Planning and Scoping Penetration Testing Assessment

Threat Actors

- Organisation Crime
- Hacktivists
- State sponsored Attackers
- Inside Threats

SET (Social Engineer Toolkit)

Bug Bounty programs

- **Used to finding vulnerabilities in the systems of the company.**

Environmental Considerations

- **Network infrastructure Test**
- **Application Based Test**
- **Cloud**

- **Unknown-Environment Test (Black Box)**
- **Known-Environment Test (White-Box)**
- **Partially Known Environment Test**

Standards and Methodologies

- **MITRE ATT&CK framework** (**https://attack.mitre.org**)
  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)

- **OWASP WSTG**
  (**https://owasp.org/www-project-web-security-testing-guide/**)
  OWASP WSTG 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.

- **NIST SP 800-115**
  (***https://csrc.nist.gov/publications/detail/sp/800-115/final***.)
  The **N**ational **I**nstitute of **S**tandards and **T**echnology provides organizations with guidelines on planning and conducting information security testing. It superseded the previous standard document, SP 800-42. SP 800-115 is considered an industry standard for penetration testing guidance and is called out in many other **industry standards and documents.**

- **OSSTMM** (***https://www.isecom.org***).
  The **O**pen **S**ource **S**ecurity **T**esting **M**ethodology **M**anual (OSSTMM), developed by Pete Herzog, has been around a long time. Distributed by the Institute for Security and Open Methodologies (ISECOM)

    - 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
    - Reporting with the Security Test Audit Report (STAR)

- **PTES** (***http://www.pentest-standard.org***)
  The **P**enetration **T**esting **E**xecution **S**tandard 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
    - Reporting

- **ISSAF** (***http://www.pentest-standard.org***)
  The Information Systems Security Assessment Framework (ISSAF) is another penetration testing methodology similar to the others on this list with some additional phases. ISSAF covers the following phases:

  - Information gathering
  - Network mapping
  - Vulnerability identification
  - Penetration
  - Gaining access and privilege escalation
  - Enumerating further
  - Compromising remote users/sites
  - Maintaining access
  - Covering the tracks

BlackArch

is a Linux distribution that includes a large collection of penetration testing tools and resources. It's designed for security researchers and penetration testers and is built on top of Arch Linux.

More information about WebSploit Labs at **websploit.org**.

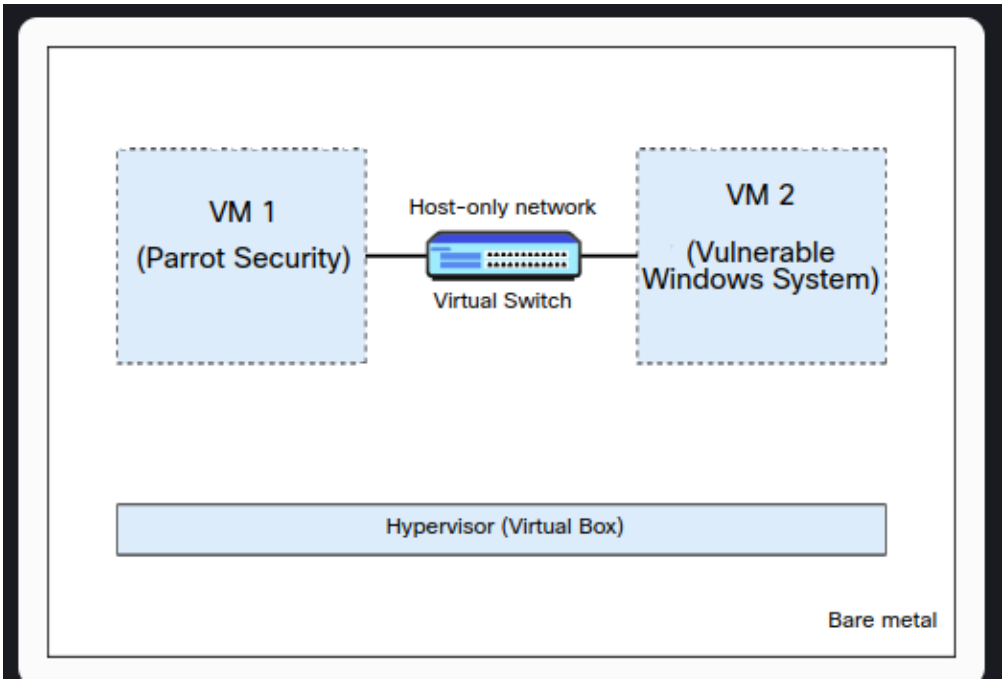


Figure 1-1 - Basic Penetration Testing Lab Environment with Two VMs

Requirements and Guidelines for Penetration Testing Labs

Requirement or Guideline	Description
Closed network	Ensure controlled access to and from the lab environment and restricted access to the internet.
Virtualized computing environment	Leverage virtual machines to simulate a variety of operating systems, networks, and applications. This allows for scalable, flexible, and isolated testing scenarios within a controlled and safe environment.

What Tools Should You Use in Your Lab?

You can access the repository at https://h4cker.org/github. You can directly access the section “Building Your Own Cybersecurity Lab and Cyber Range” at https://github.com/The-Art-of-Hacking/h4cker/tree/master/build_your_own_lab .

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

Required Resources :

- Computer with a minimum of 4 GB of RAM and 50 GB of free disk space.

Download and install VirtualBox and Kali-Lunix :

- https://www.virtualbox.org/
- https://www.kali.org/

Network infrastructure penetration test

A network infrastructure penetration test evaluates various components of an organization's network to identify vulnerabilities, weaknesses, and potential points of unauthorized access or other security issues.

AAA Servers

AAA stands for **Authentication, Authorization, and Accounting**. These servers are crucial for managing user access within networks and systems.

- **Authentication** verifies the user's identity (e.g., through passwords, biometrics).
- **Authorization** determines what an authenticated user is allowed to do (e.g., which resources they can access).
- **Accounting** keeps track of user activities, providing logs that can be analyzed for security audits, billing, and other purposes.

AAA servers are foundational to enforcing security policies and ensuring that only legitimate users can access certain resources and that their activities are monitored.

CSPs

CSPs, or **Cloud Service Providers**, offer a range of services over the internet, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). These services allow businesses and individuals to utilize computing resources, platforms for development, or software applications without needing to invest heavily in physical hardware or manage complex software setups on-premises. Examples include Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

Web Servers

A **web server** is a server that hosts websites and delivers web pages to users' browsers upon request. It processes incoming network requests over HTTP and several other related protocols. Web servers are critical for the functionality of the internet, serving not just static content (e.g., HTML pages, images) but also dynamic content by executing web application code (e.g., PHP, JavaScript) to generate and serve web pages on the fly.

IPSs

IPSs, or **Intrusion Prevention Systems**, are security appliances or software applications that monitor network or system activities for malicious activities or policy violations. An IPS is an enhancement of an Intrusion Detection System (IDS) as it not only detects attacks but also attempts to prevent them by blocking or stopping the attack in real-time. IPSs can be based on various detection methods, including signature-based, anomaly-based, and policy-based detection.

Back-end Databases

Back-end databases store data and serve as the backbone for data storage and retrieval in many applications, from websites to business applications. They are managed by Database Management Systems (DBMS) like MySQL, PostgreSQL, Microsoft SQL Server, and Oracle. Back-end databases are essential for storing, organizing, and managing data efficiently, supporting everything from user account information to large-scale data analytics. They allow for data to be securely stored and retrieved by applications, ensuring data integrity, security, and availability.

Learning environment about pen testing tools and methodologies?

parrotsec.org. Parrot Security OS (ParrotSec) is a Linux distribution designed for security experts, developers, and privacy-aware users. It includes a vast collection of tools for

penetration testing, security research, computer forensics, and privacy/anonymity. It provides a convenient learning environment for those interested in exploring pen testing tools and methodologies.

Planning and Scoping a Penetration Testing Assessment

Create penetration testing preliminary documents.

Topic Title	Topic Objective
Comparing and Contrasting Governance, Risk, and Compliance Concepts	Explain how governance, risk, compliance and environmental factors in planning penetration testing.
Explaining the importance of Scoping and Organizational or Customer Requirements	Create a penetration test scope and plan document that addresses organizational requirements for penetration testing services.
Demonstrating an Ethical Hacking Mindset by Maintaining Professionalism and Integrity	Create your personal code of conduct to provide professionalism and integrity in your ethical hacking practice.

Comparing and Contrasting Governance, Risk, and Compliance Concepts

One of the most important phases (if not the most important) of any penetration testing engagement is the planning and preparation phase. During this phase, you clearly scope your engagement. If you do not scope correctly, you will definitely run into issues with your client (if you work as a consultant) or with your boss (if you are part of a corporate red team), and you might even encounter legal problems.

NOTE A red team is a group of cybersecurity experts and penetration testers hired by an organization to mimic a real threat actor by exposing vulnerabilities and risks regarding technology, people, and physical security. A blue team is a corporate security team that defends the organization against cybersecurity threats (that is, the security operation center analysts, computer security incident response teams [CSIRTs], information security [InfoSec] teams, and others).

Some key concepts you must address and understand in the planning and preparation phase:

- The target audience
- The rules of engagement
- The communication escalation path and communication channels

- The available resources and requirements
- The overall budget for the engagement
- Any specific disclaimers
- Any technical constraints
- The resources available to you as a penetration tester

Regulatory Compliance Considerations:

Make sure the organization is compliant with specific regulations, such as the following.

PCI DSS

The **P**ayment **C**ard **I**ndustry **D**ata **S**ecurity **S**tandard (**PCI DSS**) regulation aims to secure the processing of credit card payments and other types of digital payments. **PCI DSS** specifications, documentation, and resources can be accessed at *https://www.pcisecuritystandards.org*.

HIPAA

The original intent of the **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct of 1996 (**HIPAA**) regulation was to simplify and standardize healthcare administrative processes. Administrative simplification called for the transition from paper records and transactions to electronic records and transactions. The U.S.

Department of Health and Human Services (HHS) was instructed to develop and publish standards to protect an individual's electronic health information while permitting appropriate access and use of that information by healthcare providers and other entities. Information about HIPAA can be obtained from *https://www.cdc.gov/phlp/publications/topic/hipaa.html.*

FedRAMP

The U.S. federal government uses the **F**ederal **R**isk and **A**uthorization **M**anagement **P**rogram (**FedRAMP**) standard to authorize the **use of cloud service** offerings. You can obtain information about FedRAMP at *https://www.fedramp.gov.*

Compliance with some regulations, such as NYCRR and GLBA, is mandatory.

The GLBA (Gramm-Leach-Bliley Act) defines a financial institution as any organization significantly involved in financial activities outlined in Section 4(k) of the Bank Holding Company Act. This definition applies to all financial service entities, regardless of their size. Notably, it encompasses companies not typically viewed as financial institutions.

- Check-cashing businesses
- Payday lenders
- Mortgage brokers

- Nonbank lenders (for example, automobile dealers providing financial services)
- Technology vendors providing loans to clients
- Educational institutions providing financial aid
- Debt collectors
- Real estate settlement service providers
- Personal property or real estate appraisers
- Retailers that issue branded credit cards
- Professional tax preparers
- Courier services

Healthcare Provider

A healthcare provider is a person or an organization that provides patient or medical services, such as doctors, clinics, hospitals …

Health Plan

A health plan is an entity that provides payment for medical services, such as health insurance companies, government health plans or government programs that pay for healthcare …

Healthcare Clearinghouse

A healthcare clearinghouse is an entity that processes nonstandard health information it receives from another entity into a standard format.

Business Associates

Business associates were initially defined as persons or organizations that perform certain functions or activities involving the use or disclosure of personal health information (**PHI)** on behalf of , or provide services to , a covered entity.

Sensitive authentication data may never be stored post-authorization, even if encrypted.

Cardholder Data	Sensitive Authentication Data
Primary account number (**PAN**)	**Full magnetic stripe data or equivalent data on a chip**
cardholder name	**CAV2 / CVC2 / CVV2/ CID**
Expiration date	**PINs** / **PIB** blocks
Service code	

Most credit cards and many government organizations use the Luhn algorithm to validate numbers. The Luhn algorithm is based on the principle of modulo arithmetic and digital roots. It uses modulo-10 mathematics.

The following are the typical elements on the front of a credit card:

- Embedded microchip
- PAN
- Expiration date
- cardholder name

The following are the typical elements on the back of a credit card:

- **Magnetic stripe(mag stripe):** The magnetic stripe contains encoded data required to authenticate, authorize, and process transactions.
- **CAV2/CID/CVC2/CVV2:** All these abbreviations are names for card security codes for the different payment brands.

Key Technical Elements in Regulations You Should Consider

Most regulations dictate several key elements, and a penetration tester should pay attention to and verify them during assessment to make sure the organization is compliant. Select each element for more information.

Regulations	Description
Data Isolation	Organizations that need to comply with **PCI DSS** (and other regulations, for that matter) should have a **data isolation strategy.** Also known

	as network isolation or network segmentation, the goal is to implement a completely **isolated network** that includes all systems involved in **payment card processing**.
Password Management	Most regulations mandate **solid password** management strategies. For example, organizations must not use vendor-supplied defaults for system passwords and security parameters. This requirement also extends far beyond its title and enters the realm of configuration management. In addition, most of these regulations mandate specific implementation standards, including password length, password complexity, and **session timeout**, as well as the use of multifactor authentication.
Key Management	Key management's significance in cryptography is underscored by NIST SP 800-57, focusing on the secure creation, application, and safeguarding of keys from unauthorized access or changes. Like safe combinations, **keys are vital for determining algorithm functions and ensuring data**

	security, necessitating robust protection. NIST outlines detailed key management protocols to preserve cryptographic systems' security and efficacy, stressing the need to shield **secret and private keys** from unauthorized exposure.

Local Restrictions

the following are a few examples of constraints that you might face during a penetration testing engagement:

- Certain areas and technologies that cannot be tested due to operational limitations (For instance, you might not be able to launch specific SQL injection attacks, as doing so might corrupt a production database.)
- Technologies that might be specific for the organization being tested
- Limitation of skill sets
- Limitation of known exploits
- Systems that are categorized as out of scope because of the criticality or known performance problems

General Data Protection Regulation (GDPR)	Strengthens and unifies data protection for individuals within the **European Union**

NIST SP 800-57	Guidelines for **encryption key management**
Payment Card Industry Data Security Standard (PCI DSS)	Secures the processing of **credit card** and other types of **digital payments**
Gramm-Leach-Bliley Act (GLBA)	Applies to all **financial services organizations,** regardless of size
Health Insurance Portability and Accountability Act (HIPAA)	Safeguards **electronic health information**

Legal Concepts

Service-level agreement (SLA)

An SLA is a well-documented expectation or constraint related to one or more of the minimum and/or maximum performance measures (such as **quality**, **timeline**/**timeframe**, and **cost**) of the penetration testing service. You should become familiar with any **SLAs** that the organization that hired you has provided to its customers.

Confidentiality

You must discuss and agree on the handling of **confidential data**. For example, if you are able to find passwords or other sensitive data, do you need to disclose all those passwords or all that sensitive data? Who will have access to the sensitive data? What will be the proper way to communicate and handle such data? Similarly, you must protect sensitive data and delete all records, per your agreement with your client. Your customer could have specific data retention policies that you might also have to be aware of. **Every time you finish a penetration testing engagement, you should delete any records from your systems.** You do not want your next customer to find sensitive information from another client

in any system or communication.

Statement of work (SOW)

An SOW is a document that **specifies the activities to be performed during a penetration testing engagement**. It can be used to define some of the following elements:

- Project (penetration testing) timelines, including the **report delivery schedule**
- The **scope of the work** to be performed
- The **location of the work** (geographic location or network location)
- Special **technical and nontechnical requirements**
- **Payment schedule**
- **Miscellaneous items** that may not be part of the main negotiation but that need to be listed and tracked because they could pose problems during the overall engagement

The SOW can be a standalone document or can be part of a master service agreement (MSA).

Master service agreement (MSA)

MSAs, which are very popular today, are contracts that can be used to **quickly negotiate the work** to be performed. When a master agreement is in place, **the same terms do not have to be renegotiated every time** you perform work for a customer. **MSAs are especially beneficial when you perform a penetration test, and you know that you will be rehired on a recurring basis to perform additional tests in other areas of the company or to verify that the security posture of the organization has been improved as a result of prior testing and remediation.**

Non-disclosure agreement (NDA)

An **NDA** is a legal document and contract between you and an organization that has hired you as a penetration tester. **An NDA specifies and defines confidential material, knowledge, and information that should not be disclosed and that should be kept confidential by both parties.** NDAs can be classified as any of the following:

- **Unilateral**: With a unilateral NDA, only one party discloses certain information to the other party, and the information must be kept protected and not disclosed. For example, an organization that hires you should include in an NDA certain information that you should not disclose. Of course, all of your findings must be kept secret and should not be disclosed to any other organization or individual.

- **Bilateral**: A bilateral NDA is also referred to as a mutual, or two-way, NDA. In a bilateral NDA, both parties share sensitive information with each other, and this information should not be disclosed to any other entity.

- **Multilateral**: This type of NDA involves three or more parties, with at least one of the parties disclosing sensitive information that should not be disclosed to any

entity outside the agreement. Multilateral NDAs are used in the event that an organization external to your customer (business partner, service provider, and so on) should also be engaged in the penetration testing engagement.

Service-level agreement (SLA)	Documented minimum and maximum performance expectations of the penetration test service
Confidentiality	Agreement regarding how to communicate and handle sensitive data, such as account credentials that were uncovered by the testing
Disclaimer	Statements such as "The penetration test report cannot and does not protect against personal or business loss resulting from the test agreement."
Non-disclosure agreement (NDA)	Specifies and defines confidential material, knowledge, and information that should be kept confidential and not be disclosed to outside parties

Contracts

The contract is one of the most important documents in a pen testing engagement. It specifies the terms of the agreement and how you will get paid, and it provides clear documentation of the services that will be performed. A contract should be very specific, easy to understand, and without ambiguities. Any ambiguities will likely lead to customer dissatisfaction and friction. Legal advice (from a lawyer) is always recommended for any contract.

Your customer might also engage its legal department or an outside agency to review the contract. A customer might specify and demand that any information collected or analyzed during the

penetration testing engagement cannot be made available outside the country where you performed the test. In addition, the customer might specify that you (as the penetration tester) cannot remove personally identifiable information (PII) that might be subject to specific laws or regulations without first committing to be bound by those laws and regulations or without the written authorization of the company. Your customer will also review the penetration testing contract or agreement to make sure it does not permit more risk than it is intended to resolve.

Another very important element of your contract and pre-engagement tasks is that you must obtain a signature from a proper signing authority for your contract. This includes written authorization for the work to be performed. If necessary, you should also have written authorization from any third-party provider or business partner. This would include, for example, Internet service providers, cloud service providers, or any other external entity that could be considered to be impacted by or related to the penetration test to be performed.

Disclaimers

You might want to add disclaimers to your pre-engagement documentation, as well as in the final report. For example, you can specify that you conducted penetration testing on the applications and systems that existed as of a clearly stated date. Cybersecurity threats are always changing, and new vulnerabilities are discovered daily. No software, hardware, or technology is immune to security vulnerabilities, no matter how much security testing is conducted.

You should also specify that the penetration testing report is intended only to provide documentation and that your client will

determine the best way to remediate any vulnerabilities. In addition, you should include a disclaimer that your penetration testing report cannot and does not protect against personal or business loss as a result of use of the applications or systems described therein.

Another standard disclaimer is that you (or your organizations) provide no warranties, representations, or legal certifications concerning the applications or systems that were or will be tested. A disclaimer might say that your penetration testing report does not represent or warrant that the application tested is suitable to the task and free of other vulnerabilities or functional defects aside from those reported. In addition, it is standard to include a disclaimer stating that such systems are fully compliant with any industry standards or fully compatible with any operating system, hardware, or other application.

Rules of Engagement

Sample elements of a Rules of Engagement Document

Rule of Engagement Element	Example
Testing timeline	Three weeks, as specified in a Gantt chart 
Location of the testing	Company’s addresse

Time windows of the testing (times of days)	9:00 a.m to 5:00 p.m. EST
Preferred method of communication	Final report and weekly status update meetings
The security controls that could potentially detect or prevent testing	Intrusion prevention systems (IPSs)m firewalls , data loss prevention (DLP) systems
IP addresses or networks from which testing will originate	10.10.1.0/24, 1921.168.66.66, 10.20.15.123
Types of allowed or disallowed tests	- **Testing only web applications(app1.secretcorp.co;** ..). - **No social engineering attacks are allowed.** - **No SQL injection attacks are allowed in the production environment** - **SQL injection is only allowed in the development and staging environments at : app1-dev.sercetcorp.org app1-stage.sercetcorp.org** **..**

target List and In-Scope Assets

Scoping is one of the most important elements of the pre-engagement tasks with any penetration testing engagement.

You not only have to carefully identify and document all systems, applications, and networks that will be tested but also determine any specific requirements and qualifications needed to perform the test. The broader the scope of the penetration testing engagement, the more skills and requirements that will be needed.

Your scope and related documentation must include information about what types of networks will be tested. In addition to IP ranges, you must document any wireless networks or service set identifiers (SSIDs) that you are allowed or not allowed to test.

You may also be hired to perform an assessment of modern applications using different **application programming interfaces (APIs).**

SOAP

Simple Object Access Protocol (**SOAP**) project file: SOAP is an API standard that relies on XML and related schemas. XML-based specifications are governed by **X**ML **S**chema **D**efinition (**XDS**) documents. **Having a good reference of what a specific API supports can be very beneficial for a penetration tester and will accelerate the testing.** The SOAP specification can be accessed at https://www.w3.org/TR/soap.

Swagger

Swagger (Open API) documentation is a modern framework of API documentation and development that is now the basis of the **O**pen**A**PI **S**pecification (**OAS**). These documentation are used in **R**epresentational **S**tate **T**ransfer (**REST**) APIs. REST is software architectural style designed to guide development of the architecture for web services (including APIs). **REST**, or **RESTful** ,

APIs are the most common types of APIs used today. Swagger documents can be extremely beneficial when testing APIs. Additional information about swagger can be obtained at https://swagger.io. The OAS is available at https://github.com/OAI/OpenAPI-Specification.

WSDL

Web **S**ervice **D**escription **L**anguage (**WSDL**) is an XML-based language that is used to document the functionality of a web service.
The WSDL specification can be accessed at https://www.w3.org/TR/wsdl20-primer.

GraphQL

GraphQL is a query language for APIs. It is also a server-side runtime for executing queries using a type system you define for your data. Additional technical information about GraphQL can be accessed at https://graphql.org/learn.

WADL

Web **A**pplication **D**escription **L**anguage (**WADL**) is an XML-based language for describing web applications. The WADL specification can be obtained from https://www.w3.org/Submission/wadl.

The following are some additional support resources that you might obtain from the organization that hired you to perform

the penetration test. Select each resource for more information.

SDK (**S**oftware **D**evelopment **K**it)

An **SDK**, or devkit, is a collection of software development tools that can be used to interact and deploy a **software framework**, an **operating system**, or a **hardware platform**. SDKs can also help pen testers understand certain specialized applications and hardware platforms within the organization being tested.

Source code Access

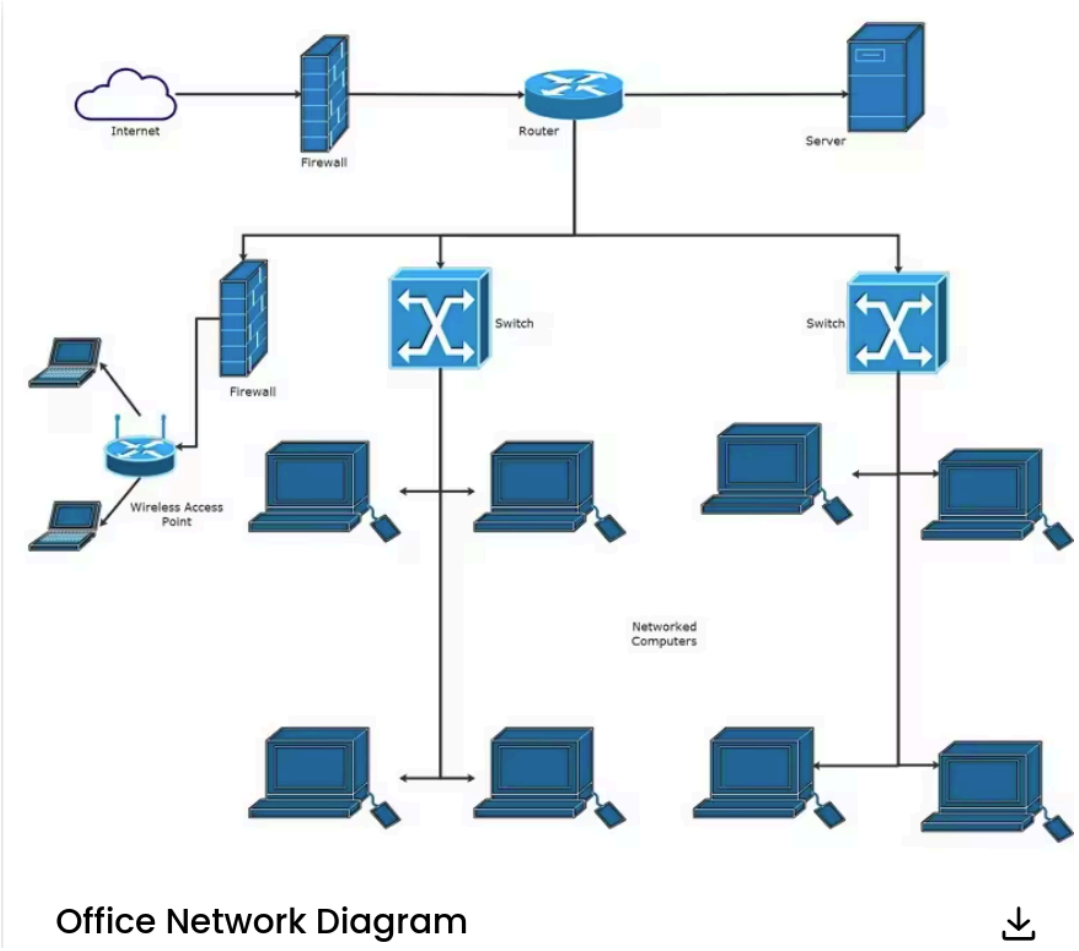
Some organizations may allow you to obtain access to the source code of applications to be tested.

Example of application requests

In most cases, you will be able to reveal context by using web application testing tools such as proxies like the Burp Suite and the OWASP Zed Attack Proxy (ZAP). You will learn more about these tools in Module 6, “Exploiting Application-Based Vulnerabilities,” and Module 10, “Tools and Code Analysis.”

System and network architectural diagrams

These documents can be very beneficial for penetration testers, and they can be used to document and define what systems are in scope during the testing.



Office Network Diagram

Scope creep is a project management term that refers to the uncontrolled growth of a project's scope. It is also often referred to as kitchen sink syndrome, requirement creep, and function creep. Scope creep can put you out of business. Many security firms suffer from scope creep and are unsuccessful because they have no idea how to identify when the problem starts or how to react to it.

- When there is poor change management in the penetration testing engagement.(**Management issue**)

- When there is ineffective identification of what technical and nontechnical elements will be required for the penetration test. (**Technical issue**)

- When there is poor communication among stakeholders, including your client and your own team.(**communication issue**)

Validating the Scope of Engagement

The first step in validating the scope of an engagement is to question the client and review contracts. You must also understand who the target audience is for your penetration testing report. You should understand the **subjects**, **business units**, and **any other entity** that will be assessed by such a penetration testing engagement.

discover different characteristics of your target audience.

- What is the entity's or individual's need for the report?

- What is the position of the individual who will be the primary recipient of the report within the organization?

- What is the main purpose and goal of the penetration testing engagement and ultimately the purpose of the report?

- What is the individual's or business unit's responsibility and authority to make decisions based on your findings?

- Who will the report be addressed to–for example, the information security manager (ISM), chief information security officer (CISO), chief information officer (CIO), chief technical officer (CTO), technical teams, and so on?

- Who will have access to the report, which may contain sensitive information that should be protected, and whether access will be provided on a need-to-know basis?

You should always have good open lines of communication with the clients and the stakeholders that hire you.

- **Primary recipient of the report**
- **Purpose and goal**
- **Responsibility and authority**
- **Report address to**
- **Others with access to the report**

Should have proper documentation of answers to the following questions.

- What is the contact information for all relevant stakeholders?

- How will you communicate with the stakeholders?

- How often do you need to interact with the stakeholders?

- Who are the individuals you can contact at any time if an emergency arises?

- **Communication process**
- **Timing of interactions**

- **Emergency contacts**

PRIMARY STAKEHOLDER			
Name		Email	
Title		Responsibility	
Work Number	Mobile Phone	Other Number	Alternate Email
Address		Notes	
City		State	ZIP Code
EMERGENCY CONTACTS			
Primary Emergency Contact		Secondary Emergency Contact	
Phone	Email	Phone	Email
Address		Address	
City, ST ZIP Code		City, ST ZIP Code	

You should ask for a form of secure bulk data transfer or storage, such as Secure Copy Protocol (SCP) or Secure File Transfer Protocol (SFTP). You should also exchange any Pretty Good Privacy (PGP) keys or Secure/Multipurpose Internet Mail Extensions (S/MIME) keys for encrypted email exchanges.

Questions about budget and return on investment (ROI) may arise from both the client side and the tester sides in penetration testing.

- How do I explain the overall cost of penetration testing to my boss?

- Why do we need penetration testing if we have all these security technical and nontechnical controls in place?

- How do I build in penetration testing as a success factor?

- Can I do it myself?

- How do I calculate the ROI for the penetration testing engagement?

ROI (**R**eturn **O**f **I**nvestment)

tester needs to answer questions like these.

- How do I account for all items of the penetration testing engagement to avoid going over budget?

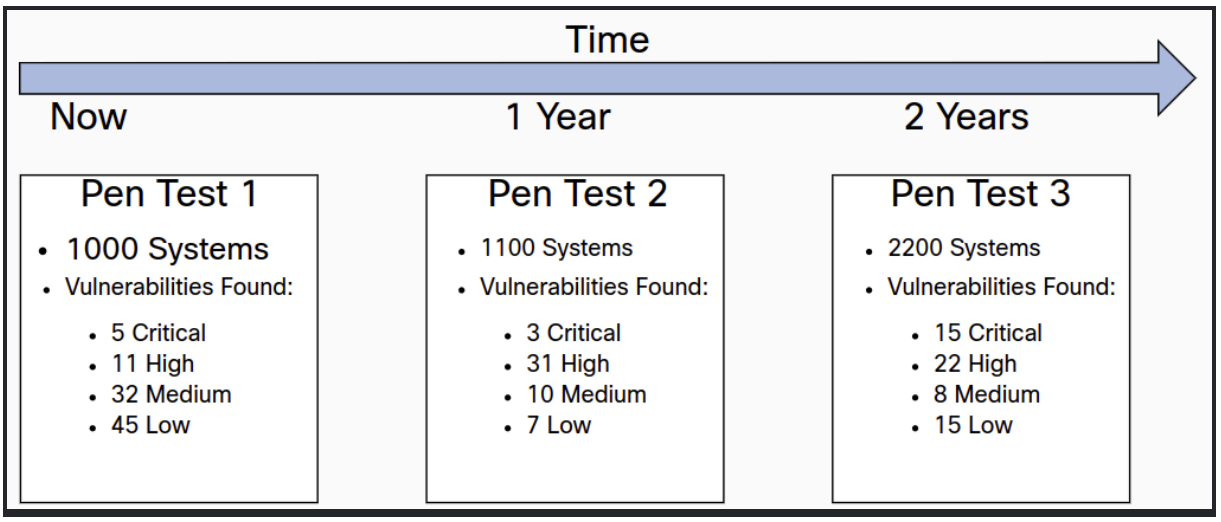
- How do I do pricing ?

- How can I clearly show ROI to my client ?

- **Budget Concerns**
- **Pricing**
- **Demonstrate ROI**

The answers to these questions depend on how effective you are at scoping and clearly communicating and understanding

all the elements of the penetration testing engagement. Another factor is understanding that penetration testing is a point-in-time assessment.



In Figure 2-3, a total of three pen testing engagements took place in a period of two years at the same company. In the first engagement, 1000 systems were assessed; 5 critical-, 11 high-, 32 medium-, and 45 low-severity vulnerabilities were uncovered. A year later, 1100 systems were assessed; 3 critical-, 31 high-, 10 medium-, and 7 low-severity vulnerabilities were uncovered. Then two years later, 2200 systems were assessed; 15 critical-, 22 high-, 8 medium-, and 15 low-severity vulnerabilities were uncovered. Is the company doing better or worse? Are the pen test engagements done just because of a compliance requirement? How can you justify the penetration testing if you continue to encounter vulnerabilities over and over after each engagement?

You can see that it is important for both the client and the pen tester to comprehend that penetration testing alone cannot guarantee the overall security of the company. The pen tester also needs to incorporate clear and achievable mitigation strategies for the vulnerabilities found. In addition, an appropriate impact analysis and remediation timelines must be discussed with the respective stakeholders.

Unknown vs. Known Environment Testing

Unknown Environment (Black-Box):

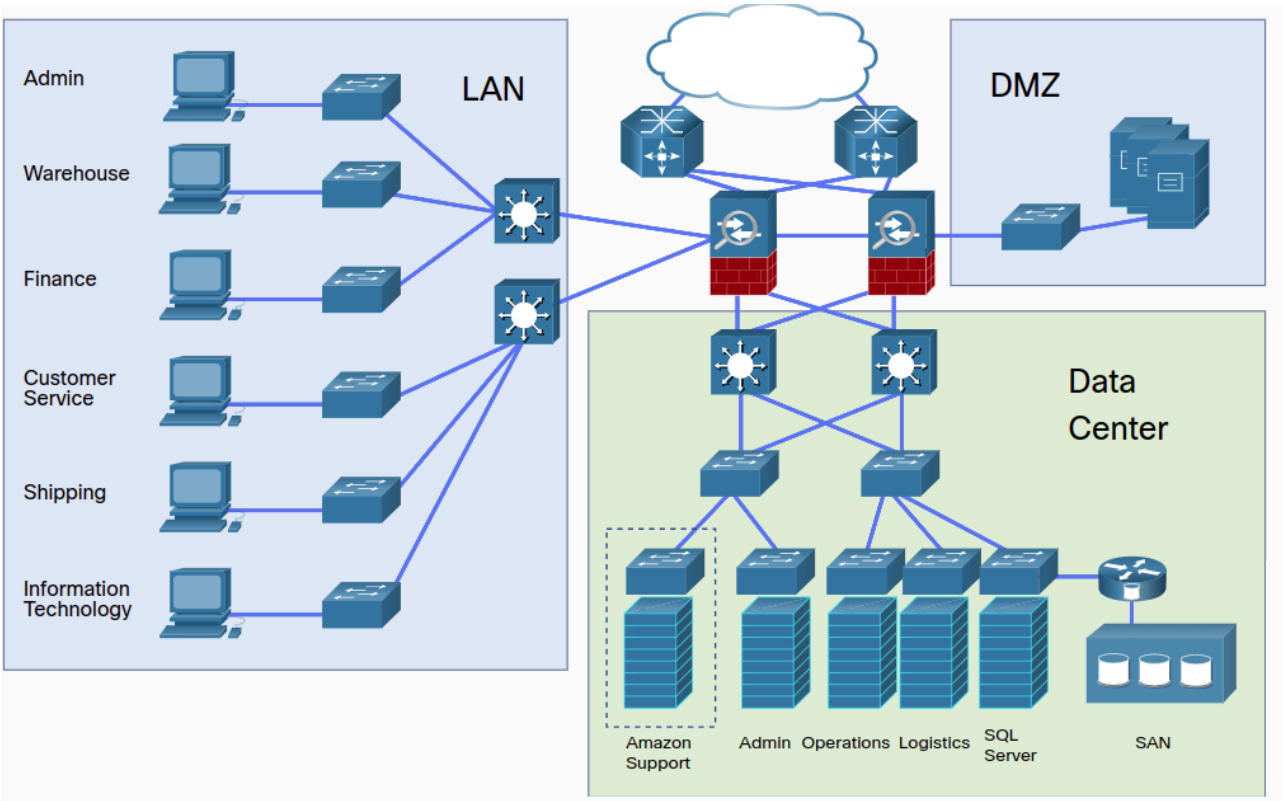
The tester is typically provided only a very limited amount of information. For instance, the tester may be provided only the **domain names** and **IP addresses** that are in scope for a particular target.

Known Environment (White-Box):

The tester starts out with a significant amount of information about the organization and its infrastructure. The tester is normally 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 testing is to identify as many security holes as possible.

Pre-Engagement Scope and Planning

Topology



Addressing Table - Data Center

Servers	VLAN	IP Address	Subnets
Administration	2-5	172.24.1.0/24	(4) 255.255.255.192

Amazon support	10 - 25	172.25.0.0/16	(11) 255.255.252.0
Operations	50 - 55	172.26.0.0/21	(5) 255.255.255.0
Logistics	80 - 85	172.27.0.0/21	(5) 255.255.255.0
Management	100 - 110	172.30.0.0/16	various an necessary

Addressing Table - LAN

Department	VLAN	IP Address	Subnet Mask
Administration	120	172.16.1.0	255.255.255.0
Finance	130	172.16.4.0	255.255.255.0
Information Technology	140	172.16.8.0	255.255.255.0
Warehouse	150	172.16.12.0	255.255.255.0
Customer Service	160	172.16.16.0	255.255.255.0
Shipping	170	172.16.20.0	255.255.255.0

Create a Pentesting Agreement

The information contained in each sections :

- **Parties to the agreement** (Highlight the personal details and

information of the parties involved.)

This section will detail the names, addresses, and contact information of the penetration testing service provider (hereafter referred to as "Tester") and the client company seeking the pentesting services (hereafter referred to as "Client"). It ensures clarity on who is involved in the agreement.

- **Scope of work**

  This outlines the expectations and deliverables from both parties.

  The penetration tester agrees to:

  - Conduct a thorough assessment in alignment with the agreed-upon scope, employing methodologies to identify vulnerabilities without causing harm to the client's systems.

  - Provide a detailed report of findings, including vulnerabilities, evidence of testing, and recommendations for mitigation.
  -
  - Ensure all testing is conducted within legal and ethical boundaries, respecting privacy and confidentiality agreements.

  The client agrees to :

  - Provide necessary access and information required for the penetration testing, including network details, system credentials, or physical access, as per the agreed scope.

  - Ensure that appropriate backups and system recovery processes are in place to mitigate any accidental damage during testing.

  - Compensate the tester as agreed upon in the fees and payment section of this agreement.

- **Timeframe** (Establish a specific timeline for the penetration testing)

  - Specifies the start and end dates of the penetration testing project, including any key milestones. It may also outline the schedule for testing to minimize impact on the client's operations.

- **Fees, billing, and payment details** (Define how and when payments are made and address how materials and equipment are obtained.)

    - Describes the financial terms of the agreement, including the total cost of the penetration testing services, payment schedule, and any additional costs (e.g., for unforeseen work or out-of-scope activities). It also details how expenses for materials and equipment necessary for the test will be handled.

- **Termination of contract** (Define the circumstances that would lead to an early termination of the contract.)

    - This section includes circumstances and situations that can lead to early contract termination by either party. It addresses the right of the penetration testing firm or the client to end the partnership for things like failure to pay fees on time or testing not done properly. It should explain the course of action to be taken in the event of early termination.

- **Bonus - Additional Agreement sections** (This could include Warranty, Disclaimer, Liability Limitation, and Dispute Resolution.)

    - **Confidentiality and Non-Disclosure**: Both parties agree not to disclose sensitive information obtained during the testing process.

    - **Liability and Indemnification:** Defines the limits of liability for both parties and includes indemnification clauses to protect against legal actions arising from the testing.

    - **Data Protection:** Ensures compliance with relevant data protection laws, detailing how data collected during testing will be handled, stored, and destroyed.

    - **Non-Compete and Non-Solicitation:** Prevents the tester from engaging in competitive activities with the client or soliciting the client's employees for a specified period.

    - **Governing Law:** Specifies the jurisdiction under which disputes will be resolved.

Ethical hacker Should demonstrate professionalism and integrity

Background check of penetration testing teams

A client may require that you and your team undergo careful background checks, depending on the environment and engagement. Organizations sometimes require these background checks to feel comfortable with the penetration testing teams that they are allowing to access their environment and information. Your clients may check your credentials and make sure that you have the skills to make their network more secure by finding vulnerabilities that could be exploited by malicious attackers.

Adherence to the specific scope of engagement

The acquiring company might ask the company that is being acquired to show whether penetration testing has been conducted in the past year or the past six months. If not, the company being acquired might be required to hire a penetration testing firm to perform an assessment. During the scoping phase, the target selection process needs to be carefully completed with the company that hired you, or, if you are part of a full-time red team, with the appropriate stakeholders in your organization. The organization might create a list of applications, systems, or networks to be tested. This is often referred to as a penetration testing scope “allow list.” An allow list is a list of applications, systems, or networks that are in scope and should be tested. On the other hand, a deny list is a list of applications, systems, or

networks that are not in scope and should not be tested. You must always obey those rules.

Identification of criminal activity and immediate reporting of breaches/criminal activities

In some cases, you may find that a real attacker has already compromised the client's systems and network. In such cases, you must identify any criminal activities and report them immediately.

Limiting the use of tools to a particular engagement

In some penetration testing engagements, you will not be allowed to use a particular set of tools that the organization does not permit because of legal reasons or because those tools could bring down the network and underlying systems.

Limiting invasiveness based on scope

Some tools and attacks could be detrimental and extremely disruptive for your client's systems and mission. You should always limit the verbosity and invasiveness of your tests and tools based on the agreed scope.

Confidentiality of data/information

The results of the penetration testing engagement (report) and information that you may gather and have access to during the penetration must be protected and kept confidential. If this information is lost or shared, it could be used by an adversary to cause a lot of damage to your client.

Risks to the professional

If you do not adhere to the best practices outlined in this list, you could be subject to different fees or fines and, in some cases, even criminal charges. Therefore, companies and individuals conducting professional penetration testing often have at least general business liability insurance. If you are in the cybersecurity field (often dealing with risk management), you need to know the risks to your business and protect yourself against this risk.

Approaches to Ethical Decision Making

Ethical decision-making involves evaluating and choosing among alternatives in a manner consistent with ethical principles. In facing a decision, individuals or organizations often need to consider ethical standards, principles, and the potential impact of their decisions on stakeholders and society as a whole. There are several approaches to ethical decision-making, each offering a different perspective on how to determine the most ethical course of action. Here are some of the key approaches:

1. Utilitarian Approach

Principle: The best decision is the one that maximizes overall happiness or utility.

Key Consideration: Assess the outcomes of different actions and choose the one that produces the greatest benefit (or least harm) for the greatest number of people.

2. Deontological (Duty-Based) Approach

Principle: The decision should be based on what is morally right or wrong according to a set of rules, regardless of the consequences.

Key Consideration: Follow moral principles or duties, such as honesty, fairness, and rights. Actions are considered ethical if they respect the rights of individuals and are in accordance with moral rules or duties.

3. Rights Approach

Principle: The most ethical action is the one that best protects and respects the moral rights of those affected.

Key Consideration: Focus on the rights of individuals and ensure that these rights are not violated. This approach emphasizes the importance of human dignity and the right to be treated as ends rather than means.

4. Virtue Ethics Approach

Principle: Ethical actions ought to be consistent with certain ideal virtues that provide for the full development of our humanity.

Key Consideration: Focus on the character and virtues of the individual making the decision, rather than on the specifics of the decision itself. Virtues might include honesty, courage, compassion, integrity, and wisdom.

5. Justice or Fairness Approach

Principle: Ethical decisions should be made based on fairness, equity, and impartiality.

Key Consideration: Treat all people equally, or if unequally, then fairly based on some standard that is defensible. This approach also considers issues of fairness in the distribution of goods and harms.

6. Common Good Approach

Principle: The most ethical action is the one that advances the common good.

Key Consideration: Focus on what is beneficial for the community as a whole, emphasizing the interconnection of society and the relationships that make a society or community.

7. Ethical Egoism

Principle: The best decision is the one that advances one's own best long-term interests.

Key Consideration: In some interpretations, ethical egoism suggests that actions are ethical if they benefit the individual, but it can be argued that what is in an individual's best interest can also be in the interest of others.

Code of ethics for information technology

A Code of Ethics for Information Technology (IT) professionals is essential for guiding behavior and decision-making in a field that impacts almost every aspect of modern life. Information technology involves complex ethical considerations, ranging from data privacy and security to the digital divide and intellectual property rights. Below is an outline of key principles that might be included in a Code of Ethics for IT professionals:

Common Elements of a Code of Ethics:

1. Respect for Privacy: IT professionals should protect the privacy of individuals and organizations by handling personal data responsibly, ensuring confidentiality, integrity, and availability of information.

2. Integrity: Maintain honesty and fairness in all professional dealings. Avoid conflicts of interest and ensure that personal gain does not influence professional decisions.

3. Transparency: Be transparent in the development, implementation, and maintenance of systems. Clearly communicate the capabilities, limitations, and potential impacts of technology solutions.

4. Accountability: Take responsibility for the work performed and decisions made. Acknowledge mistakes and work to rectify them promptly.

5. Quality: Strive for excellence in all aspects of IT work. Ensure that products, services, and systems are reliable, safe, and meet the highest standards of quality.

6. Security: Prioritize the security of information systems and data. Protect against unauthorized access, cyber threats, and vulnerabilities to maintain trust and confidence in IT systems.

7. Equity and Inclusion: Work to eliminate discrimination and ensure equal access to information technology regardless of race, gender, age, disability, or economic status.

8. Professional Development: Engage in lifelong learning to keep skills and knowledge current. Contribute to the professional development of others and the advancement of the field.

9. Compliance with Laws and Regulations: Adhere to applicable laws, regulations, and professional standards. Stay informed about legal requirements affecting IT and ensure compliance.

10. Social Responsibility: Recognize the broader impacts of information technology on society. Work to ensure that technology serves the public good and contributes to the betterment of humanity.

11. Environmental Sustainability: Advocate for and implement environmentally sustainable practices in IT operations, development, and disposal of technology products and services.

12. Respect for Intellectual Property: Respect copyright, trademarks, and patents. Avoid plagiarism and ensure that the use of software, hardware, and content is legally and ethically appropriate.

Personal Code of Professional Ethics for Ethical Hacking

1- Maintain confidentiality: Protect all confidential information I come across in my professional activities, ensuring that data privacy and client trust are never compromised.

2- Prioritize security: Always prioritize the security of systems, networks, and data against unauthorized access, use, disclosure, disruption, modification, or destruction.

3- Act with integrity: Conduct all activities with the highest level of integrity, ensuring honesty, fairness, and transparency in every action and decision.

4- Respect for privacy: Respect the privacy of individuals and organizations by handling data responsibly and in accordance with relevant laws and ethical standards.

5- Legal compliance: Adhere strictly to all applicable laws, regulations, and standards governing information technology and cybersecurity.

6- Professional competence: Commit to lifelong learning and professional development to maintain and enhance my knowledge and skills in ethical hacking and cybersecurity.

7- Accountability: Take full responsibility for my actions and their consequences, ensuring accountability in all professional endeavors.

8- Promote security awareness: Educate clients, stakeholders, and the community about cybersecurity risks and best practices to foster a safer digital environment.

9- Avoid conflicts of interest: Identify and avoid any conflicts of interest, and disclose any potential conflicts to involved parties.

10- Contribute to the community: Share knowledge and contribute to the development of ethical hacking practices, helping to improve the security posture of the broader community.

I commit myself to uphold these ethical principles in my practice of ethical hacking, ensuring that my actions benefit my clients, society, and the field of cybersecurity.

Signature: AIT OUFKIR BRAHIM

Date: 02/23/2024

What Did I Learn in this Module ?

Comparing and contrasting governance, Risk, and Compliance Concepts

Key Technical Elements in Regulations You Should Consider

Several key technical elements are mandated by most regulations, including data isolation, password management, and key management. Data isolation involves creating a separate network for systems involved in payment card processing to ensure they are completely isolated. Password management strategies must meet specific implementation standards and should include the use of strong passwords and multifactor authentication. Key management is also critical and involves the proper management and protection of cryptographic keys to ensure the security of information protected by cryptography. Policies and standards for key management should include assigned responsibilities, the nature of information to be protected, the classes of threats, and the cryptographic protection mechanisms to be used.

Legal Considerations

Important legal concepts that are relevant to performing a penetration test include Service-level Agreements (SLAs), confidentiality agreements, statements of work (SOWs), master service agreements (MSAs), and non-disclosure agreements (NDAs). The section also emphasizes the importance of contracts in a penetration testing engagement and the need for clarity, specificity, and legal advice. Finally, it suggests adding disclaimers to pre-engagement documentation and final reports to address the limitations of penetration testing and to avoid potential legal liabilities.

Explaining the importance of Scoping and Organizational or Customer Requirements

The rules of engagement document outlines the conditions under which the testing will be performed and includes details such as the testing timeline, location of testing, time window of testing, preferred method of

communication, security controls that could potentially prevent testing, IP addresses or networks from which testing will originate, and types of allowed or disallowed tests. Gantt charts and work breakdown structures can be used to document the timeline of the testing.

Scoping is one of the most important elements of the pre-engagement tasks and includes documentation of the systems, networks, and applications to be tested, as well as any specific requirements needed for the test. There are different types of API documentation and additional support resources that might be available for the penetration tester. The engagement scope must include physical location, DNS fully qualified domain names, and external vs. internal target identification.

The scope of the test and the amount of time and money spent on it depend on various factors, such as the company's specific concerns and the level of sophistication and capabilities of potential attackers. While known-environment testing can be useful for identifying specific vulnerabilities, unknown-environment testing is often a good choice because it provides a more realistic assessment of the network's security posture.

Demonstrating an Ethical Hacking Mindset by Maintaining Professionalism and integrity

This topic discusses several key considerations for ethical hackers or penetration testers to demonstrate professionalism and integrity. These include undergoing background checks, adhering to the specific scope

of engagement, identifying criminal activity and reporting it immediately, limiting tool usage, respecting invasiveness based on scope, maintaining confidentiality of data and information, and understanding the risks involved. Additionally, the topic emphasizes the importance of risk management and risk tolerance in cybersecurity governance programs. All parties involved should make informed decisions and manage risk while keeping organizational objectives in mind.