. The payload is the part that performs the malware's intended activity. |
| Malicious code | Code that defines the malware's basic functionality, such as deleting data or opening backdoors into the target. |
| Sheep dipping | The process of analyzing emails, suspect files, and systems for malware. |

This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|------|-----------|
|------|-----------|

EC-Council

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

Video/Demo

| | Time |
|--|-------------|
|  9.1.1 Malware Overview | 9:40 |
|  9.1.3 Trojans and Backdoors | 5:36 |
|  9.1.5 Malware Concerns | 3:51 |
|  9.1.7 Malware Analysis | 4:25 |
|  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 | <u>3:14</u> |

Total Video Time**32:32****Fact Sheets**

-  9.1.2 Malware Overview Facts
-  9.1.4 Trojan and Backdoor Facts
-  9.1.6 Malware Concern Facts
-  9.1.8 Malware Analysis Facts

Number of Exam Questions

12 questions

Total Time*About 65 minutes*

9.2: Combat Malware

Lecture Focus Questions:

- What are the best methods for detecting malware?
- What steps should you take when penetration testing for malware?
- What actions should be taken when malware is discovered?

In this section, you will learn to:




- Detect open ports with nmap
- View open ports with netstat
- Counter malware with Windows Defender

Key terms for this section include the following:

| Term | Definition |
|---------------------|--|
| Heuristic algorithm | Heuristic algorithms generate fairly accurate results in a short amount of time by focusing on speed instead of accuracy and completeness. |

This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|----------------------------|---|
| TestOut Ethical Hacker Pro | 1.2 Perform scanning <ul style="list-style-type: none"> • Identify open ports |
| | 5.1 Defend systems and devices <ul style="list-style-type: none"> • Use malware protection |
| EC-Council | 3. Security <ul style="list-style-type: none"> • Information Security Attack Prevention |
| | 4. Tools/Systems/Programs <ul style="list-style-type: none"> • Information Security Tools |

| Video/Demo | Time |
|--|--------------|
|  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 | <u>2:31</u> |
| Total Video Time | 10:44 |

Lab/Activity

- 🔗 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

Fact Sheets

- 📄 9.2.4 Anti-Malware Software Facts

Number of Exam Questions

5 questions

Total Time

About 69 minutes

10.1: Sniffing

Lecture Focus Questions:

- What is network sniffing?
- Which tools can be used for network sniffing?
- How can sniffing methods be used to exploit switched networks?
- What are some countermeasures to network sniffing?

In this section, you will learn to:

- Capture traffic with TCPDump
- Poison ARP
- Poison DNS
- Filter and analyze traffic with Wireshark
- Analyze ARP poisoning with Wireshark

Key terms for this section include the following:

| Term | Definition |
|------------------|--|
| Sniffing | Sniffing is the process of collecting information as it crosses the network. |
| Promiscuous mode | Turning on promiscuous mode gives the network interface permission to grab every frame that comes its way, even if it's addressed to someone else. |
| MAC spoofing | MAC spoofing is the process of changing the MAC address of the interface driver in an attempt to impersonate another host on the network. |
| MAC flooding | MAC flooding is the process of overloading a switch's CAM table in hopes that it will respond by broadcasting all traffic across the network. |
| ARP poisoning | ARP poisoning is the process of sending spoofed messages onto a network in an attempt to associate your MAC address with the IP address of another host so the target machine will send frames to your system. |
| Port mirroring | Port mirroring creates a duplicate of all network traffic on a port and sends it to another device. |









This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|----------------------------|---|
| TestOut Ethical Hacker Pro | 2.3 Gain access by cracking <ul style="list-style-type: none"> • Obtain credentials through sniffing |
| EC-Council | 3. Security |

- Information Security Attack Detection
- Information Security Attack Prevention

4. Tools/Systems/Programs

- Information Security Tools

| Video/Demo | Time |
|--|--------------|
|  10.1.1 Sniffing | 6:38 |
|  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 |
|  10.1.7 Poison ARP | 5:13 |
|  10.1.9 Poison DNS | 6:17 |
|  10.1.14 Sniffing Countermeasures and Detection | 2:54 |
|  10.1.15 Detect Promiscuous Mode | <u>3:16</u> |
| Total Video Time | 40:32 |

Lab/Activity

- 10.1.6 Spoof MAC Addresses with SMAC
- 10.1.8 Poison ARP and Analyze with Wireshark
- 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

Fact Sheets

-  10.1.2 Sniffer Facts
-  10.1.16 Sniffing Countermeasure and Detection Facts

Number of Exam Questions

14 questions

Total Time

About 137 minutes

10.2: Session Hijacking

Lecture Focus Questions:

- What is session hijacking? How can it be used to gather sensitive information?
- What are some methods that can be used for session hijacking at the application and network layers?
- What actions can be taken to prevent session hijacking?

In this section, you will learn to:

- Perform a DHCP spoofing man-in-the-middle attack
- Hijack a web session







Key terms for this section include the following:

| Term | Definition |
|-------------------|---|
| Session hijacking | The process of taking over an established connection between a host and a web server. The session token can be stolen or a predicted session token can be used. |
| Session ID | A combination of numbers and letters assigned to an open connection between a user and a server. |





This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|----------------------------|---|
| TestOut Ethical Hacker Pro | 2.2 Gain administrative access and escalate privileges <ul style="list-style-type: none"> • Hijack a web session |
| | 3.1 Perform passive online attacks <ul style="list-style-type: none"> • Examine hidden web form fields • Conduct a man-in-the-middle attack |
| EC-Council | 3. Security <ul style="list-style-type: none"> • Information Security Attack Detection • Information Security Attack Prevention |
| | 4. Tools/Systems/Programs <ul style="list-style-type: none"> • Information Security Tools |




S

| Video/Demo | Time |
|--|--------------|
|  10.2.1 Session Hijacking Overview | 2:36 |
|  10.2.3 Client-Side and Network Attacks | 8:02 |
|  10.2.5 Perform a Man-in-the-Middle DHCP Attack | 6:55 |
|  10.2.9 Use Burp Suite | 5:36 |
|  10.2.10 Hijack a Web Session | 3:33 |
|  10.2.12 Session Hijacking Countermeasures | <u>3:56</u> |
| Total Video Time | 30:38 |

Lab/Activity

-  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
-  10.2.11 Hijack a Web Session

Fact Sheets

-  10.2.2 Session Hijacking Facts
-  10.2.4 Client-Side and Network Attack Facts
-  10.2.13 Session Hijacking Countermeasure Facts

Number of Exam Questions

12 questions

Total Time

About 106 minutes

10.3: Denial of Service

Lecture Focus Questions:

- What is the difference between a denial-of-service attack and a distributed denial-of-service attack?
- What are the four categories of denial-of-service attacks?
- What types of devices can be used in a denial-of-service attack?
- What measures can be taken to prevent your network or devices from a denial-of-service or distributed denial-of-service attack?

In this section, you will learn to:

- Perform and analyze a SYN flood attack
- Analyze ICMP traffic in Wireshark
- Perform a DoS attack
- Analyze a DDoS attack






Key terms for this section include the following:

| Term | Definition |
|--------------------------------------|--|
| Denial-of -service attack | A denial-of-service attack occurs when a computer is used to flood a server with more packets than it can handle. |
| Distributed denial-of-service attack | Distributed denial-of-service attacks use numerous computers and internet connections across the globe to overload target systems. |





This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|----------------------------|--|
| TestOut Ethical Hacker Pro | 3.2 Perform active online attacks <ul style="list-style-type: none"> • Execute a DoS or DDoS attack |
| | 3. Security <ul style="list-style-type: none"> • Information Security Controls • Information Security Attack Detection • Information Security Attack Prevention |
| EC-Council | 4. Tools/Systems/Programs <ul style="list-style-type: none"> • Information Security Tools |
| | 5. Procedures/Methodology |




- Information Security Procedures

| Video/Demo | Time |
|---|--------------|
|  10.3.1 Denial of Service (DoS) Overview | 6:44 |
|  10.3.3 DoS Attack Types | 5:12 |
|  10.3.5 Perform a SYN Flood | 6:18 |
|  10.3.8 Launch a DoS and DDoS Attack | 5:42 |
|  10.3.11 DoS Countermeasures | <u>3:42</u> |
| Total Video Time | 27:38 |

Lab/Activity

-  10.3.6 Perform and Analyze a SYN Flood Attack
-  10.3.7 Analyze ICMP Traffic in Wireshark
-  10.3.9 Perform a DoS Attack
-  10.3.10 Analyze a DDoS Attack

Fact Sheets

-  10.3.2 Denial of Service (DoS) Facts
-  10.3.4 DoS Attack Type Facts
-  10.3.12 DoS Countermeasure Facts

Number of Exam Questions

13 questions

Total Time

About 104 minutes

11.1: Intrusion Detection Systems

Lecture Focus Questions:

- What are the different types of Intrusion Detection Systems (IDSs)?
- Where are IDSs located?
- What are the three main detection types?
- What are some IDS avoidance and evasion techniques?

In this section, you will learn to:

- Implement intrusion detection

Key terms for this section include the following:






| Term | Definition |
|--|---|
| Network intrusion detection system (NIDS) | A network intrusion detection system is a security technology installed on a network that monitors network traffic to detect exploits against a network. |
| Host intrusion detection system (HIDS) | A host intrusion detection system is a security technology installed on a host that monitors activity to detect exploits against the host. |
| Signature-based detection | A signature-based intrusion detection system (IDS) is a security technology that compares network traffic to known signatures in the signature file database. |
| Anomaly-based detection | An anomaly-based detection IDS is a security technology that compares network or host behavior to baseline profiles. |
| Protocol-based detection | A protocol-based IDS is a security technology that detects anomalies specific to a given protocol. |
| True positive | A true positive is an assessment of an IDS alert that indicates an alert was issued in response to an anomaly. |
| False positive | A false positive is an assessment of an IDS alert that indicates an alert was issued, but no anomaly occurred. |
| True negative | A true negative is an assessment of an IDS that indicates no alert was issued, and no anomaly occurred. |
| False negative | A false negative is an assessment of an IDS that indicates no alert was issued, but an anomaly occurred. |
| Denial-of-service (DoS) and Distributed denial-of-service (DDoS) | Denial-of-service and distributed denial-of-service are attacks in which a host or network is compromised or completely brought down by a flood of malicious traffic bombarding the system. |
| Insertion | Insertion is an attack that uses one of three techniques: inserts malicious code in the packet payload, modifies the attack signature so that it is no longer recognized by the IDS, |

| | |
|-------------------------------------|---|
| | or changes the packet header so that it can't be processed by the IDS. |
| Obfuscation | Obfuscation is the act of disguising or obscuring. In hacking, it refers to disguising or obscuring malicious activity. |
| nmap | nmap is an open-source network mapping tool that performs port scanning and network mapping. |
| Transmission Control Protocol (TCP) | Transmission Control Protocol a network communication standard used with Internet Protocol (IP) to send data packets over the internet. It is a connection-oriented protocol, meaning that a connection must be established and maintained for data transfer. |
| User Datagram Protocol (UDP) | User Datagram Protocol is a transport layer protocol that is used with many internet services. It is a connectionless protocol that doesn't require a connection for data transfer. |
| ICMP | Internet Control Message Protocol is a member of the IP suite that network devices use to send error and control messages. |

This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|----------------------------|---|
| | 5.2 Implement defensive systems |
| TestOut Ethical Hacker Pro | <ul style="list-style-type: none"> Implement an Intrusion Detection System (IDS) |
| | 1. Background |
| | <ul style="list-style-type: none"> Information Security Technologies |
| | 3. Security |
| EC-Council | <ul style="list-style-type: none"> Information Security Attack Detection Information Security Attack Prevention |
| | 4. Tools/Systems/Programs |
| | <ul style="list-style-type: none"> Information Security Systems Information Security Tools |
| | 5. Procedures/Methodology |





- Information Security Assessment Methodologies

| Video/Demo | Time |
|--|--------------|
|  11.1.1 Intrusion Detection Systems | 5:15 |
|  11.1.3 Avoid IDS Detection | 9:36 |
|  11.1.5 Evade IDS | 11:25 |
|  11.1.8 Detect IDS Intrusion with Snort | 9:16 |
|  11.1.9 Implement Intrusion Detection | <u>5:58</u> |
| Total Video Time | 41:30 |

Lab/Activity

-  11.1.10 Implement Intrusion Detection

Fact Sheets

-  11.1.2 Intrusion Detection System Facts
-  11.1.4 Avoid IDS Detection Facts
-  11.1.6 Evade IDS Facts
-  11.1.7 IDS Penetration Testing Facts

Number of Exam Questions

14 questions

Total Time

About 88 minutes

11.2: Firewalls

Lecture Focus Questions:

- What are two types of firewalls?
- How do firewalls provide intrusion detection?
- What are three firewall configurations?

In this section, you will learn to:

- Configure a perimeter firewall
- Perform decoy scans
- Bypass Windows firewall






Key terms for this section include the following:

| Term | Definition |
|-----------------------------------|---|
| Packet-filtering | Packet filtering firewalls look at the header information of the packets and distinguish legitimate traffic from traffic that is not legitimate. |
| Access Control List (ACL) | An access control list specifies the permissions associated with an object. |
| Stateful firewall | Also referred to as stateful multilayer firewalls, this type of firewall determines the legitimacy of traffic based on the state of the connection from which the traffic originated. |
| Virtual Private Network (VPN) | A virtual private network is an encrypted connection across a public network. |
| Network Address Translation (NAT) | Network address translation remaps IP addresses. It is a critical component of the continued use of IPv4 because available addresses are exhausted. |
| Domain Name Server (DNS) | Domain name server is a directory of domain names that specifies the IP address for the domain. |
| Demilitarized Zone (DMZ) | Demilitarized zone is a subnet that interfaces with external networks to protect the internal network. |
| Bastion host | Also called a boundary firewall, a bastion host is designed to have an entry and exit point on the network, which allows the public and internal interfaces to connect. |
| Screened subnet | A configuration using a single firewall to protect multiple interfaces. |
| Multihomed | A network, or host, connected to two or more networks. Each interface is connected to its own network segment logically and physically. |
| Firewalking | The process of probing a firewall to determine the configuration of ACLs by sending TCP and UDP packets. |

| | |
|---------------|---|
| Spoofting | A hijacking technique in which a hacker masquerades as a trusted host to conceal identity, hijack browsers, or gain unauthorized access to a network. |
| Fragmentation | An attacker creates fragments of outgoing packets, forcing some of the TCP packet's header information into the next packet. |
| Tunneling | Tunneling is a communication protocol for transmitting data from one network to another. A hacker can include malicious code in an HTTP, ICMP, or ACK tunneling packet, bypassing the firewall and reaching an internal system. |

This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|----------------------------|---|
| TestOut Ethical Hacker Pro | 3.3 Perform infrastructure attacks <ul style="list-style-type: none"> Evade firewalls, IDSs, and honeypots |
| | 1. Background <ul style="list-style-type: none"> Information Security Technologies |
| | 3. Security <ul style="list-style-type: none"> Information Security Attack Detection Information Security Attack Prevention |
| EC-Council | 4. Tools/Systems/Programs <ul style="list-style-type: none"> Information Security Systems Information Security Tools |
| | 5. Procedures/Methodology <ul style="list-style-type: none"> Information Security Assessment Methodologies |

| Video/Demo | Time |
|---|--------------|
|  11.2.1 Firewalls | 10:07 |
|  11.2.3 Evade Firewalls | 6:38 |
|  11.2.6 Configure a Perimeter Firewall | 7:53 |
|  11.2.8 Avoid Firewall Detection | 5:26 |
|  11.2.11 Bypass Windows Firewall with Metasploit | <u>3:45</u> |
| Total Video Time | 33:49 |

Lab/Activity

- 🔗 11.2.7 Configure a Perimeter Firewall
- 🔗 11.2.9 Perform a Decoy Scan
- 🔗 11.2.10 Perform a Decoy Scan with Zenmap
- 🔗 11.2.12 Bypass Windows Firewall with Metasploit

Fact Sheets

- 📄 11.2.2 Firewall Facts
- 📄 11.2.4 Evade Firewalls Facts
- 📄 11.2.5 Firewall Penetration Testing Facts

Number of Exam Questions

14 questions

Total Time

About 111 minutes

11.3: Honeypots

Lecture Focus Questions:

- What are the main objectives of setting up a honeypot?
- What kind of interactions take place with honeypots?
- What are the three levels of honeypot interactions?
- How can attackers evade honeypots?

In this section, you will learn to:

- Create a honeypot with Pentbox

Key terms for this section include the following:

| Term | Definition |
|-----------------------------|---|
| Honeypot | A honeypot is a physical or virtual network device set up to look like a legitimate network resource to a hacker and designed to attract a hacker. |
| Low-level | A low-level honeypot is a honeypot that simulates a limited number of services and applications of a target system or network. It relies on the emulation of service and programs that would be found on a vulnerable system. |
| Honeypot interaction levels | The honeypot interaction level indicates the amount of interaction that a hacker can have with a honeypot. |
| Medium-level | A medium-level honeypot is a honeypot that simulates a real OS, applications, and services. |
| High-level | A high-level honeypot is a honeypot that simulates all services and applications. It can be completely compromised by hackers to give full access to the system in a controlled area. |
| VMware | VMware is a software company that provides virtualization software. |
| User-Mode Linux (UML) | User-Mode Linux is a software program that allows a user to virtually run one or more versions of Linux inside a Linux session. |

This section helps you prepare for the following certification exam objectives:




| Exam | Objective |
|----------------------------|---|
| TestOut Ethical Hacker Pro | 5.2 Implement defensive systems <ul style="list-style-type: none"> • Create a honeypot |
| | 1. Background <ul style="list-style-type: none"> • Information Security Technologies |
| EC-Council | |

3. Security

- Information Security Attack Detection
- Information Security Attack Prevention

4. Tools/Systems/Programs

- Information Security Systems
- Information Security Programs
- Information Security Tools

| Video/Demo | Time |
|---|--------------|
|  11.3.1 Honeypots | 4:36 |
|  11.3.3 Evade Honeypots | 4:35 |
|  11.3.5 Detect Malicious Network Traffic with a Honeypot | <u>3:23</u> |
| Total Video Time | 12:34 |

Lab/Activity

- 11.3.6 Create a Honeypot with Pentbox

Fact Sheets

-  11.3.2 Honeypot Facts
-  11.3.4 Evade Honeypots Facts

Number of Exam Questions

11 questions

Total Time

About 46 minutes

12.1: Web Servers

Lecture Focus Questions:

- What is a web server?
- What are a web server's vulnerabilities?
- What are the steps in the web server hacking methodology?
- What are some of the actions you can take to help prevent web server attacks?

In this section, you will learn to:

- Extract web server information with nmap
- Crack FTP credentials with Wireshark






Key terms for this section include the following:

| Term | Definition |
|------------|---|
| Web server | A web server is a computer used to store and distribute web pages to clients. |



This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|----------------------------|---|
| TestOut Ethical Hacker Pro | 2.1 Obtain login credentials <ul style="list-style-type: none"> • Obtain credentials using tools |
| | 3.3 Perform infrastructure attacks <ul style="list-style-type: none"> • Attack a web server |
| | 1. Background <ul style="list-style-type: none"> • Information Security Technologies |
| EC-Council | 3. Security <ul style="list-style-type: none"> • Information Security Attack Detection • Information Security Attack Prevention |
| | 4. Tools/Systems/Programs <ul style="list-style-type: none"> • Information Security Tools |
| | 5. Procedures/Methodology |




- Information Security Procedures

| Video/Demo | Time |
|---|--------------|
|  12.1.1 Web Server Hacking | 3:38 |
|  12.1.3 Web Server Attacks | 5:05 |
|  12.1.5 Mirror a Website with HTTrack | 2:13 |
|  12.1.6 Extract Web Server Information | 4:30 |
|  12.1.9 Web Server Countermeasures | <u>4:58</u> |
| Total Video Time | 20:24 |

Lab/Activity

-  12.1.7 Extract Web Server Information with Nmap
-  12.1.8 Crack FTP Credentials with Wireshark

Fact Sheets

-  12.1.2 Web Server Hacking Facts
-  12.1.4 Web Server Attack Facts
-  12.1.10 Web Server Countermeasures Facts

Number of Exam Questions

13 questions

Total Time

About 73 minutes

12.2: Web Applications

Lecture Focus Questions:

- What are web application?
- What are the steps in the web application attack methodology?
- What are the steps in web application penetration testing?
- What are some measures you can take to help prevent web application attacks?

In this section, you will learn to:

- Perform hidden field manipulation attacks
- Exploit cross-site scripting vulnerabilities
- Scan a website with Acunetix







Key terms for this section include the following:

| Term | Definition |
|-----------------|---|
| Web application | A web application is software that has been installed on top of a web server. |

This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|------------|---|
| EC-Council | 3. Security <ul style="list-style-type: none"> • Information Security Attack Detection • Information Security Attack Prevention |
| | 4. Tools/Systems/Programs <ul style="list-style-type: none"> • Information Security Tools |
| | 5. Procedures/Methodology <ul style="list-style-type: none"> • Information Security Procedures |




Video/Demo

| | Time |
|---|------|
|  12.2.1 Web Applications | 4:39 |
|  12.2.3 Web Application Hacking | 5:32 |
|  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 |

Total Video Time

26:44

Fact Sheets

-  12.2.2 Web Application Facts
-  12.2.4 Web Application Hacking Facts
-  12.2.9 Web Application Countermeasure Facts

Number of Exam Questions

14 questions

Total Time

About 56 minutes

12.3: SQL Injections

Lecture Focus Questions:

- What is an SQL injection? Why is this attack method commonly used?
- What are the steps of the SQL injection methodology?
- What measures can you take to evade intrusion detection systems?
- What measures can you take to defend systems against SQL injection attacks?

In this section, you will learn to:

- Perform an SQL injection attack





Key terms for this section include the following:

| Term | Definition |
|---|---|
| Structured query language (SQL) | SQL is a language that was designed to request data from a database. |
| Structured query language (SQL) injection | SQL injection is an attack that attacks a web application by manipulating SQL statements entered into a web page. |

This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|----------------------------|---|
| TestOut Ethical Hacker Pro | 3.2 Perform active online attacks <ul style="list-style-type: none"> • Perform an SQL injection |
| | 3. Security <ul style="list-style-type: none"> • Information Security Attack Detection • Information Security Attack Prevention |
| EC-Council | 4. Tools/Systems/Programs <ul style="list-style-type: none"> • Information Security Tools |

Video/Demo

| | Time |
|--|------|
|  12.3.1 SQL Injection | 5:52 |
|  12.3.3 SQL Injection Attack Types | 4:32 |
|  12.3.5 Exploit SQL on a Web Page | 3:57 |
|  12.3.7 SQL Injection Countermeasures | 2:26 |

Total Video Time

16:47

Lab/Activity

🔒 12.3.6 Perform an SQL Injection Attack

Fact Sheets

- 📄 12.3.2 SQL Injection Facts
- 📄 12.3.4 SQL Injection Attack Facts
- 📄 12.3.8 SQL Injection Countermeasure Facts

Number of Exam Questions

8 questions

Total Time

About 52 minutes

13.1: Wi-Fi

Lecture Focus Questions:

- What is the main component used to link or bridge wireless devices?
- What is Wi-Fi overlap? Why is it important?
- What are two types of wireless connections?
- Which encryption method is used with WPA? Which method is used with WPA2?
- What is one of the key steps used to defend against WPA/WPA2 cracking?
- What type of system helps find and eliminate the threat of rogue access points?
- What is the purpose of performing a vulnerability scan?
- What is the purpose of performing a penetration test?

In this section, you will learn to:

- Discover a hidden network
- Discover a rogue DHCP server
- Locate a rogue wireless access point

Key terms for this section include the following:

| Term | Definition |
|-------------------------------|---|
| Wi-Fi | Wi-Fi is a trademarked term meaning IEEE 802.11x. Wi-Fi allows computers, smartphones, or other devices to connect wirelessly to the internet or communicate with one another wirelessly within a particular area. |
| Access Point (AP) | A device that allows wireless devices to connect to it by means of antennas. Acting as a wireless version of a switch, an access point connects users to other users within the network and can also serve as the point of interconnection between the wireless LAN and a wired network. Sometimes the access point is combined with the router, as is often the case with home wireless routers. |
| Hotspot | Mobile hotspots let you connect an internet-capable device to the internet through a wireless portable device such as a phone. |
| Service set identifier (SSID) | A unique character ID up to 32 characters long used to uniquely identify an access point. Each packet sent over a wireless network will include the SSID, ensuring that the data being sent over the air arrives at the correct location. |
| Open System Authentication | A system that allows any device to connect to the wireless network. The major advantage of open mode is its simplicity. Any client can connect easily and without complex configuration. For guest access only, these are often used at locations such as airports, coffee shops, and universities. |

| | |
|--|---|
| Pre-Shared Encryption Key | Each device that requires a wireless connection is installed with a software key that can be used to connect to the wireless network. When the client and the access point have different keys, access to the network is denied. |
| Passphrase | A passphrase is a combination of letters, numbers, spaces, and punctuation symbols used as a security key for network connections. |
| Wired Equivalent Privacy (WEP) | WEP is based on the RC4 encryption scheme and designed to provide the same level of security as a wired LAN. Because of 40-bit encryption and problems with the initialization vector (IV), it was found to be unsecure. |
| Wi-Fi Protected Access (WPA) | A security standard for wireless networks designed to be more secure than Wired Equivalent Privacy (WEP) and used as an interim replacement until WPA2 was released. |
| Temporal Key Integrity Protocol (TKIP) | A security protocol used in the IEEE 802.11 wireless networking standard. TKIP implements a key mixing function that combines the secret root key with the initialization vector before passing it to the RC4 cipher initialization. TKIP also implements a 64-bit Message Integrity Check (MIC). |
| Message Integrity Code (MIC) | The MIC value protects a message's data integrity and authenticity by using verifiers that detect any changes to the message content. This is also known as a Message Authentication code (MAC). |
| Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) | An encryption protocol designed for Wireless LAN products that implements the standards of the IEEE 802.11i. CCMP is an enhanced data cryptographic encapsulation mechanism designed for data confidentiality. |
| Lightweight Extensible Authentication Protocol (LEAP) | Created by Cisco, LEAP is an 802.1x authentication type for Wireless LANs that supports strong mutual authentication between the client and a RADIUS server with a logon password as the shared secret. It also provides dynamic per-user, per-session encryption keys. |
| Protected Extensible Authentication Protocol (PEAP) | An 802.1x authentication type for wireless. PEAP provides strong security, user database extensibility, and support for one-time token authentication and password change or aging. |
| Wardriving | The act of using a car and an electronic device to drive around and locate wireless networks. |
| MAC spoofing | Changing a network interface card's (NIC) media access control (MAC) address to a different MAC address in an attempt to impersonate another computer or disguise the source of the transmission. |

| | |
|------------------------------------|---|
| Ad hoc networking | A network that has been established between two or more computers without using a pre-existing infrastructure, such as routers in wired networks or access points in managed wireless networks. |
| Evil twin | A rogue access point that appears to be legitimate, but is set up to eavesdrop on wireless communications. In most cases, the evil twin is configured to use the same SSID and BSSID used by the legitimate AP. Since the evil twin is often configured to pass internet traffic through to the legitimate AP, users are unaware that their data is being monitored and captured. |
| Advanced Encryption Standard (AES) | A symmetric block cipher chosen by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data. AES is often used with WPA2 encryption methods, but can also be used with WPA encryption. |








This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|----------------------------|--|
| TestOut Ethical Hacker Pro | 1.2 Perform scanning <ul style="list-style-type: none"> Discover wireless devices |
| | 2.3 Gain access by cracking <ul style="list-style-type: none"> Crack Wi-Fi devices |
| | 3.3 Perform infrastructure attacks <ul style="list-style-type: none"> Access wireless networks |
| EC-Council | 2. Analysis/Assessment <ul style="list-style-type: none"> Information Security Assessment and Analysis |
| | 3. Security <ul style="list-style-type: none"> Information Security Controls Information Security Attack Detection Information Security Attack Prevention |
| | 4. Tools/Systems/Programs <ul style="list-style-type: none"> Information Security Tools |




5. Procedures/Methodology

- Information Security Procedures





S

| Video/Demo | Time |
|--|--------------|
|  13.1.1 Wireless Overview | 9:31 |
|  13.1.3 Wireless Encryption and Authentication | 8:56 |
|  13.1.5 Wireless Hacking | 10:51 |
|  13.1.7 Wi-Fi Packet Analysis | 5:33 |
|  13.1.8 Crack Wi-Fi Encryption with Aircrack-ng | 5:40 |
|  13.1.10 Wireless Hacking Countermeasure Tools | 11:12 |
|  13.1.12 Detect a Rogue Device | <u>5:53</u> |
| Total Video Time | 57:36 |

Lab/Activity

-  13.1.9 Discover a Hidden Network
-  13.1.13 Discover a Rogue DHCP Server
-  13.1.14 Locate a Rogue Wireless Access Point

Fact Sheets

-  13.1.2 Wireless Facts
-  13.1.4 Wireless Encryption and Authentication Facts
-  13.1.6 Wireless Hacking Facts
-  13.1.11 Wireless Hacking Countermeasures Tool Facts

Number of Exam Questions

15 questions

Total Time

About 129 minutes

13.2: Bluetooth Hacking

Lecture Focus Questions:

- What are the differences between Bluetooth and Wi-Fi?
- What are the threats from Bluetooth hacking?
- What are common forms of Bluetooth hacking?
- What tools can be used to perform Bluetooth hacking?
- What countermeasures can be used to help defeat Bluetooth hacking?

In this section, you will learn to:

- Discover Bluetooth devices

Key terms for this section include the following:



| Term | Definition |
|------------------------|--|
| BlueSmacking | A Bluetooth denial-of-service attack. |
| Bluejacking | An attack characterized by sending unwanted data to Bluetooth devices. |
| Bluesnarfing | An attack that uses the OBEX protocol to gain access to a Bluetooth device. |
| Bluesniffing | The use of the Bluesniff wardriving utility to discover Bluetooth devices. |
| Bluebugging | An attack that exploits a Bluetooth device to install a backdoor that bypasses normal authentication, giving full access to the device. |
| BluePrinting | The act of gathering details about a Bluetooth device that indicates its manufacturer and model. |
| Bluetooth MAC spoofing | An attack characterized by changing the device address of a Bluetooth device to match the address of a target device. |
| BluetoothView | A small utility that lists discoverable Bluetooth devices with information such as the device name, Bluetooth address, major device type, and minor device type. |
| BTScanner | A Bluetooth sniffing tool that provides the same functions as BluetoothView. |
| Btlejuice | A complete framework to perform man-in-the-middle attacks on Bluetooth smart devices. |
| Bluediving | A Bluetooth penetration suite used to implement BlueBug, BlueSnarf, and BlueSmack attacks as well as Bluetooth address spoofing. |
| Super Bluetooth Hack | An Android phone application that can be used to view the files on another Bluetooth-connected Android phone. |

This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|------|-----------|
|------|-----------|

| | |
|----------------------------|---|
| TestOut Ethical Hacker Pro | 1.2 Perform scanning |
| | <ul style="list-style-type: none"> Discover wireless devices |
| EC-Council | 3. Security |
| | <ul style="list-style-type: none"> Information Security Attack Detection |


Video/Demo

-  13.2.1 Bluetooth Hacking
-  13.2.3 Discover Vulnerable Bluetooth Devices

Time

6:45

3:28**Total Video Time****10:13****Lab/Activity**

-  13.2.4 Discover Bluetooth Devices

Fact Sheets

-  13.2.2 Bluetooth Hacking Facts

Number of Exam Questions

12 questions

Total Time*About 40 minutes*

13.3: Mobile Devices

Lecture Focus Questions:

- What are some security concerns that are unique to mobile devices or have a special emphasis in a mobile environment?
- Why is data loss on mobile devices a security concern?
- What is rooting and jailbreaking?
- What is sideloading?
- What are some security best practices for mobile device users and administrators?
- What is mobile device management?
- What is a BYOD policy?

In this section, you will learn to:

- Secure a mobile device

Key terms for this section include the following:







| Term | Definition |
|---|---|
| Mobile phishing attack | A social engineering attack that is perpetrated on a mobile user. The attack is often more productive on mobile device users since they can be easily distracted and might not be as alert to sharing sensitive information or downloading malware. |
| The Open Web Application Security Project (OWASP) | The organization that publishes an annual Top 10 Mobile Risks list. |
| Open source | Software code that is available to anyone without a fee and can be redistributed and modified. |
| Rooting | Overriding security features on an Android device in order to modify, remove, or replace applications; run apps with administrator privilege; change system settings; and gain low-level access to device hardware. |
| Jailbreaking | Overriding security features on an iOS device in order to sideload applications, run apps with administrator privilege, change system files, and gain low-level access to device hardware. |
| Sideloading | Downloading and installing unapproved apps on a mobile device. |
| Mobile device management (MDM) | A general term used to describe the policies and procedures used by an organization to maintain security and permissions on mobile devices. Also a specific term that describes the software administrators use to secure mobile devices and control them by enforcing enterprise policies. |

| | |
|------------------------------|---|
| Bring-your-own device (BYOD) | A policy that allows employees to use their own computers and mobile devices for work purposes. |
|------------------------------|---|

This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|----------------------------|---|
| TestOut Ethical Hacker Pro | 5.1 Defend systems and devices <ul style="list-style-type: none"> Secure mobile devices |
| | 1. Background <ul style="list-style-type: none"> Network and Communication Technologies Information Security Threats and Attack Vector Information Security Technologies |
| EC-Council | 3. Security <ul style="list-style-type: none"> Information Security Attack Detection Information Security Attack Prevention |
| | 4. Tools/Systems/Programs <ul style="list-style-type: none"> Information Security Tools |
| | 5. Procedures/Methodology <ul style="list-style-type: none"> Information Security Procedures |

Video/Demo

| | Time |
|--|-------------|
|  13.3.1 Mobile Device Attacks | 7:52 |
|  13.3.3 Mobile Device Operating Systems | 8:58 |
|  13.3.5 Secure a Device | 5:43 |
|  13.3.7 Mobile Device Hacking | 7:54 |
|  13.3.8 Hack Android with Binary Payloads | 7:18 |
|  13.3.10 Mobile Device Management | <u>6:00</u> |

Total Video Time

43:45

Lab/Activity

-  13.3.6 Secure a Mobile Device

Fact Sheets

-  13.3.2 Mobile Device Attack Facts

- ☰ 13.3.4 Mobile Device Operating System Facts
- ☰ 13.3.9 Mobile Device Hacking Facts
- ☰ 13.3.11 Mobile Device Management Facts

Number of Exam Questions

16 questions

Total Time

About 92 minutes

14.1: Cloud Computing

Lecture Focus Questions:

- What is cloud computing?
- What are the characteristics, types, and deployment models of cloud computing?
- What are some of the most prominent cloud computing risks, threats, and attacks?
- What are some cloud security tools that help combat attackers?

Key terms for this section include the following:

| Term | Definition |
|---|--|
| Content security policy (CSP) | CSP is a trusted entity that gives subscribers security tokens and electronic credentials. |
| Domain name system security extensions (DNSSEC) | DNSSEC is a network control. |
| Triple data encryption standard (3DES) | 3DES is a symmetric-key block cipher that applies the DES cipher algorithm three times to each data block. |
| Structured query language (SQL) | SQL is a standard computer language used with relational database management and data manipulation. |
| Cloud access security broker (CASB) | CASB is a software that sits between cloud service users and cloud applications to monitor all activity and enforce security policies. |
| Infrastructure as a service (IaaS) | IaaS is a cloud computing service model that delivers infrastructure to the client. |
| Platform as a service (PaaS) | PaaS is a cloud computing service model that delivers everything a developer needs to build an application. |
| Software as a service (SaaS) | SaaS is a cloud computing service model that delivers software applications to the client. |
| Quality of service (QoS) | QoS is a network control. |






| | |
|--|---|
| Service-level agreement (SLA) | SLA is an agreement between a service provider and a client, like a contract. |
| System development life cycle (SDLC) | SDLC is an application layer control. |
| Data loss prevention (DLP) | DLP is an information control. |
| Content management framework (CMF) | CMF is an information control. |
| Information security management program (ISMP) | ISMP is a program that protects information from being deleted, modified or stolen. |
| Governance risk compliance (GRC) | GRC is a management control. |
| Identity and access management (IAM) | IAM is a management control. |
| Virtual appliance/virtual machine (VA/VM) | VA/VM is a management control. |
| Network intrusion detection system/network intrusion protection system (NIDS/NIPS) | NIDS/NIPS is a network control. |
| Open authorization (OAuth) | OAuth is a network control. |
| Root of trust (RoT) | RoT is a security control. |
| Host-based intrusion detection system/host-based intrusion protection system (HIDS/HIPS) | HIDS/HIPS is a computation and storage control. |
| LoadStorm | LoadStorm is a cloud load testing solution to find the scalability of web or mobile applications. |
| BlazeMeter | BlazeMeter is a continuous testing solution to help with the early stages of app development. |

| | |
|---------|--|
| JMeter | JMeter is an Apache project used as a load testing tool for analyzing and measuring the performance of a variety of services, especially web applications. |
| Nexpose | Nexpose is a vulnerability scanner that strives to support the entire vulnerability management lifecycle. It integrates with Rapid7's Metasploit for vulnerability exploitation. |

This section helps you prepare for the following exam objectives:

| Exam | Objective |
|------------|--|
| EC-Council | 1. Background <ul style="list-style-type: none"> Network and Communication Technologies Information Security Threats and Attack Vector Information Security Technologies 3. Security <ul style="list-style-type: none"> Information Security Controls 4. Tools/Systems/Programs <ul style="list-style-type: none"> Information Security Tools |





Video/Demo

| | Time |
|--|-------------|
|  14.1.1 Cloud Computing | 13:06 |
|  14.1.3 Cloud Computing Threats | 6:13 |
|  14.1.5 Cloud Computing Attacks | 9:04 |
|  14.1.7 Cloud Security | 6:40 |
|  14.1.9 Secure Files in the Cloud | <u>3:52</u> |

Total Video Time

38:55

Fact Sheets

-  14.1.2 Cloud Computing Facts
-  14.1.4 Cloud Threats Facts
-  14.1.6 Cloud Attacks Facts
-  14.1.8 Cloud Security Facts

Number of Exam Questions

13 questions

Total Time

About 72 minutes

14.2: Internet of Things

Lecture Focus Questions:

- What is IoT?
- What are the primary systems of IoT technology? How do they work together?
- What layers are included in the IoT architecture? How do they help you understand how IoT systems work?
- What are some of the most prominent IoT application areas?
- What are some of the technologies and protocols related to IoT?
- How do the different IoT communication models promote flexibility and convenience for users?
- What security challenges does the IoT world currently face?
- What are some of the most prominent attacks on IoT?
- How do hackers find vulnerabilities and then launch attacks on IoT? What steps are necessary for successful IoT hacking?
- What are some tools that make IoT hacking easier?

In this section, you will learn to:

- Scan for IoT devices

Key terms for this section include the following:

| Term | Definition |
|--------------------------------------|--|
| Internet of things (IoT) | IoT is a system of connected computing devices and other things that use unique identifiers and the ability to send data over a network without requiring human interaction. |
| Internet of everything (IoE) | IoE is another name for IoT. |
| Industrial internet of things (IIoT) | IIoT encompasses all IoT systems that are applied in the industrial sector. |
| Near-field communication (NFC) | NFC is a simple, low-energy, and versatile protocol that uses magnetic field induction to communicate between mobile and standard electronic devices. |
| Bluetooth low energy (BLE) | Also known as Bluetooth Smart, BLE is a wireless personal area network. |
| Light-Fidelity (Li-Fi) | Li-Fi is a Visible Light Communications system. It uses light bulbs to transfer data at a high speed of 224Gigabits per second. |
| Quick Response (QR) | QR codes are two-dimensional tags attached to products. They are machine-readable and contain information about the product. |
| HaLow | HaLow is a branch of Wi-Fi with extended range. |







| | |
|---|--|
| LTE-Advanced | LTE-Advanced is a mobile communication that provides higher capacity than LTE. |
| LoRaWAN | A low-power wide area network for IoT devices. |
| Sigfox | Sigfox is a global network operator. |
| Neul | NeulNET is the cloud-based solution that offers an end-to-end pipe. |
| Very Small Aperture Terminal (VSAT) | VSAT is a long-range protocol that uses small dish antennas to transfer both broadband and narrowband data. |
| Multimedia over Coax Alliance (MoCA) | MoCA is a long-range protocol that uses coaxial cables to provide high-definition videos of a home and other content related to it. |
| Power-line Communication (PLC) | PLC is a long-range protocol that uses electrical wires to transmit power and data from one point to another. |
| Broadband over power lines (BLP) | BLP is a sector of PLC. |
| RIOT | RIOT is a free, open-source operating system for IoT. |
| ARM mbed | Arm Mbed IoT Device Platform is an operating system for IoT devices. |
| RealSense OS X | RealSense OS X is an operating system for IoT. |
| Real-time operating system (RTOS) | A real-time operating system is designed to function without buffer delays. |
| Brillo | Brillo is an android-based embedded OS for IoT. |
| Contiki | Contiki is an open-source operating system for IoT. |
| Zephyr | Zephyr is an operating system for IoT. |
| Apache Mynewt | Apache Mynewt is a modular real-time operating system for IoT. |
| Two-factor authentication (2FA) | 2FA is a two-factor authentication standard that strengthens IoT devices against hacking. |
| Heating, ventilation, and air conditioning (HVAC) | HVAC includes different systems, machines, and technologies that provide comfort through environmental regulation in most indoor settings. |
| Censys | Censys is a search engine for IoT devices. |
| Thingful | Thingful is a search engine for IoT devices. |
| Foren6 | Foren6 is a non-intrusive 6LoWPAN network analysis tool. |
| Zniffer | Zniffer is a development tool that captures Z-Wave communication signals and presents them visually in a graphical user interface. |
| CloudShark | CloudShark is a capture management system. |
| RFCrack | RFCrack is an RF test bench. |

| | |
|-----------------|---|
| KillerBee | KillerBee is a Python-based tool. |
| SquashFS/CramFS | CramFS (compressed ROM file system) is a Linux compressed read-only file system. SquashFS is a newer version of CramFS. |
| ZMap | ZMap is a network scanner. |
| ZGrab | ZGrab is a Go-based Application layer scanner. |
| beSTORM | beSTORM is a tool that performs an exhaustive analysis. |

This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|----------------------------|---|
| TestOut Ethical Hacker Pro | 1.2 Perform scanning <ul style="list-style-type: none"> • Scan for IoT devices |
| | 1. Background <ul style="list-style-type: none"> • Network and Communication Technologies • Information Security Threats and Attack Vector • Information Security Technologies |
| EC-Council | 4. Tools/Systems/Programs <ul style="list-style-type: none"> • Information Security Tools |
| | 5. Procedures/Methodology <ul style="list-style-type: none"> • Information Security Procedures |

Video/Demo

| | Time |
|---|-------------|
|  14.2.1 Internet of Things | 6:40 |
|  14.2.3 IoT Technologies and Protocols | 8:37 |
|  14.2.5 IoT Security Challenges | 7:17 |
|  14.2.7 IoT Hacking | 6:14 |
|  14.2.9 Search for IoT with Shodan | 4:38 |
|  14.2.10 Scan for IoT with Nmap | <u>3:23</u> |

Total Video Time

36:49

Lab/Activity

-  14.2.11 Scan for IoT Devices

Fact Sheets

-  14.2.2 Internet of Things Facts
-  14.2.4 IoT Technologies and Protocols Facts
-  14.2.6 IoT Security Challenge Facts
-  14.2.8 IoT Hacking Facts

Number of Exam Questions

10 questions

Total Time

About 79 minutes

15.1: Cryptography

Lecture Focus Questions:

- What is the difference between a transposition cipher and a substitution cipher?
- A user needs to communicate securely with five other users using symmetric key encryption. How many keys are required?
- How are symmetric keys typically exchanged between communication partners?
- What is an advantage of increasing the number of bits in the key? What is a disadvantage?
- How do public keys differ from private keys? What is the relationship between the two?
- For which type of environment is asymmetric cryptography best suited?
- Why does asymmetric encryption require fewer keys than symmetric encryption?

In this section, you will learn to:

- Verify MD5 hash integrity

Key terms for this section include the following:





| Term | Definition |
|------------------|--|
| Cryptography | The science and study of concealing information that is used in electronic communication to protect the privacy of passwords, secret keys, and data. |
| Cipher/Algorithm | A process or formula used to convert or otherwise hide the meaning of a message. |
| Key | A variable in a cipher that is used to encrypt or decrypt a message. |
| Plain text | The readable form of a communication that is visible to everyone. |
| Ciphertext | An encrypted form of a communication that makes the communication unreadable to all but those who have the decryption cipher or key. |
| Encryption | The process of using an algorithm or cipher to transform data from clear text to ciphertext. The intent is to protect the confidentiality, integrity, and authenticity of the message. |
| Decryption | The process of converting data from ciphertext into plain text so that it can be read. |
| Steganography | The process of hiding data or a message so that only the sender and the recipient suspects that the hidden data exists. |
| Cryptanalysis | The method that is used to recover data that has been encrypted without having access to the key used in the encryption process. |

| | |
|--|---|
| Symmetric Encryption | A form of cryptography that provides confidentiality with a weak form of authentication or integrity. |
| Block Cipher | Symmetric encryption that transposes plain text to ciphertext in chunks (block by block). |
| Stream Cipher | A symmetric encryption that is performed on each bit within a stream of data in real time. |
| Ron's Cipher v5 or Ron's Code v5 (RC5) | A symmetric cryptography method that implements a symmetric-key block cipher cryptographic algorithm produced by RSA Security, Inc. |
| Ron's Cipher v6 or Ron's Code v6 (RC6) | A symmetric-key block cipher cryptographic algorithm that was produced by RSA Security, Inc. |
| International Data Encryption Algorithm (IDEA) | A symmetric cryptography method that is a minor revision of an earlier PES (Proposed Encryption Standard). It uses 64-bit blocks with 128-bit keys and is used by Pretty Good Privacy (PGP) email encryption. |
| Data Encryption Standard (DES) | A very popular symmetric cryptography method created by the National Security Agency (NSA) that was one of the first symmetric encryption methods. It is now obsolete due to known weaknesses. |
| Triple DES (3DES) | An enhanced version of DES that corrects the DES's known weaknesses. |
| Advanced Encryption Standard (AES) | An iterative symmetric block cipher that was developed as a replacement for DES in 2001. |
| Blowfish | A keyed symmetric block cipher that was intended to be free of the problems associated with other algorithms and replace DES. |
| Twofish | A symmetric block cipher that permits a wide variety of tradeoffs between speed, software size, key setup time, and memory. |
| Asymmetric Encryption | An encryption method that uses two mathematically related keys called a key pair. |
| Challenge-Handshake Authentication Protocol (CHAP) | Challenge-Handshake Authentication Protocol is a procedure that uses a challenge/response (three-way handshake) mechanism to protect passwords. |
| Diffie-Hellman Key Exchange | Diffie-Hellman Key Exchange is an asymmetric algorithm that generates symmetric keys simultaneously at sender and recipient sites over non-secure channels. |
| Digital Signature Algorithm (DSA) | A federal standard for digital signatures that uses modular exponentiation and the discrete logarithm problem. |
| Elliptic Curve Cryptography (ECC) | A public-key cryptography method that is based on groups of numbers in an elliptical curve. |

| | |
|--|---|
| Extensible Authentication Protocol (EAP) | A framework that provides a standardized method to negotiate wireless authentications between wireless devices. |
| Message Digest Function (MD5) | An algorithm that produces a value of 128 bits with 32 hexadecimal characters. |
| Rivest, Shamir, Adleman (RSA) | A public-key cryptosystem that is used for secure data transmission. |
| Secure Hashing Algorithm (SHA) | A cryptographic function that produces a hash value for input data. |

This section helps you prepare for the following certification exam objectives:




| Exam | Objective |
|----------------------------|---|
| TestOut Ethical Hacker Pro | 5.1 Defend systems and devices <ul style="list-style-type: none"> • Ensure file integrity |
| | 3. Security <ul style="list-style-type: none"> • Information Security Attack Prevention |
| EC-Council | 4. Tools/Systems/Programs <ul style="list-style-type: none"> • Information Security Tools |
| | 5. Procedures/Methodology <ul style="list-style-type: none"> • Information Security Procedures |

| Video/Demo | Time |
|--|--------------|
|  15.1.1 Cryptography | 5:22 |
|  15.1.3 Symmetric Encryption | 4:11 |
|  15.1.5 Asymmetric Encryption | 5:40 |
|  15.1.7 Verify MD5 Hash Integrity | <u>2:50</u> |
| Total Video Time | 18:03 |

Lab/Activity

-  15.1.8 Compare an MD5 Hash

Fact Sheets

-  15.1.2 Cryptography Facts
-  15.1.4 Symmetric Encryption Facts
-  15.1.6 Asymmetric Encryption Facts

Number of Exam Questions

16 questions

Total Time

About 62 minutes

15.2: Public Key Infrastructure

Lecture Focus Questions:

- What is public key infrastructure (PKI)?
- Where is PKI used?
- What are the key components of PKI?

Key terms for this section include the following:

| Term | Definition |
|-------------------------------|---|
| Public key infrastructure | A security architecture often used to ensure data transmissions between entities are validated and secure. |
| Certificate management system | The primary component that manages the certificate process. |
| Digital certificates | Electronic passwords created using PKI that allow secure data exchange over the internet. |
| Validation authority (VA) | The PKI component used to verify the validity of a digital certificate by way of the X.509 standard and RFC 5280. |
| Certificate authority (CA) | The organization that issues the digital certificate and is also the controller of the PKI certificates. |
| Registration authority (RA) | Acts as the verifier for the CA. |

This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|------------|---|
| EC-Council | 5. Procedures/Methodology <ul style="list-style-type: none"> • Information Security Procedures |

Video/Demo

 15.2.1 Public Key Infrastructure

Time

6:49

Total Video Time

6:49

Fact Sheets

 15.2.2 Public Key Infrastructure Facts

Number of Exam Questions

5 questions

Total Time

About 17 minutes

15.3: Cryptography Implementations

Lecture Focus Questions:

- What can you encrypt with GPG?
- What is the benefit of using encryption?
- What is the difference between SSL and TLS?

In this section, you will learn to:

- Encrypt a hard drive





Key terms for this section include the following:

| Term | Definition |
|--------------------------------------|---|
| Pretty Good Privacy (PGP) | A popular encryption program that can be used to encrypt texts, emails, files, folders, and disks. |
| GNU Privacy Guard (GPG) | An encryption tool that is used to protect laptops, desktops, USB drives, optical media, and smartphones. GPG is an implementation of the PGP protocol. |
| BitLocker | A Microsoft Windows utility that provides full volume encryption. |
| Windows Encrypting File System (EFS) | A proprietary encryption function of Windows operating systems. |
| Secure Sockets Layer (SSL) | An Application layer protocol developed for managing security of message transmission on the internet. |
| Transport Layer Security (TLS) | A protocol used to establish a secure connection between a client and a server. TLS ensures privacy and integrity of information during transmission. |
| OpenSSL | An open-source cryptography toolkit implementing SSL and TLS network protocols and related cryptography standards. |
| Keyczar | An open-source cryptographic toolkit designed to make it easier and safer for developers to use cryptography in applications. |

This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|----------------------------|---|
| TestOut Ethical Hacker Pro | 5.1 Defend systems and devices <ul style="list-style-type: none"> • Implement drive encryption |
| | 3. Security |
| EC-Council | <ul style="list-style-type: none"> • Information Security Attack Prevention |
| | 4. Tools/Systems/Programs |

- Information Security Tools

| Video/Demo | Time |
|--|--------------|
|  15.3.1 Disk and Email Encryption | 5:58 |
|  15.3.2 PGP and GPG | 4:22 |
|  15.3.4 Encrypt Files with GPG | 5:46 |
|  15.3.5 Encrypt a Hard Disk | <u>6:01</u> |
| Total Video Time | 22:07 |

Lab/Activity

-  15.3.6 Encrypt a Hard Drive

Fact Sheets

-  15.3.3 Disk and Email Encryption Facts

Number of Exam Questions

5 questions

Total Time

About 45 minutes

15.4: Cryptanalysis and Cryptographic Attack Countermeasures

Lecture Focus Questions:

- What are three types of cryptanalysis methods?
- What are some of the common code breaking methods?
- What are three countermeasures that can be used to prevent cryptography attacks?



Key terms for this section include the following:

| Term | Definition |
|----------------------------|---|
| Linear cryptanalysis | Linear cryptanalysis finds the affine approximations to the action of a cipher. |
| Differential cryptanalysis | A form of cryptanalysis applicable to symmetric key algorithms. Differential cryptanalysis works on statistical differences between ciphertexts of chosen data. |
| Integral cryptanalysis | A integral cryptanalysis attack is useful against block ciphers based on substitution-permutation networks. It is an extension of differential cryptanalysis. |
| Brute force attack | An attack in which cryptography keys are discovered by trying every possible combination. |
| Frequency analysis | The study of the frequency of letters or groups of letters in a ciphertext. |
| One-time pad | A cryptography method that contains many non-repeating, randomly chosen groups of letters or numbers. |

This section helps you prepare for the following certification exam objectives:

| Exam | Objective |
|------------|---|
| EC-Council | 3. Security <ul style="list-style-type: none"> • Information Security Attack Detection • Information Security Attack Prevention |
| | 4. Tools/Systems/Programs <ul style="list-style-type: none"> • Information Security Programs • Information Security Tools |

Video/Demo

| | |
|---|------|
|  15.4.1 Cryptanalysis and Cryptographic Attack Countermeasures | 5:56 |
|  15.4.3 Data Encryption | 4:31 |

Total Video Time

10:27

Fact Sheets

📄 15.4.2 Cryptanalysis and Cryptographic Attack Countermeasures Facts

Number of Exam Questions

5 questions

Total Time

About 21 minutes

Practice Exams

A.0: TestOut Ethical Hacker Pro - Practice Exams

TestOut Ethical Hacker Pro Certification Practice Exam (18 questions)

B.0: EC-Council Certified Ethical Hacker - Practice Exams

Appendix A: Approximate Time for the Course

The total time for the LabSim for TestOut Ethical Hacker Pro course is approximately **42 hours and 55 minutes**. Time is calculated by adding the approximate time for each section which is calculated using the following elements:

- Video/demo times
- Text Lessons (5 minutes assigned per text lesson)
- Simulations (12 minutes assigned per simulation)
- Questions (1 minute per question)

Additionally, there are approximately another **28 hours and 38 minutes** of Practice Test material at the end of the course.

The breakdown for this course is as follows:

| Module | Sections | Time | Videos | Labs | Text | Exams |
|--|--|-------------|-------------|-------------|-------------|-------------|
| 1.0: Introduction to Ethical Hacking | | | | | | |
| | 1.1: Introduction | 31 | 31 | 0 | 0 | 0 |
| | Total | 0:31 | 0:31 | 0:00 | 0:00 | 0:00 |
| 2.0: Introduction to Penetration Testing | | | | | | |
| | 2.1: Penetration Testing Process and Types | 18 | 5 | 0 | 5 | 8 |
| | 2.2: Threat Actors | 17 | 7 | 0 | 5 | 5 |
| | 2.3: Target Selection | 29 | 9 | 0 | 5 | 15 |
| | 2.4: Assessment Types | 25 | 7 | 0 | 5 | 13 |
| | 2.5: Legal and Ethical Compliance | 42 | 17 | 0 | 10 | 15 |
| | Total | 2:11 | 0:45 | 0:00 | 0:30 | 0:56 |
| 3.0: Social Engineering and Physical Security | | | | | | |
| | 3.1: Social Engineering | 79 | 35 | 12 | 20 | 12 |
| | 3.2: Physical Security | 39 | 18 | 0 | 10 | 11 |
| | 3.3: Countermeasures and Prevention | 31 | 9 | 12 | 5 | 5 |
| | Total | 2:29 | 1:02 | 0:24 | 0:35 | 0:28 |
| 4.0: Reconnaissance | | | | | | |
| | 4.1: Reconnaissance Overview | 53 | 19 | 12 | 10 | 12 |
| | 4.2: Reconnaissance Countermeasures | 73 | 15 | 48 | 5 | 5 |
| | Total | 2:06 | 0:34 | 1:00 | 0:15 | 0:17 |
| 5.0: Scanning | | | | | | |
| | 5.1: Scanning Overview | 74 | 21 | 24 | 15 | 14 |
| | 5.2: Banner Grabbing | 15 | 5 | 0 | 5 | 5 |
| | Total | 1:29 | 0:26 | 0:24 | 0:20 | 0:19 |
| 6.0: Enumeration | | | | | | |
| | 6.1: Enumeration Overview | 92 | 34 | 36 | 10 | 12 |
| | 6.2: Enumeration Countermeasures | 29 | 7 | 12 | 5 | 5 |
| | Total | 2:01 | 0:41 | 0:48 | 0:15 | 0:17 |

| | | | | | |
|---|-------------|-------------|-------------|-------------|-------------|
| 7.0: Analyze Vulnerabilities | | | | | |
| 7.1: Vulnerability Assessment | 26 | 13 | 0 | 5 | 8 |
| 7.2: Vulnerability Management Life Cycle | 27 | 9 | 0 | 10 | 8 |
| 7.3: Vulnerability Scoring Systems | 18 | 6 | 0 | 5 | 7 |
| 7.4: Vulnerability Assessment Tools | 88 | 16 | 60 | 5 | 7 |
| Total | 2:39 | 0:44 | 1:00 | 0:25 | 0:30 |
| 8.0: System Hacking | | | | | |
| 8.1: System Hacking | 124 | 48 | 60 | 5 | 11 |
| 8.2: Privilege Escalation | 67 | 29 | 24 | 5 | 9 |
| 8.3: Maintain Access | 48 | 14 | 24 | 5 | 5 |
| 8.4: Cover Your Tracks | 87 | 28 | 36 | 10 | 13 |
| Total | 5:26 | 1:59 | 2:24 | 0:25 | 0:38 |
| 9.0: Malware | | | | | |
| 9.1: Malware | 65 | 33 | 0 | 20 | 12 |
| 9.2: Combat Malware | 69 | 11 | 48 | 5 | 5 |
| Total | 2:14 | 0:44 | 0:48 | 0:25 | 0:17 |
| 10.0: Sniffers, Session Hijacking, and Denial of Service | | | | | |
| 10.1: Sniffing | 137 | 41 | 72 | 10 | 14 |
| 10.2: Session Hijacking | 106 | 31 | 48 | 15 | 12 |
| 10.3: Denial of Service | 104 | 28 | 48 | 15 | 13 |
| Total | 5:47 | 1:40 | 2:48 | 0:40 | 0:39 |
| 11.0: IDS, Firewalls, and Honeypots | | | | | |
| 11.1: Intrusion Detection Systems | 88 | 42 | 12 | 20 | 14 |
| 11.2: Firewalls | 111 | 34 | 48 | 15 | 14 |
| 11.3: Honeypots | 46 | 13 | 12 | 10 | 11 |
| Total | 4:05 | 1:29 | 1:12 | 0:45 | 0:39 |
| 12.0: Web Servers, Web Applications, and SQL Injections | | | | | |
| 12.1: Web Servers | 73 | 21 | 24 | 15 | 13 |
| 12.2: Web Applications | 56 | 27 | 0 | 15 | 14 |
| 12.3: SQL Injections | 52 | 17 | 12 | 15 | 8 |
| Total | 3:01 | 1:05 | 0:36 | 0:45 | 0:35 |
| 13.0: Wi-Fi, Bluetooth, and Mobile Devices | | | | | |
| 13.1: Wi-Fi | 129 | 58 | 36 | 20 | 15 |
| 13.2: Bluetooth Hacking | 40 | 11 | 12 | 5 | 12 |
| 13.3: Mobile Devices | 92 | 44 | 12 | 20 | 16 |
| Total | 4:21 | 1:53 | 1:00 | 0:45 | 0:43 |
| 14.0: Cloud Computing and Internet of Things | | | | | |
| 14.1: Cloud Computing | 72 | 39 | 0 | 20 | 13 |
| 14.2: Internet of Things | 79 | 37 | 12 | 20 | 10 |
| Total | 2:31 | 1:16 | 0:12 | 0:40 | 0:23 |
| 15.0: Cryptography | | | | | |
| 15.1: Cryptography | 62 | 19 | 12 | 15 | 16 |
| 15.2: Public Key Infrastructure | 17 | 7 | 0 | 5 | 5 |
| 15.3: Cryptography Implementations | 45 | 23 | 12 | 5 | 5 |
| 15.4: Cryptanalysis and Cryptographic Attack Countermeasures | 21 | 11 | 0 | 5 | 5 |
| Total | 2:25 | 1:00 | 0:24 | 0:30 | 0:31 |

| Total Course Time 42:57 | | |
|--|----------------------------|--------------|
| Practice Exams | | |
| A.0: TestOut Ethical Hacker Pro - Practice Exams | Number of Questions | Time |
| A.2: TestOut Ethical Hacker Pro Practice Exams - All Questions | 65 | 13:00 |
| A.3: TestOut Ethical Hacker Pro Certification Practice Exam | 18 | 2:00 |
| Total | 83 | 15:00 |
| B.0: EC-Council Certified Ethical Hacker - Practice Exams | Number of Questions | Time |
| B.2: Ethical Hacker Practice Exams - 20 Random Questions | 140 | 2:20 |
| B.3: Ethical Hacker Practice Exams - All Questions | 438 | 7:18 |
| B.4: Ethical Hacker Practice Exams - Practice Certification | 125 | 4:00 |
| Total | 703 | 13:38 |
| Total Practice Exam Time 28:38 | | |