

CompTIA®

The Official CompTIA

PenTest+

Study Guide

Exam PTO-002



Official CompTIA Content Series for CompTIA Performance Certifications

**The Official
CompTIA
PenTest+
Study Guide
(Exam PT0-002)**

Course Edition: 1.0

Acknowledgments



Lisa Bock, Author

Co-authors:

Henry Flefel, NC-Expert

Phil Morgan, NC-Expert

Rie Vainstein, NC-Expert

Thomas Reilly, Senior Vice President, Learning

Katie Hoenicke, Senior Director, Product Management

Evan Burns, Senior Manager, Learning Technology Operations and Implementation

James Chesterfield, Manager, Learning Content and Design

Becky Mann, Director, Product Development

Danielle Andries, Manager, Product Development

Notices

Disclaimer

While CompTIA, Inc. takes care to ensure the accuracy and quality of these materials, we cannot guarantee their accuracy, and all materials are provided without any warranty whatsoever, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. The use of screenshots, photographs of another entity's products, or another entity's product name or service in this book is for editorial purposes only. No such use should be construed to imply sponsorship or endorsement of the book by nor any affiliation of such entity with CompTIA. This courseware may contain links to sites on the internet that are owned and operated by third parties (the "External Sites"). CompTIA is not responsible for the availability of, or the content located on or through, any External Site. Please contact CompTIA if you have any concerns regarding such links or External Sites.

Trademark Notice

CompTIA®, PenTest+®, and the CompTIA logo are registered trademarks of CompTIA, Inc., in the U.S. and other countries. All other product and service names used may be common law or registered trademarks of their respective proprietors.

Copyright Notice

Copyright © 2021 CompTIA, Inc. All rights reserved. Screenshots used for illustrative purposes are the property of the software proprietor. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of CompTIA, 3500 Lacey Road, Suite 100, Downers Grove, IL 60515-5439.

This book conveys no rights in the software or other products about which it was written; all use or licensing of such software or other products is the responsibility of the user according to terms and conditions of the owner. If you believe that this book, related materials, or any other CompTIA materials are being reproduced or transmitted without permission, please call 1-866-835-8020 or visit <https://help.comptia.org>.

Table of Contents

Lesson 1: Scoping Organizational/Customer Requirements	1
Topic 1A: Define Organizational PenTesting.....	2
Topic 1B: Acknowledge Compliance Requirements.....	8
Topic 1C: Compare Standards and Methodologies	12
Topic 1D: Describe Ways to Maintain Professionalism	18
Lesson 2: Defining the Rules of Engagement.....	23
Topic 2A: Assess Environmental Considerations.....	24
Topic 2B: Outline the Rules of Engagement.....	29
Topic 2C: Prepare Legal Documents	35
Lesson 3: Footprinting and Gathering Intelligence	41
Topic 3A: Discover the Target	42
Topic 3B: Gather Essential Data	51
Topic 3C: Compile Website Information.....	57
Topic 3D: Discover Open-Source Intelligence Tools	65
Lesson 4: Evaluating Human and Physical Vulnerabilities	75
Topic 4A: Exploit the Human Psyche	76
Topic 4B: Summarize Physical Attacks	85
Topic 4C: Use Tools to Launch a Social Engineering Attack	92
Lesson 5: Preparing the Vulnerability Scan	99
Topic 5A: Plan the Vulnerability Scan	100
Topic 5B: Detect Defenses.....	109
Topic 5C: Utilize Scanning Tools	114

Lesson 6: Scanning Logical Vulnerabilities	121
Topic 6A: Scan Identified Targets	122
Topic 6B: Evaluate Network Traffic	130
Topic 6C: Uncover Wireless Assets.....	137
Lesson 7: Analyzing Scanning Results	143
Topic 7A: Discover Nmap and NSE	144
Topic 7B: Enumerate Network Hosts.....	150
Topic 7C: Analyze Output from Scans.....	155
Lesson 8: Avoiding Detection and Covering Tracks	167
Topic 8A: Evade Detection.....	168
Topic 8B: Use Steganography to Hide and Conceal.....	177
Topic 8C: Establish a Covert Channel.....	185
Lesson 9: Exploiting the LAN and Cloud	193
Topic 9A: Enumerating Hosts.....	194
Topic 9B: Attack LAN Protocols	202
Topic 9C: Compare Exploit Tools	208
Topic 9D: Discover Cloud Vulnerabilities	215
Topic 9E: Explore Cloud-Based Attacks.....	220
Lesson 10: Testing Wireless Networks	229
Topic 10A: Discover Wireless Attacks	230
Topic 10B: Explore Wireless Tools	238
Lesson 11: Targeting Mobile Devices	245
Topic 11A: Recognize Mobile Device Vulnerabilities.....	246
Topic 11B: Launch Attacks on Mobile Devices.....	253
Topic 11C: Outline Assessment Tools for Mobile Devices	260

Lesson 12: Attacking Specialized Systems	267
Topic 12A: Identify Attacks on the IoT.....	268
Topic 12B: Recognize Other Vulnerable Systems	275
Topic 12C: Explain Virtual Machine Vulnerabilities	280
Lesson 13: Web Application-Based Attacks	289
Topic 13A: Recognize Web Vulnerabilities	290
Topic 13B: Launch Session Attacks	294
Topic 13C: Plan Injection Attacks	299
Topic 13D: Identify Tools	305
Lesson 14: Performing System Hacking	311
Topic 14A: System Hacking	312
Topic 14B: Use Remote Access Tools.....	315
Topic 14C: Analyze Exploit Code	319
Lesson 15: Scripting and Software Development.....	329
Topic 15A: Analyzing Scripts and Code Samples.....	330
Topic 15B: Create Logic Constructs.....	337
Topic 15C: Automate Penetration Testing	347
Lesson 16: Leveraging the Attack: Pivot and Penetrate	357
Topic 16A: Test Credentials.....	358
Topic 16B: Move Throughout the System.....	366
Topic 16C: Maintain Persistence	378
Lesson 17: Communicating During the PenTesting Process	389
Topic 17A: Define the Communication Path.....	390
Topic 17B: Communication Triggers	393
Topic 17C: Use Built-In Tools for Reporting.....	397

Lesson 18: Summarizing Report Components	403
Topic 18A: Identify Report Audience	404
Topic 18B: List Report Contents	407
Topic 18C: Define Best Practices for Reports	415
Lesson 19: Recommending Remediation	425
Topic 19A: Employ Technical Controls	426
Topic 19B: Administrative and Operational Controls	433
Topic 19C: Physical Controls	442
Lesson 20: Performing Post-Report Delivery Activities	445
Topic 20A: Post-Engagement Cleanup	446
Topic 20B: Follow-Up Actions	450
Appendix A: Mapping Course Content to CompTIA Certification+ (PT0-002)	A-1
Solutions	S-1
Glossary	G-1
Index	I-1

About This Course

CompTIA is a not-for-profit trade association with the purpose of advancing the interests of IT professionals and IT channel organizations; its industry-leading IT certifications are an important part of that mission. CompTIA's PenTest+ Certification is an intermediate-level certification designed for professionals with three to four years of hands-on experience working in a security consultant or penetration tester job role.

This exam will certify the successful candidate has the knowledge and skills required to plan and scope a penetration testing engagement, understand legal and compliance requirements, perform vulnerability scanning and penetration testing using appropriate tools and techniques, and then analyze the results and produce written reports containing proposed remediation techniques, effectively communicate results to the management team, and provide practical recommendations.

CompTIA PenTest+ Exam Objectives

Course Description

Course Objectives

This course can benefit you in two ways. If you intend to pass the CompTIA PenTest+ (Exam PT0-002) certification examination, this course can be a significant part of your preparation. But certification is not the only key to professional success in the field of server management. Today's job market demands individuals have demonstrable skills, and the information and activities in this course can help you build your penetration testing skill set so that you can confidently perform your duties in a security consultant or penetration tester job role.

On course completion, you will be able to:

- Scope organizational/customer requirements.
- Define the rules of engagement.
- Footprint and gather intelligence.
- Evaluate human and physical vulnerabilities.
- Prepare the vulnerability scan.
- Scan logical vulnerabilities.
- Analyze scan results.
- Avoid detection and cover tracks.
- Exploit the LAN and cloud.
- Test wireless networks.
- Target mobile devices.
- Attack specialized systems.
- Perform web application-based attacks.
- Perform system hacking.
- Script and software development.

- Leverage the attack: pivot and penetrate.
- Communicate during the PenTesting process.
- Summarize report components.
- Recommend remediation.
- Perform post-report delivery activities.

Target Student

The Official CompTIA PenTest+ Guide (Exam PT0-002) is the primary course you will need to take if your job responsibilities include planning and scoping, information gathering and vulnerability scanning, attacks and exploits, reporting and communication, and tools and code analysis. You can take this course to prepare for the CompTIA PenTest+ (Exam PT0-002) certification examination.

Prerequisites

To ensure your success in this course, you should have basic IT skills comprising three to four years of hands-on experience working in a performing penetration tests, vulnerability assessments, and code analysis. CompTIA Network+ certification, Security+ certification, or the equivalent knowledge is strongly recommended.



The prerequisites for this course might differ significantly from the prerequisites for the CompTIA certification exams. For the most up-to-date information about the exam prerequisites, complete the form on this page: www.comptia.org/training/resources/exam-objectives.

How to Use The Study Notes

The following sections will help you understand how the course structure and components are designed to support mastery of the competencies and tasks associated with the target job roles and help you to prepare to take the certification exam.

As You Learn



At the top level, this course is divided into **lessons**, each representing an area of competency within the target job roles. Each lesson is composed of a number of topics. A **topic** contains subjects that are related to a discrete job task, mapped to objectives and content examples in the CompTIA exam objectives document. Rather than follow the exam domains and objectives sequence, lessons and topics are arranged in order of increasing proficiency. Each topic is intended to be studied within a short period (typically 30 minutes at most). Each topic is concluded by one or more activities, designed to help you to apply your understanding of the study notes to practical scenarios and tasks.

Additional to the study content in the lessons, there is a glossary of the terms and concepts used throughout the course. There is also an index to assist in locating particular terminology, concepts, technologies, and tasks within the lesson and topic content.



In many electronic versions of the book, you can click links on key words in the topic content to move to the associated glossary definition and on page references in the index to move to that term in the content. To return to the previous location in the document after clicking a link, use the appropriate functionality in your eBook viewing software.

Watch throughout the material for the following visual cues.

Student Icon	Student Icon Descriptive Text
	A Note provides additional information, guidance, or hints about a topic or task.
	A Caution note makes you aware of places where you need to be particularly careful with your actions, settings, or decisions so that you can be sure to get the desired results of an activity or task.

As You Review

Any method of instruction is only as effective as the time and effort you, the student, are willing to invest in it. In addition, some of the information that you learn in class may not be important to you immediately, but it may become important later. For this reason, we encourage you to spend some time reviewing the content of the course after your time in the classroom.

Following the lesson content, you will find a table mapping the lessons and topics to the exam domains, objectives, and content examples. You can use this as a checklist as you prepare to take the exam, and review any content that you are uncertain about.

As a Reference

The organization and layout of this book make it an easy-to-use resource for future reference. Guidelines can be used during class and as after-class references when you're back on the job and need to refresh your understanding. Taking advantage of the glossary, index, and table of contents, you can use this book as a first source of definitions, background information, and summaries.

Lesson 1

Scoping Organizational/Customer Requirements

LESSON INTRODUCTION

Penetration testing is a proactive exercise that tests the strength of an organization's security defenses. While there are many reasons why an organization might conduct a Penetration Test (PenTest), many times it is to provide due diligence and due care in meeting compliance requirements. Prior to beginning a PenTest exercise, you will need to devise a structured plan and outline the terms. Once you step into an organization to conduct the PenTest, it is essential that you and your team maintain a professional attitude at all times. In addition, if during testing your team discovers possible indications of an ongoing or previous compromise, you must immediately report the details to the appropriate stakeholder.

Lesson Objectives

In this lesson, you will:

- Define organizational Penetration Testing and recognize the CompTIA structured PenTesting process
- Acknowledge compliance requirements such as PCI DSS along with GDPR, that drive the need to assess the security posture
- Compare different standards and methodologies used to outline best practice activities during a PenTesting exercise that include MITRE ATT&CK, OWASP, and NIST
- Describe some best practice methods of ensuring professionalism and maintaining confidentiality before, during, and after testing.

Topic 1A

Define Organizational PenTesting



EXAM OBJECTIVES COVERED

- 1.2 Explain the importance of scoping and organizational/customer requirements.
- 4.3 Explain the importance of communication during the penetration testing process.

The economic impact of cybercrime has grown to trillions of dollars annually. Because of the expanded attack vectors and blurring of boundaries that cross into partner networks, the cloud and supply chains, the impact will continue to rise. Organizations remain vigilant in protecting against cyberattacks; however, significant breaches continue to increase in number and severity.

Even with proactive security mechanisms such as firewalls, intrusion detection/intrusion prevention systems (IDS/IPS), and antimalware protection, a threat may be able to slip by system defenses and find a home on the network. That is why PenTesting is essential in today's environment.

In this section, we'll outline how organizational PenTesting provides a way to evaluate cyberhealth and resiliency with the goal of reducing overall organizational risk. In addition, we'll review the CompTIA structured PenTesting process, which provides uniformity and structure to security testing.

Let's start with outlining the purpose of PenTesting.

Assessing Cyber Health and Resiliency

Companies recognize the potential for an attack in a complex security architecture. As a result, many employ proactive processes and follow best practice procedures to secure their systems. Methods include patch and configuration management of all operating systems and applications, along with providing security education, training, and awareness to all employees to prevent social engineering attacks. Today many controls are utilized, to ensure the confidentiality, integrity, and availability of system resources.

Today many controls are utilized, to ensure the confidentiality, integrity, and availability of system resources. Controls include the following:

- **Administrative controls** are security measures implemented to monitor the adherence to organizational policies and procedures. Those include activities such as hiring and termination policies, employee training along with creating business continuity and incident response plans.
- **Physical controls** restrict, detect and monitor access to specific physical areas or assets. Methods include barriers, tokens, biometrics or other controls such as ensuring the server room doors are properly locked, along with using surveillance cameras and access cards.
- **Technical or logical controls** automate protection to prevent unauthorized access or misuse, and include **Access Control Lists (ACL), and Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)** signatures and antimalware protection that are implemented as a system hardware, software, or firmware solution.

All controls should use the **Principle of Least Privilege**, which states that an object should only be allocated the *minimum* necessary rights, privileges, or information in order to perform its role.

However, even with all of the security controls in place, the only way you will know if the network can withstand a cyber event is by actively simulating attacks. This is achieved by completing a structured PenTest.



It's important to note that a vulnerability scan and PenTest represent two different concepts. A vulnerability scan will scan computer systems, networks and applications for vulnerabilities or system weaknesses. A penetration test will use a vulnerability scan, however, will take the process further by attempting to actively exploit system vulnerabilities. Once complete, the results are documented in a report format and presented to the stakeholders.

As a result, organizations need to continually assess the security measures in place in order to defend against ongoing threats, instead of waiting for a real breach to occur and face the consequences.

PenTesting (also called Ethical Hacking) is an important element of a comprehensive security plan. Testing provides a method to assess internal and external computer systems with the purpose of locating vulnerabilities that can potentially be exploited, so they can be addressed.

One of the primary goals of a PenTest is to reduce overall risk by taking proactive steps to reduce vulnerabilities. Let's explore this concept, next.

Reducing Overall Risk

Risk represents the consequence of a threat exploiting a vulnerability. When dealing with cybersecurity, a risk can result in financial loss, business disruption, or physical harm. The formula for determining risk is as follows:

Determining Risk

$$\text{Risk} = \text{Threat} \times \text{Vulnerability}$$

Formula for determining risk

We can break down this concept by outlining the elements that comprise risk:

- A **threat** represents something such as malware or a natural disaster, that can accidentally or intentionally exploit a vulnerability and cause undesirable results.
- A **vulnerability** is a weakness or flaw, such as a software bug, system flaw, or human error. A vulnerability can be exploited by a threat.

To put this into perspective of how threats and vulnerabilities work together to reflect a risk level, let's complete a risk analysis.

Analyzing Risk

A **risk analysis** is a security process used to assess risk damages that can affect an organization. To illustrate this concept, we'll see how using different levels of antimalware protection on a system will alter the risk:

- One system will be protected using a **free antivirus** with no automatic updates
- One system will be protected using a **paid antivirus** with automatic updates
- One system will be protected using a **unified threat management (UTM)** appliance with automatic updates.

In each case, there is a 100% chance that malware will be a threat. Knowing this let's build our matrix. Within the matrix, I assigned each of the systems a vulnerability rating as to how easily malware will infect the system. Then using the formula $\text{Risk} = \text{Threats} \times \text{Vulnerabilities}$, we'll be able to calculate the level of risk.

Calculating Risk

Scenario	Risk	=	Threat	×	Vulnerability
Free antivirus	90%	=	100%	×	90%
Paid antivirus	40%	=	100%	×	40%
UTM	10%	=	100%	×	10%

Anti-malware protection – Risk Assessment

In this case, the system using the free antivirus was the most vulnerable, and the risk of infection was 90% vulnerable. The system using free antivirus had a 40% risk of being infected. However, the system using UTM was minimally vulnerable, and therefore had a 10% risk rating.

In general, threats to our systems and well-being exist, however, we cannot control the threats. What we can do is minimize or control the vulnerabilities. If we reduce the vulnerabilities, we will reduce overall risk. Therefore, identifying and mitigating vulnerabilities as early as possible will reduce overall risk.

Risk analysis is part of a larger process called **risk management**, which is the cyclical process of identifying, assessing, analyzing, and responding to risks. PenTesting is a key component in managing risk. While an organization has a choice as to how they conduct a PenTesting exercise, one method is to use a structured approach, which provides consistency, as we'll see next.

Recognizing the CompTIA Process

When using a structured approach to PenTesting, each step will serve a purpose with the goal of testing an infrastructure's defenses by identifying and exploiting any known vulnerabilities.



CompTIA structured PenTesting process

Each of the steps relate to CompTIA's PenTest+ Certification exam objectives.



When comparing the steps to exam objectives, you'll note that the Tools and Code Analysis domain is not listed. However, we will cover the tools used during the appropriate stage of the PenTest process.

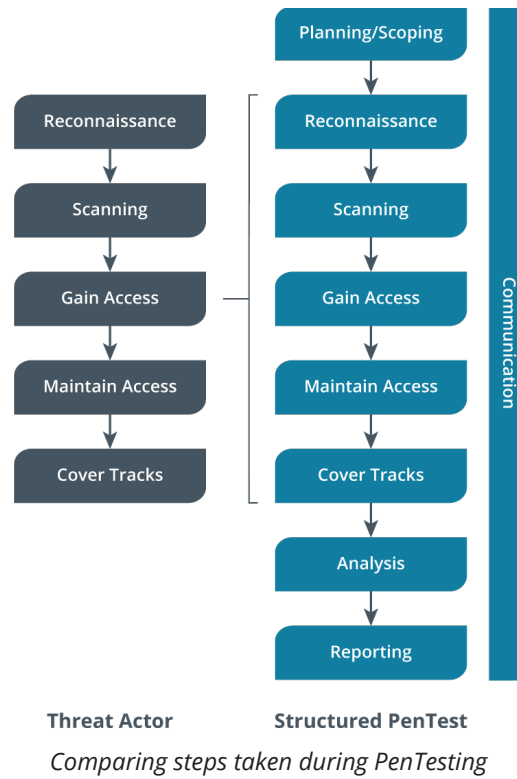
Each of the main steps of the structured PenTesting process is broken down into more detailed steps as follows:

1. **Planning and scoping** is when the team meets with the stakeholders to outline a plan for the PenTest. Some of the information obtained includes the rules of engagement, budget, technical constraints along with the types of assessments, and selection of targets.
2. **Reconnaissance** focuses on gathering as much information about the target as possible. This process includes searching information on the Internet, using Open-Source Information Gathering Tools (OSINT), along with social networking sites and company websites.
3. **Scanning** is a critical phase as it provides more information about available network resources. Scanning identifies live hosts, listening ports, and running services. In addition, the team uses enumeration to gather more detailed information on usernames, network shares, services, and DNS details.
4. **Gaining access** occurs after the team has gathered information on the network. In this phase, the team will attempt to gain access to the system, with the goal of seeing how deep into the network they can travel. Then once in, the team will attempt to access protected resources.
5. **Maintaining access** once the team is in the system the goal is to maintain access undetected for as long as possible
6. **Covering tracks** removes any evidence that the team was in the system, including executable files, rootkits, logs, and any user accounts that were used during the exercise.
7. **Analysis** occurs after the team has completed the exercise, and will go through the results of all activities, analyze the findings, and derive a summary of their risk rating.
8. **Reporting** will deliver the results and any remediation suggestions to the stakeholders, along with a realistic timeline of reducing risk and implementing corrective actions.

Throughout the entire process, the team will constantly communicate with the stakeholders of any irregularities such as an indication of a possible breach.

What's important to note is that the same main process is used by the threat actor, as shown in the graphic:

PenTesting Process



The threat actor has a main goal of altering the integrity of the system and/or causing harm, and are sometimes called an **unauthorized hacker**, which is a hacker operating with malicious intent.

Review Activity:

Organizational PenTesting

Answer the following questions:

- 1. Management has gathered the team leaders at 515support.com and outlined the importance of conducting a PenTesting exercise. Your supervisor has asked the group why PenTesting is important. How would you respond?**
- 2. Management at 515support.com has been working hard at ensuring employees are well trained in identifying a phishing email. Concurrently the IT team has implemented strong spam filters to prevent phishing emails from getting to their employees. What is the RISK of an employees falling victim to a phishing attack using the following information?**
 - 75% = THREAT of a phishing email reaching an employee
 - 40% = VULNERABLE employees that might fall for a phishing attack
- 3. When using a structured approach to PenTesting, each step will serve a purpose with the goal of testing an infrastructure's defenses by identifying and exploiting any known vulnerabilities. List the four main steps of the CompTIA Pen Testing process.**
- 4. Threat actors follow the same main process of hacking as a professional PenTester: Reconnaissance, Scanning, Gain Access, Maintain Access, and Cover Tracks. What steps are added during a structured PenTest?**

Topic 1B

Acknowledge Compliance Requirements



EXAM OBJECTIVES COVERED

1.1 Compare and contrast governance, risk, and compliance reports.

Today's organizations face strong regulatory oversight, which forces us to secure our systems. Penetration testing helps provide a gap analysis to see how close you are to being compliant.

For many organizations, there are several standards and regulations that define security measures that must be taken in order to prevent data loss. Examples include Payment Card Industry Data Security Standard (PCI DSS) and General Data Protection Regulation (GDPR). In this section, we'll discover some of the common elements of compliance requirements, as they relate to data protection, starting with PCI DSS. We'll also review the different types of assessments, such as goal-based, compliance-based, and objective-based, and review the different strategies taken when performing a PenTest.

First, let's see what's involved when a company must adhere to PCI DSS controls.

Outlining PCI DSS

One standard that outlines exact requirements for safely handling data, is **Payment Card Industry Data Security Standard (PCI DSS)**. This specifies the controls that must be in place to securely handle credit card data. Controls include methods to minimize vulnerabilities, employ strong access control, along with consistently testing and monitoring the infrastructure.

Threat actors attempt to obtain credit card information, such as account number and other elements necessary to impersonate the cardholder. The standards exist as a way of dealing with threats to the security of cardholder data, whether online or at a brick-and-mortar store.



PCI DSS documentation is found at: <https://www.pcisecuritystandards.org/pci-security/>. Within the documentation you will find a list of the four main tenets and guidelines

The attack vectors and threats to credit card data can be vast. To address this, PCI DSS standards provide granular details on methods to secure data. Within the framework, there are six categories that describe what is required. The categories list a specific goal, and then define the requirement. To summarize, an organization must do the following in order to protect cardholder data:

- Create and maintain a secure infrastructure by using dedicated appliances and software, that monitor and prevent attacks.
- Employ good practice strategies, such as changing passwords from the vendor default, and training users not to open suspicious emails.

- Continuously monitor for vulnerabilities and employ appropriate anti-malware protection that is continuously updated.
- Provide strong access control methods by using the principle of least privilege, and routinely monitor and test networks.

In addition, the organization must create and maintain appropriate information security policies that define the rules of proper behavior. If a merchant fails to comply and are in violation of the requirements, they can face a substantial fine, and even lose the ability to handle credit card transactions.

PCI DSS compliance relies on a continuous process of assess, remediate, and report. By using the prescribed controls, this ongoing process provides the greatest level of security.

A company must be vigilant and take efforts to secure the data. However, although in a company's best effort, they may not have done enough. The only way to tell if they have achieved the goal of being PCI DSS compliant is by completing an assessment and then reporting the results.

PCI DSS is not a law; therefore, there is no government oversight. However, it's imperative that anyone that deals with cardholder data must comply with the guidelines.

The security level will define whether the merchant must complete a self-assessment or have an external auditor assess whether or not the merchant is compliant. In addition, the level also defines whether they must complete a **Report on Compliance (RoC)**. Therefore, the first step is to identify how many transactions are done on a yearly basis. Once the value is determined; the merchant is then ranked.

The levels are as follows:

- **Level 1** is a large merchant with over six million transactions a year.
- **Level 2** is a merchant with one to six million transactions a year.
- **Level 3** is a merchant with 20,000 to one million transactions a year.
- **Level 4** is a small merchant with under 20,000 transactions a year.

The activity required for each level to prove compliance with the guidelines, is as follows:

Level 1—must have an external auditor perform the assessment by an approved **Qualified Security Assessor (QSA)**.

Levels 1 and 2 must complete a RoC.

Levels 2–4—can either have an external auditor or submit a self-test that proves they are taking active steps to secure the infrastructure.

In addition to PCI DSS, there are several laws in the United States and the European Union (EU) that deal with the protection of consumer data. One such law is GDPR, which has a global reach.

Dissecting GDPR

In 2018 the EU enacted the **General Data Protection Regulation (GDPR)**, which outlines specific requirements on how consumer data is protected. The law affects *anyone* who does business with residents of the EU and Britain. This comprehensive law focuses on the privacy of consumer data and, more importantly, gives consumers the ability to control how their data is handled.

Some of the components of this law include:

- **Require consent** if a company wants to gather information on your searching and buying patterns, it must first obtain permission. A client must be allowed to accept or decline for *each separate data source*, i.e., email addresses for marketing or IP addresses for analytics.
- **Rescind consent**—just as the consumer can give consent for a company to use their information, they can opt out at any time. Known as the *right to be forgotten* rule, this puts control back in the hands of the consumer.
- **Global reach**—the GDPR affects anyone who does business with residents of the EU and Britain. The statute relates to e-commerce, as websites do not have a physical boundary. If you do business with anyone in the EU and Britain, this rule will prevail.
- **Restrict data collection**—organizations should collect only the minimal amount of data that is needed to interact with the site.
- **Violation reporting**—if the company's consumer database is compromised, they must report the breach within 72 hours.

The GDPR clearly outlines that consumer data must be protected. Within the document, found at <https://gdpr.eu/>, you will find a checklist that outlines the requirements for regularly testing the strength of the infrastructure for vulnerabilities, with the goal of preventing a data breach. Any company with over 250 employees will need to audit their systems and take rigorous steps to protect any data that is processed within their systems, either locally managed or in the cloud.

In addition to PCI DSS and GDPR, there are many other laws that govern the protection of data. Let's review a few of these that might impact a PenTest.

Recognizing other Privacy Laws

Some of the laws govern data protection for a location, such as a country, providence or state, or an industry, such as the banking or health care industry. Some examples include:

- The **Stop Hacks and Improve Electronic Data Security (SHIELD)** is a law that was enacted in New York state in March 2020 to protect citizens data. The law requires companies to bolster their cybersecurity defense methods to prevent a data breach and protect consumer data.
- The **California Consumer Privacy Act (CCPA)** was enacted in 2020 and outlines specific guidelines on how to appropriately handle consumer data. To ensure that customer data is adequately protected, vendors should include PenTesting of all web applications, internal systems along with social engineering assessments.
- The **Health Insurance Portability and Accountability Act (HIPAA)** is a law the mandates rigorous requirements for anyone that deals with patient information. Computerized electronic patient records are referred to as **electronic protected health information (e-PHI)**. With HIPAA, the e-PHI of any patient must be protected from exposure, or the organization can face a hefty fine.

While many compliance requirements focus PenTesting on larger companies, smaller companies can benefit from a PenTesting exercise as well. Not only will it ensure compliance, but it will also help to identify vulnerabilities before they can be exploited. The type of assessment along with the approach your team will take will depend on the objectives.

Review Activity:

Compliance Requirements

Answer the following questions:

1. **Part of completing a PenTesting exercise is following the imposed guidelines of various controls, laws, and regulations. Summarize Key takeaways of PCI DSS.**
2. **With PCI DSS a merchant is ranked according to the number of transactions completed in a year. Describe a Level 1 merchant.**
3. **With PCI DSS, a Level 1 merchant must have an external auditor perform the assessment by an approved ____.**
4. **Another regulation that affects data privacy is GDPR, which outlines specific requirements on how consumer data is protected. List two to three components of GDPR.**
5. **What should a company with over 250 employees do to be compliant with the GDPR?**

Topic 1C

Compare Standards and Methodologies



EXAM OBJECTIVES COVERED

- 1.2 Explain the importance of scoping and organizational/customer requirements.
- 2.1 Given a scenario, perform passive reconnaissance.

In addition to the laws that govern the need to protect data, there are also *guidelines* that help security professionals effectively manage and protect their information and infrastructure. In this section, we'll cover organizations that provide guidance and frameworks for PenTesting, such as the National Institute of Standards and Technology (NIST). In addition, we'll also cover *methods* that help outline best practices, such as the Open-Source Security Testing Methodology Manual (OSSTMM) and the Penetration Testing Execution Standard (PTES).

In addition, because one of the key components of PenTesting is identifying vulnerabilities, we'll review the Common Vulnerabilities and Exposures (CVE), along with the Common Weakness Enumeration (CWE).

Let's start with an overview of some of the PenTesting frameworks available today.

Identifying PenTesting Frameworks

In some cases, a PenTesting exercise is required, however, many companies may opt to conduct one voluntarily to ensure that they have properly secured their data. Regardless, a complete assessment will pay off in many ways. The obvious reasons are to discover system weaknesses and answer questions such as:

- Do we have any unnecessary services running?
- Are social engineering techniques effective?
- What are the exploitable vulnerabilities?
- Are antimalware signatures up-to-date?
- Are the operating system patches current?

A company might need some assistance either in getting started in the process, or guidance on how to conduct an effective PenTesting exercise. The good news is that there are plenty of resources available, such as the United States (U.S.) National Institute of Standards and Technology (NIST), and Open Web Application Security Project (OWASP).

Let's discuss some of the resources, starting with OWASP.

Understanding OWASP

The **Open Web Application Security Project (OWASP)** is an organization aimed at increasing awareness of web security and provides a framework for testing during each phase of the software development process. Once on the site, you'll find open-source tools and testing guidelines such as a list of **Top 10** vulnerabilities.

In addition, you'll find the OWASP Testing Guide (OTG). The OTG steps through the testing process and outlines the importance of assessing the whole organization, that includes the people, processes, and technology, with a focus on web applications. You can learn more at www.owasp.org.

Next, let's take a look at NIST, an organization that develops computer security standards used by U.S. federal agencies and publishes cybersecurity best practice guides and research.

Evaluating Resources at NIST

Visit **NIST** at <https://www.nist.gov/>, and you will find a large number of topics in areas such as climate, communication, and cybersecurity. NIST has many resources for the cybersecurity professional that include the Special Publication (SP) 800 series, which deals with cybersecurity policies, procedures, and guidelines.

NIST SP 800-115 is the "Technical Guide to Information Security Testing and Assessment." SP 800-115 was published in 2008, however contains a great deal of relevant information about PenTesting planning, techniques, and related activities.

Another detailed manual on security testing is the **Open-source Security Testing Methodology Manual (OSSTMM)**.

Exploring OSSTMM

It's a well-known fact many of us work well by following a framework. OSSTMM provides a holistic structured approach to PenTesting. Written in 2000, the open-source document stresses auditing, validation, and verification. While OSSTMM doesn't provide the tools needed to accomplish a complete PenTesting exercise, it does cover other areas, such as Human Security and Physical Security testing.

Version 3 (v3) is freely available, however access to the latest version will require a paid membership to The Institute for Security and Open Methodologies (ISECOM). Even still, it's worth exploring the site, as they have other cyber security resources that include:

- **Hacker Highschool**—provides security awareness to teens
- **Cybersecurity Playbook**—outlines cybersecurity best practice for small to medium sized organizations

You can find OSSTMM v3 at <https://www.isecom.org/OSSTMM.3.pdf>.

When preparing your team to begin testing, it's sometimes beneficial to review documentation on established frameworks. In the next section, let's review some of the additional resources that can provide advice and guidance.

Providing Guidance

Over the years, several organizations have invested a great deal of time and resources in developing structured guidelines and best practices to accomplish a PenTesting exercise. In this section, we'll evaluate the Information Systems Security Assessment Framework (ISSAF), the Penetration Testing Execution Standard, along with MITRE ATT&CK.

Let's start with the ISSAF, an open-source resource available to cybersecurity professionals.

Examining ISSAF

If you do a keyword search for ISSAF, you will find a few locations where you can obtain the components of the framework. Once you download and unpack the ISSAFv1, Roshal Archive (rar) Compressed file, you will be able to view the contents, as shown in the screenshot:

ISSAF Documentation



Contents of ISSAF rar file (Screenshot courtesy of Microsoft.)

Once in the folder, you will find a list of 14 documents that relate to PenTesting, such as guidelines on business continuity and disaster recovery along with legal and regulatory compliance. Although the ISSAF was created in 2005, there are plenty of valuable resources related to PenTesting. In addition, there is a knowledge base that includes a Security Assessment Contract, Request for Proposal and Reporting templates.

The Penetration Testing Execution Standard (PTES) was developed by business professionals as a best practice guide to PenTesting.

Describing the PTES

The **Penetration Testing Execution Standard (PTES)** has seven main sections that provide a comprehensive overview of the proper structure of a complete PenTest. Some of the sections include details on topics such as:

- Preengagement interactions
- Threat modeling
- Vulnerability analysis
- Exploitation
- Reporting

The PTES approaches the standard business aspect in that it doesn't have technical guidelines specifically addressed in the document. It does, however, have a separate document that provides technical guidelines, along with a list of tools used in the PenTesting process. For more information, visit: www.pentest-standard.org.

Another powerful site that provides a great deal of research is MITRE ATT&CK, which conducts vulnerability research, and then shares the research with the general public and coordinating agencies.

Utilizing MITRE ATT&CK

MITRE Corporation is a U.S. based non-profit organization that provides research, publications, and tools at no charge for anyone who accesses the site. Research provided by MITRE is sponsored by the U.S. Computer Emergency Readiness Team (US-CERT) and the U.S. Department of Homeland Security (DHS).

One of the tools provided by MITRE Corporation is the **ATT&CK (Adversarial Tactics, Techniques & Common Knowledge)** framework, which provides tools and techniques specific to PenTesting. Once in the framework (found at <https://attack.mitre.org/>), you will see many columns in the matrix that describe some task that is completed during the PenTest. The following are some examples of the column headers you can find while on the site:

Initial Access lists attack vectors a threat actor can use to gain access to your network. This category defines many techniques, such as:

- Drive by compromise
- Supply chain compromise
- External remote services

The **Persistence** category provides details on how to remain in a system. Within this category there are many techniques that include:

- Create account
- Modify authentication process
- Browser extensions

Credential access provides multiple solutions on how to obtain credentials, that include:

- Brute force
- Man in the Middle
- Forced authentication

While the matrix and details provided in each section are valuable, MITRE is also actively involved with providing key information on vulnerabilities and weaknesses within software. Next, let's see what's available in these areas.

Investigating CVE and CWE

Identifying and mitigating vulnerabilities is at the heart of a structured PenTest. As vulnerabilities are identified, they are first rated as to the severity using the **Common Vulnerability Scoring System (CVSS)**. The score is derived using a set of metrics, which helps in prioritizing vulnerabilities. You can learn more by visiting <https://www.first.org/cvss/>.



It's important to note that vulnerability scores will change over time.

The information from the CVSS is then fed into the **Common Vulnerabilities and Exposures (CVE)**.

Recognizing the CVE

The CVE is a listing of all publicly disclosed vulnerabilities. Each entry refers to *specific* vulnerability of a particular product and is cataloged with the following information:

- Name of the vulnerability using the following format: CVE-[YEAR]-[NUMBER].
- Description of the vulnerability, for example: An SQL injection vulnerability exists (with user privileges) in the pets console of Kiddikatz chip records system.

To learn more about the vulnerability, click on the name, which is a hyperlink to the record in the **National Vulnerability Database (NVD)**. Once there, you can read more details about the vulnerability.

Another community-developed database is the **Common Weakness Enumeration (CWE)**.

Detailing Weaknesses with the CWE

The CWE is a database of software-related vulnerabilities maintained by the MITRE Corporation. Once in the site, you will see a detailed list of weaknesses in hardware and software. For example, if we select **Software Development**, this will take us to the **Software Development** page. Once there, you will see a list of common software issues where you can select a topic.

For example, if you select **Data Validation Issues**, that will take you to a new page where you will find more detailed information on the weakness such as affected platforms, and what possible consequences could result as a result of exploiting this weakness.

Review Activity:

Standards and Methodologies

Answer the following questions:

1. **Completing a PenTest can be overwhelming. While doing your research you found some PenTesting frameworks that will help guide the process. Describe how OWASP can help your team.**
2. **Describe some of the resources available at NIST.**
3. **Discuss the significance of NIST SP 800-115.**
4. **Explain how the MITRE ATT&CK Framework provides tools and techniques specific to PenTesting.**
5. **Compare and contrast CVE and CWE.**

Topic 1D

Describe Ways to Maintain Professionalism



EXAM OBJECTIVES COVERED

1.3 Given a scenario, demonstrate an ethical hacking mindset by maintaining professionalism and integrity.

Prior to assembling the PenTesting team, the ground rules are laid out so that everyone understands the need to provide rigorous controls, prior to, during, and after the PenTest exercise. To reassure the client, the team may be asked to provide credentials and evidence that the team has an excellent reputation for respecting the safety of the customers' personal data. Other related activities can include presenting background checks and credentials of the team members. In addition, prior to beginning the PenTest, the team should receive training on how to identify criminal behavior along with the procedure for reporting breaches or evidence of criminal activity.

Let's start with providing background checks of the team members.

Background Checks of the Team

When entering into a discussion on conducting PenTesting for an organization, the team will most likely be asked several questions. The questions will help assure the organization that they have the appropriate experience and an excellent reputation. Aside from experience, there are more considerations. Each member of a PenTesting team needs to provide credentials that prove they can work in a secure environment. Some of the considerations include:

- Provide credentials, such as certifications that prove they have the appropriate skills to conduct PenTesting.
- Produce recent background checks, that can include credit scores and driving records. Make sure no one has a criminal record or felony conviction.

Even if someone has a Top Secret clearance from the military, you'll want to provide recent information to reassure the client.

Identify and Report Criminal Activity

The penetration test is a simulated attack, in that systems will face the same scrutiny that would be evident during a real attack by a threat actor. While PenTesting, many times it's an advantage to think like a criminal. However, it's also important to be able to identify and report any criminal activity, even if the activity occurred by accident. For example, if someone were to inadvertently scan the wrong network, this action must be immediately reported to the team leader, as there could be legal ramifications.

Another consideration when PenTesting is the need to ensure privacy of any information obtained during the PenTest process.

Maintaining Confidentiality

Throughout the course of the PenTest process, the team may expose sensitive information or discover system vulnerabilities. As a result, everyone on the PenTest team must agree to conform to the policy on handling proprietary and sensitive information.

For example, if a team member finds a major vulnerability in the company's public-facing website, the organization may require them to keep this information confidential to minimize risk. The requirements might also set restrictions that state only privileged personnel, such as IT managers only, and not standard employees, should be informed of any issues.

During the planning meeting, the team should explicitly state that the testers will protect information they discover during testing, and not disclose confidential information to any other parties. In some cases, the team may need to supply legal documentation that includes confidentiality provisions. In addition, because of the sensitive nature of the PenTest reports, they should be protected by using encryption, and password protected when in storage.

Along with ensuring confidentiality, the team must be aware of any legal issues that might impact the testing process.

Avoiding Prosecution

Formalized PenTesting goes through a process of assessing the cyberhealth and resiliency of an organization. However, prior to beginning any testing, the team should carefully outline the terms of the contract and be aware of all possible legal considerations that might be applicable.

The team must keep in mind there can be risks to the professional, by inadvertently performing an illegal activity.

If any member of the team is apprehended and found guilty of an illegal act, they can face serious consequences. Let's see just what's at stake.

Facing Fees, Fines, and Criminal Charges

Before doing any active testing, the team will gather with the stakeholders and outline the terms of the PenTesting process. In addition to agreeing on the terms of the test, the team will carefully consider the scope and methods to be used while testing.

It's important to carefully think through all scenarios. Using a tabletop exercise, have the team step through how they will complete the testing, along with possible conflicts that might occur. For example, if the organization requests that the team attempt to break into a facility to expose possible physical vulnerabilities, they should ask appropriate questions:

- Who will notify the authorities and/or security personnel that the team will actively try to break into a facility?
- If the team is to attempt to circumvent security measures "through various means" make sure the organization defines "various means," so there is no confusion.

Even though a PenTest is performed with the mutual consent of the customer, the team may inadvertently violate a local, state, or regional law. This could result in criminal charges, along with significant fines.

Prior to testing, the team should carefully question the stakeholders as to any possible legal ramifications. In addition, the team should independently research any regulations that will prevent certain types of testing.

Review Activity:

Professionalism

Answer the following questions:

- 1. A couple of your colleagues thought it might be a good idea to share some guidance on how the team should conduct themselves during the PenTesting process. What topics should be covered so that all members exhibit professional behavior before, during and after the PenTest?**
- 2. The team is involved with planning a PenTest exercise for 515support.com. Management is concerned that the loading dock is vulnerable to a social engineering attack, whereby someone can gain access to the building by asking someone who is on a smoking break. Prior to conducting the tests, what should the team do to prepare for the test.**
- 3. The team is involved with planning a PenTest exercise for 515support.com. Management has asked the team to run a series of scans at a satellite facility. Once the team is on site and begins testing, one of the team members shows you the result of the vulnerability scan. After examining the scan, you realized the team member has scanned the wrong network. How should you proceed?**

Lesson 1

Summary

In this lesson we defined organizational Penetration Testing and recognize the CompTIA structured PenTesting process. We learned how although a malicious actor follows the same steps to perform unauthorized hacking, the team will add analysis and reporting during the PenTesting exercise.

We then reviewed compliance requirements such as PCI DSS along with GDPR, that drive the need to assess the security posture. We compared different standards and methodologies used to outline best practice activities during a Penetration Testing exercise that include MITRE ATT&CK, OWASP and NIST. We then finished with some best practice methods of ensuring professionalism and maintaining confidentiality before, during and after testing.