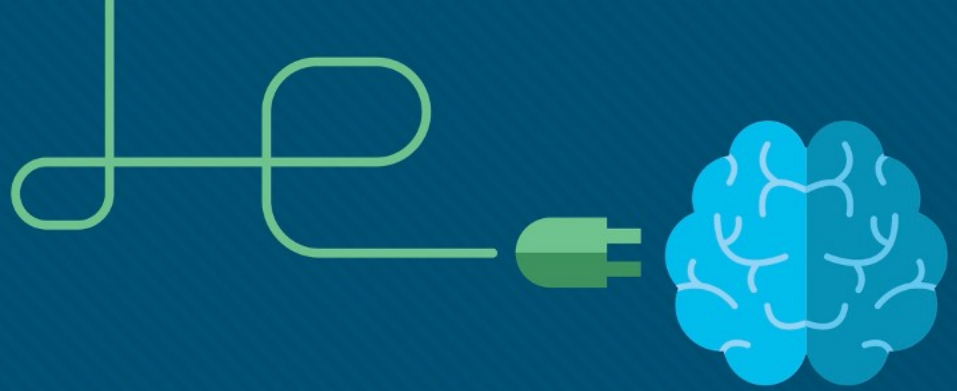


Module 1: Introduction to Ethical Hacking and Penetration Testing

Ethical Hacker

Module Objectives

Module Title: Introduction to Ethical Hacking and Penetration Testing

Module Objective: Explain the importance of methodological ethical hacking and penetration testing.

Topic Title	Topic Objective
Understanding Ethical Hacking and Penetration Testing	Explain the importance of ethical hacking and penetration testing.
Exploring Penetration Testing Methodologies	Explain different types of penetration testing methodologies and frameworks.
Building Your Own Lab	Configure a virtual machine for your penetration testing learning experience.

1.1 Understanding Ethical Hacking and Penetration Testing

Overview

- ***Ethical hacker***: a person who acts as an attacker and evaluates the security posture of a network's or system's infrastructure to identify and possibly exploit any security weaknesses found and then determine if a compromise is possible.
- This process is called *security* ***penetration testing*** or *ethical hacking*.
- The key factor in defining ethical versus nonethical hacking is that the latter involves malicious intent.
- The permission to attack is often referred to as "the scope" of the test (what you are allowed and not allowed to test) and it is crucial for getting you out of trouble!
- A security researcher looking for vulnerabilities in products, applications, or web services is considered an ethical hacker if he or she responsibly discloses those vulnerabilities to the vendors or owners of the targeted research.
- The same type of "research" performed by someone who then uses the same ***vulnerability*** to gain unauthorized access to a target network/system would be considered a nonethical hacker.
- Someone who finds a vulnerability and discloses it publicly without working with a vendor is considered a nonethical hacker.
- An ethical hacker uses the same tools to find vulnerabilities and exploit targets as do nonethical hackers.
- An ethical hacker typically reports the findings to the vendor or customer he/she is helping to make the network more secure, trying to avoid performing any tests or exploits that might be destructive in nature.

Why Do We Need to Do Penetration Testing?

- Someone who is responsible for securing and defending a network/system wants to find any possible paths of compromise before the bad guys do.
- Over the years, many different defensive techniques such as antivirus, firewalls, intrusion prevention systems [IPSs], and anti-malware have been developed and implemented.
- How do we know if those defenses really work and whether they are enough to keep out the bad guys?
- How valuable is the data that we are protecting, and are we protecting the right things?
- These are some of the questions that should be answered by a penetration test.
- We need to determine what it is we are protecting and whether our defenses can hold up to the threats that are imposed on them.
- Simply implementing a firewall, an IPS, anti-malware, a VPN, a web application firewall (WAF), and other modern security defenses isn't enough.
- You also need to test their validity.
- And you need to do this on a regular basis because networks and systems change constantly.
- The attack surface can change as well, and when it does, you need to consider reevaluating the security posture by way of a penetration test.

Lab - Researching PenTesting Careers

In this lab, you will complete the following objectives:

- Conduct a Penetration Tester Job Search
- Analyze Penetration Tester Job Requirements
- Discover Resources to Further Your Career

Threat Actors

The following are the most common types of **threat actors** (malicious attackers) we see today:

Types of malicious attackers	Description
Organized Crime	Organized crime goes where the money is. It consists of very well-funded and motivated groups that will typically use any and all of the latest attack techniques. Whether that is ransomware or data theft, if it can be monetized, organized crime will use it.
Hacktivists	Hacktivists are not motivated by money. They are looking to make a point or to further their beliefs, using cybercrime as their method of attack. These types of attacks are often carried out by stealing sensitive data and then revealing it to the public for the purpose of embarrassing or financially affecting a target.
State-Sponsored Attackers	Cyber war and cyber espionage are two terms that fit into this category. Many governments around the world today use cyberattacks to steal information from their opponents and cause disruption.
Insider Threats	Insider threats come from inside an organization. They are often normal employees who are tricked into divulging sensitive information or mistakenly clicking on links that allow attackers to gain access to their computers. However, they could also be malicious insiders who are possibly motivated by revenge or money.

1.2 Exploring Penetration Testing Methodologies

Overview

- There is more to penetration testing than hacking away at a customer's network.
- A haphazard approach will result in haphazard results.
- It is important to follow well-known methods and standards to approach pentesting engagements in an organized, systematic way.
- You should understand the major documented methodologies and standards so that you can create strategies that draw on their strengths.
- Documenting your approach with the methodologies and standards that you used also provides accountability for our company and helps make our results defensible in case issues arise with our customers.
- The process of completing a penetration test varies based on many factors.
- The tools and techniques used to assess the security posture of a network or system also vary.
- The networks and systems being evaluated are often highly complex.
- Because of this, it is very easy when performing a penetration test to go off scope.
- This is where testing methodologies come in.

Why Do We Need to Follow a Methodology for Penetration Testing?

- As just mentioned, scope creep is one reason for utilizing a specific methodology; however, there are many other reasons.
- For instance, when performing a penetration test for a customer, you must show that the methods you plan to use for testing are tried and true.
- By utilizing a known methodology, you are able to provide documentation of a specialized procedure that has been used by many people.

Environmental Considerations

- Several different types of penetration tests are often combined in the overall scope of a penetration test, but they can also be performed as individual tests as well.
- A list of some of the most common environmental considerations for the types of penetration tests today are:

Environmental Considerations	Description
Network Infrastructure Tests	These tests can mean a few things. This course is focused on evaluating the security posture of the actual network infrastructure and how it is able to help defend against attacks. This often includes the switches, routers, firewalls, and supporting resources, such as AAA servers and IPSs. A penetration test on wireless infrastructure may sometimes be included in the scope of a network infrastructure test.
Application-Based Tests	It focuses on testing for security weaknesses in enterprise applications. These weaknesses can include but are not limited to misconfigurations, input validation issues, injection issues, and logic flaws. Because a web application is typically built on a web server with a back-end database, the testing scope normally includes the database as well. However, it focuses on gaining access to that supporting database through the web application compromise.
Penetration Testing in the Cloud	The responsibility for cloud security depends on the type of cloud model (SaaS, PaaS, or IaaS). Regardless of the model used, cloud security is the responsibility of both the client and the cloud provider. These details need to be worked out before a cloud computing contract is signed. These contracts vary depending on the security requirements of the client. Considerations include disaster recovery, SLAs, data integrity, and encryption.

Environmental Considerations (Cont.)

- Many penetration testers find the physical aspect of testing to be the most fun because they are essentially being paid to break into the facility of a target.
- This type of test can help expose any weaknesses in the physical perimeter as well as any security mechanisms that are in place, such as guards, gates, and fencing.
- The result should be an assessment of the external physical security controls.
- Most of the compromises today start with some kind of social engineering attack, such as a phone call, an email, a website, an SMS message, and so on.
- It is important to test how your employees handle these types of situations.
- This type of test is often omitted from the scope of a penetration testing engagement mainly because it primarily involves testing people instead of the technology.
- In most cases, management does not agree with this type of approach, but it is important to get a real-world view of the latest attack methods.
- The result of a social engineering test should be to assess the security awareness program so that you can enhance it.
- It should not be to identify individuals who fail the test.
- A great tool for performing social engineering testing campaigns is Social-Engineer Toolkit (SET), created by Dave Kennedy.

Environmental Considerations (Cont.)

The terms below are used to describe the perspective from which the testing is performed:

Penetration Testing Method	Description
Unknown-Environment Test (previously known as *black-box*)	The tester is typically provided only a very limited amount of information. For instance, the tester may be provided only the domain names and IP addresses that are in scope for a particular target. The idea of this type of limitation is to have the tester start out with the perspective that an external attacker might have. Typically, an attacker would first determine a target and then begin to gather information about the target, using public information, and gain more and more information to use in attacks. The tester would not have prior knowledge of the target's organization and infrastructure.
Known-Environment Test (previously known as *white-box*)	The tester starts out with a significant amount of information about the organization and its infrastructure. The tester would normally be provided things like network diagrams, IP addresses, configurations, and a set of user credentials. If the scope includes an application assessment, the tester might also be provided the source code of the target application. The idea of this type of test is to identify as many security holes as possible.
Partially Known Environment Test (previously known as *gray-box*)	It is somewhat of a hybrid approach between unknown- and known-environment tests. With partially known environment testing, the testers may be provided credentials but not full documentation of the network infrastructure. This would allow the testers to still provide results of their testing from the perspective of an external attacker's point of view.

Surveying Different Standards and Methodologies

- There are several penetration testing methodologies that have been around for a while and continue to be updated as new threats emerge.
- The following is a list of some of the most common penetration testing methodologies and other standards:

MITRE ATT&CK	An amazing resource for learning about an adversary's tactics, techniques, and procedures (TTPs). Both offensive security professionals (penetration testers, red teamers, bug hunters, and so on) and incident responders and threat hunting teams use this framework today. It is a collection of different matrices of tactics, techniques, and subtechniques. These matrices–including the Enterprise ATT&CK Matrix, Network, Cloud, ICS, and Mobile–list the tactics and techniques that adversaries use while preparing for an attack, including gathering of information (open-source intelligence [OSINT], technical and people weakness identification, and more) as well as different exploitation and post-exploitation techniques.
OWASP Web Security Testing Guide (WSTG)	A comprehensive guide focused on web application testing. It is a compilation of many years of work by OWASP members. It covers the high-level phases of web application security testing and digs deeper into the testing methods used. For instance, it goes as far as providing attack vectors for testing cross-site scripting (XSS), XML external entity (XXE) attacks, cross-site request forgery (CSRF), and SQL injection attacks; as well as how to prevent and mitigate these attacks. It is the most detailed and comprehensive guide available.
NIST SP 800-115	A document created by the National Institute of Standards and Technology (NIST), which is part of the U.S. Department of Commerce. It provides organizations with guidelines on planning and conducting information security testing. It superseded the previous standard document, SP 800-42. It is considered an industry standard for penetration testing guidance and is called out in many other industry standards and documents.

Surveying Different Standards and Methodologies (Cont.)

OSSTMM	The Open Source Security Testing Methodology Manual (OSSTMM) has been around a long time. Distributed by the Institute for Security and Open Methodologies (ISECOM), it is a document that lays out repeatable and consistent security testing. It is currently in version 3, and version 4 is in draft status. The OSSTMM has the following key sections: Operational Security Metrics, Trust Analysis, Work Flow, Human Security Testing, Physical Security Testing, Wireless Security Testing, Telecommunications Security Testing, Data Networks Security Testing, Compliance Regulations, and Reporting with the Security Test Audit Report (STAR).
PTES	The Penetration Testing Execution Standard (PTES) provides information about types of attacks and methods, and it provides information on the latest tools available to accomplish the testing methods outlined. PTES involves seven distinct phases: Pre-engagement interactions, Intelligence gathering, Threat modeling, Vulnerability analysis, Exploitation, Post-exploitation, and Reporting.
ISSAF	The Information Systems Security Assessment Framework (ISSAF) is another penetration testing methodology like the others on this list with some additional phases. It covers the following phases: Information gathering, Network mapping, Vulnerability identification, Penetration, Gaining access and privilege escalation, Enumerating further, Compromising remote users/sites, Maintaining access, and Covering the tracks.

Lab – Compare PenTesting Methodologies

In this lab you will complete the following objectives:

- Compare Various Pentesting Methodologies
- Conduct Research on Popular Pentesting Methodologies

1.3 Building Your Own Lab

Overview

- It is important that you develop your skills.
- Skills come with practice, but how can you practice if you don't have something to practice on?
- It is not possible for you to practice on clients' networks and applications.
- You can practice on simulated targets, networks that you have permission to access, and certain sites on the open internet.
- Remember! Some tools and techniques that are used in ethical hacking can be seen as illegal.
- What's more, the definition of what is legal or illegal can differ from place to place.
- Before you use ethical hacking tools on any network or application, carefully consider the legality of what you are planning to do.
- When in doubt, research the law and ask others for advice.
- In this topic, you will install and explore a Kali Linux virtual machine (VM) that is full of popular ethical hacking tools.
- The VM also includes simulated internal IP networks that include a variety of intentionally vulnerable systems.

Overview (Cont.)

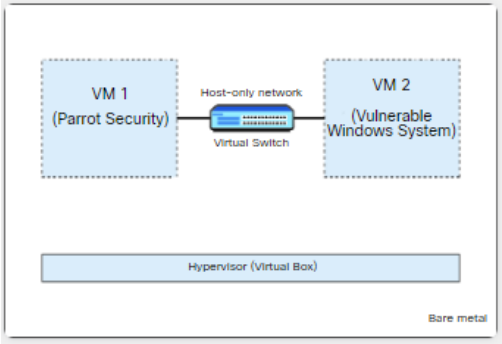
- When it comes to penetration testing, a proper lab environment is very important.
- The way this environment looks depends on the type of testing you are doing.
- The types of tools used in a lab also vary based on different factors.
- Whether you are performing penetration testing on a customer network, your own network, or a specific device, you always need some kind of lab environment to use for testing.
- For example, when testing a customer network, you will most likely be doing most of your testing against the customer's production or staging environments because these are the environments a customer is typically concerned about securing properly.
- Because this might be a critical network environment, you must be sure that your tools are tried and true – and this is where your lab testing environment comes in.

Overview (Cont.)

- You should always test your tools and techniques in your lab environment before running them against a customer network.
- There is no guarantee that the tools you use will not break something.
- In fact, many tools are designed for breaking things.
- You therefore need to know what to expect before unleashing tools on a customer network.
- When testing a specific device or solution that is only in a lab environment, there is less concern about breaking things.
- With this type of testing, you would typically use a closed network that can easily be reverted if needed.

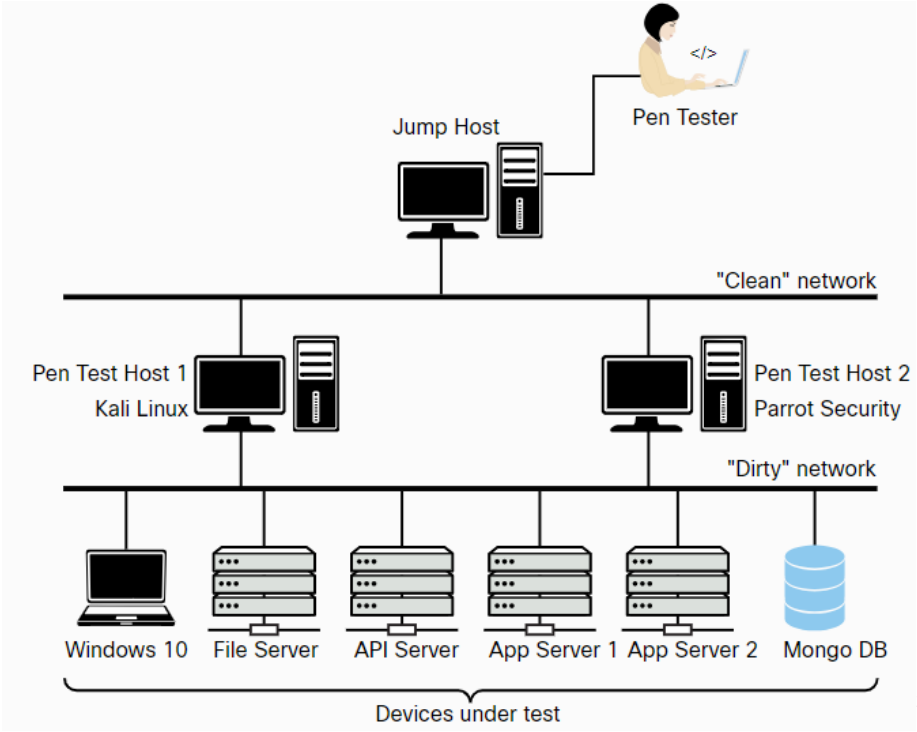
Overview (Cont.)

- There are many different Linux distributions that include penetration testing tools and resources, such as Kali Linux (kali.org), Parrot OS (parrotsec.org), and BlackArch (blackarch.org).
- These Linux distributions provide you with a very convenient environment to start learning about the different security tools and methodologies used in pen testing.
- You can deploy a basic penetration testing lab using just a couple of VMs in virtualization environments such as Virtual Box (virtualbox.org) or VMware Workstation/Fusion (vmware.com).
- Figure shows two VMs (one running Parrot OS and another running a vulnerable Microsoft Windows system).
  - The two VMs are connected via a virtual switch configuration and a “host-only network.”
  - This type of setup allows you to perform different attacks and send IP packets between VMs without those packets leaving the physical (bare-metal) system.



Overview (Cont.)

- Figure 1-2 shows a more elaborate topology for a penetration testing lab environment.



Requirements and Guidelines for Penetration Testing Labs

The following table contains a list of requirements and guidelines for a typical penetration testing environment.

Requirement or Guideline	Description
Closed Network	You need to ensure controlled access to and from the lab environment and restricted access to the Internet.
Virtualized computing environment	This allows for easy deployment and recovery of devices being tested.
Realistic environment	If you are staging a testing environment, it should match the real environment as closely as possible.
Health monitoring	When something crashes, you need to be able to determine why it happened.
Sufficient hardware resources	You need to be sure that a lack of resources is not the cause of false results.
Multiple operating systems	Many times you will want to test or validate a finding from another system. It is always good to test from different operating systems to see if the results differ.
Duplicate tools	A great way to validate a finding is to run the same test with a different tool to see if the results are the same.
Practice targets	You need to practice using your tools. To do this, you need to practice on targets that are known to be vulnerable.

What Tools Should You Use in Your Lab?

- Basically, the tools you use in penetration testing depend on the type of testing you are doing.
- If you are doing testing on a customer environment, you will likely be evaluating various attack surfaces – such as network infrastructure, wireless infrastructure, web servers, database servers, Windows systems, or Linux systems, for example.
- Network infrastructure-based tools might include tools for sniffing or manipulating traffic, flooding network devices, and bypassing firewalls and IPSs.
- For wireless testing purposes, you might use tools for cracking wireless encryption, de-authorizing network devices, and performing on-path attacks (also called man-in-the-middle attacks).
- When testing web applications and services, you can find several automated tools built specifically for scanning and detecting web vulnerabilities, as well as manual testing tools such as interception proxies.

What Tools Should You Use in Your Lab? (Cont.)

- Some of these same tools can be used to test for database vulnerabilities (such as SQL injection vulnerabilities).
- For testing the server and client platforms in an environment, you can use several automated ***vulnerability scanning*** tools to identify things such as outdated software and misconfigurations.
- With a lot of development targeting mobile platforms, there is an increasing need for testing these applications and the servers that support them.
- For such testing, you need another set of tools specific to testing mobile applications and the back-end APIs that they typically communicate with.
- And you should not forget about fuzzing tools, which are normally used for testing the robustness of protocols.

What If You Break Something?

- Being able to recover your lab environment is important for many reasons.
- When doing penetration testing, you will break things, and sometimes they do not recover on their own.
- For instance, when you are testing web applications, some of the attacks you send will input bogus data into form fields, and that data will likely end up in the database, so your database will be filled with that bogus data.
- Obviously, in a production environment, this is not a good thing.
- The data being input can also be of malicious nature, such as scripting and injection attacks.
- This can cause corruption of the database as well.
- It is also an issue in a lab environment if you do not have an easy way to recover.

What If You Break Something? (Cont.)

- Without a quick recovery method, you would likely be stuck rebuilding your system under test.
- This can be time-consuming, and if you are doing this for a customer, it can affect your overall timeline.
- Using some kind of virtual environment is ideal as it offers snapshot and restore features for the system state.
- Sometimes this is not possible, though.
- For example, you may be testing a system that cannot be virtualized.
- In such a case, having a full backup of the system or environment is required.
- This way, you can quickly be back up and testing if something gets broken – because it most likely will.
- After all, you are doing penetration testing.

Lab - Deploy a Pre-Built Kali Linux Virtual Machine (VM)

In this lab, you will complete the following objectives:

- Part 1: Deploying a Customized Kali Linux VM on AMD or Intel Chip-based Computer
- Part 2: Deploying a Customized Kali Linux VM on ARM M1/M2 based MacOS Computer
- Part 3: Exploring Linux

Lab - Investigate Kali Linux

In this lab, you will complete the following objectives:

- Familiarize yourself with the Kali Linux GUI.
- Familiarize yourself with the Kali Linux shell.

1.4 Introduction to Ethical Hacking and Penetration Testing Summary

What Did I Learn in this Module?

- Ethical hacker is someone who uses the same tools as nonethical hackers to find vulnerabilities in a network's or system's infrastructure but reports their findings to the vendor or customer to help make the system more secure.
- The purpose of penetration testing is to identify possible paths of compromise before malicious attackers do.
- It is important to evaluate and test the effectiveness of defensive techniques used to secure and defend networks and systems, and this is where penetration testing comes in.
- Some types of threat actors are organized crime, hacktivists, state-sponsored attackers, and insider threats.
- It is important to use a methodology for penetration testing to avoid scope creep and to provide documentation of a specialized procedure that has been used successfully by many organizations to test their network and data infrastructures.
- Some types of penetration tests are network infrastructure tests, application-based tests, and penetration testing in the cloud.
- Some perspectives from which testing is performed are unknown-environment testing, known-environment testing, and partially known environment testing.

What Did I Learn in this Module? (Cont.)

- Some penetration testing methodologies are MITRE ATT&CK, OWASP WSTG, NIST SP 800-115, OSSTMM, PTES, and ISSAF.
- It is important to have a proper lab environment for penetration testing and know how to use different types of tools in the testing process.
- It is needed to test tools and techniques in a lab environment before running them against a customer network to avoid breaking anything.
- Requirements for a typical penetration testing lab includes closed network, virtualized computing environment, realistic environment, health monitoring, sufficient hardware resources, multiple operating systems, duplicate tools, and practice targets.
- The types of tools used in penetration testing depend on the type of testing being done, such as network infrastructure-based tools, web application testing tools, automated vulnerability scanning tools, and mobile application testing tools.
- It is important to have a recovery method in case something breaks during testing.

Reflection Questions

- Why do organizations need to hire ethical hackers?
- Why is it important to follow a well-documented methodology when doing an penetration test?
- What is the value of having an ethical hacking lab, and what are the requirements for setting one up?