

Master of Cybersecurity

Prepared by Dr. Nermin Hamza

CYB740

Penetration test and Ethical hacking

Lecture 01



ETHICAL HACKING AND PENETRATION TESTING GUIDE

RAFAY BALOCH



CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

Introduction for Penetration test and Ethical hacking

Lecture 01

CYB740

Penetration test and Ethical hacking

Prepared by
Dr. Nermin Hamza

Outlines

- Hacking Introduction
- What Is a Penetration Test?
- Pre-engagement
- Penetration Testing Viewpoints
- Penetration Testing Methodologies and Standards
- Phases of Penetration Testing
- Understand the audience
- Types of Penetration Tests
- How to become a Penetration Tester
- Vulnerability Assessments versus Penetration Test

Hacking Introduction

- **“White-hat hackers”** break security for non-malicious purposes, usually when performing authorized security tests.
- **“Black-hat hackers”** violate computer security for maliciousness or personal gain.
- **“Grey-hat hackers”** rationalize that they are acting moral when they are not. e.g.: Breaking into systems for fun, then emailing the sysadmin to tell them about the security hole.

Introduction

1- White hat hacker

- This kind of hacker is often referred to as a security professional or security researcher.
- Such hackers are employed by an organization and are permitted to attack an organization to find vulnerabilities that an attacker might be able to exploit.

Introduction

2. Black hat hacker

- Also known as a **cracker**, this kind of hacker is referred to as a **bad guy**, who uses his or her knowledge for negative purposes.
- They are often referred to by the media as hackers.

Introduction

3. Gray hat hacker

- This kind of hacker is an intermediate between a white hat and a black hat hacker.
- For instance, a gray hat hacker would work as a security professional for an organization and responsibly disclose everything to them; however, he or she might leave a backdoor to access it later and might also sell the confidential information, obtained after the compromise of a company's target server, to competitors.

Introduction : Main Definitions

Hacktivist

Ethical
hacker

Vulnerability

Exploit

Threat

Risk

Introduction : Main Definitions

Hacktivist—Hacktivists are defined as group of hackers that hack into computer systems for a cause or purpose. The purpose may be political gain, freedom of speech, human rights, and so on.

Ethical hacker—An ethical hacker is as a person who is hired and permitted by an organization to attack its systems for the purpose of identifying vulnerabilities, which an attacker might take advantage of. The sole difference between the terms “hacking” and “ethical hacking” is the permission.

Introduction: Main Definitions

Vulnerability ثغرة

Vulnerability is defined as a flaw or a weakness inside the asset that could be used to gain unauthorized access to it. The successful compromise of a vulnerability may result in data manipulation, privilege elevation, etc.

Introduction: Main Definitions

Exploit استغلال

An exploit is something that takes advantage of vulnerability in an asset to cause unintended or unanticipated behavior in a target system, which would allow an attacker to gain access to data or information.

Introduction: Main Definitions

Threat تهديد

A threat represents a possible danger to the computer system. It represents something that an organization doesn't want to happen. A successful exploitation of vulnerability is a threat. A threat may be a malicious hacker who is trying to gain unauthorized access to an asset.

Introduction: Main Definitions

Risk مخاطرة

A risk is defined as the impact (damage) resulting from the successful compromise of an asset.

Chapter

01

What Is a Penetration Test?

What Is a Penetration Test?

A penetration test is a subclass of ethical hacking; it comprises a set of methods and procedures that aim at testing/protecting an organization's security.

The penetration tests prove helpful in finding vulnerabilities in an organization and check whether an attacker will be able to exploit them to gain unauthorized access to an asset.

Pre-engagement

Before you start doing a penetration test, there is whole lot of things you need to discuss with clients. This is the phase where both the customer and a representative from your company would sit down and discuss about the legal requirements and the “**rules of engagement.**”

Rules of Engagement

Following are important requirements that are present in almost every ROE:

- A proper “permission to hack” and a “nondisclosure” agreement should be signed by both the parties.
- The scope of the engagement and what part of the organization must be tested.
- The project duration including both the start and the end date.
- The methodology to be used for conducting a penetration test.
- The goals of a penetration test.

Rules of Engagement

- The allowed and disallowed techniques, whether denial-of-service testing should be performed or not.
- The liabilities and responsibilities, which are decided ahead of time. As a penetration tester you might break into something that should not be accessible, causing a denial of service; also, you might access sensitive information such as credit cards. Therefore, the liabilities should be defined prior to the engagement.

Penetration Testing Viewpoints

- **External vs. Internal**

Penetration Testing can be performed from the viewpoint of an external attacker or a malicious employee.

- **Overt vs. Covert**

Penetration Testing can be performed with or without the knowledge of the IT department of the company being tested.

Categories of Penetration Test

The entire penetration test upon what the organization wants to test and how it wants the security paradigm to be tested.

1. Black Box
2. White Box
3. Gray Box

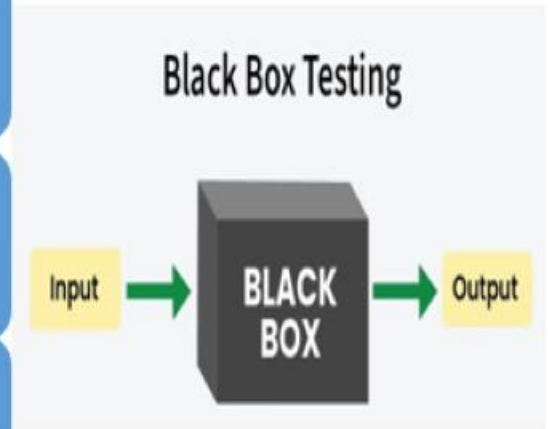
Black Box

A **black box penetration test** is where little or no information is provided about the specified target.

In the case of a network penetration test this means that the target's DMZ, target operating system, server version, etc., will not be provided; the only thing that will be provided is the IP ranges that you would test.

In the case of a web application penetration test, the source code of the web application will not be provided.

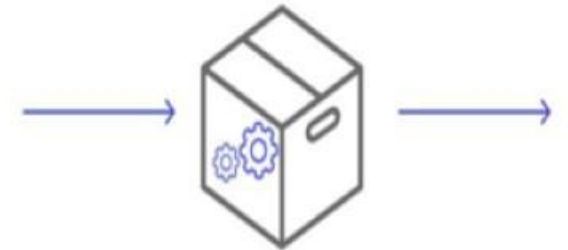
This is a very common scenario that you will encounter when performing an **external** penetration test.



White Box

- A **white box penetration test** is where almost all the information about the target is provided.
- In the case of a network penetration test, information on the application running, the corresponding versions, operating system, etc., are provided.
- In the case of a web application penetration test the application's source code is provided, enabling us to perform the static/dynamic "source code analysis."
- This scenario is very common in **internal**/onsite penetration tests, since organizations are concerned about leakage of information.

White Box Testing



Gray Box

- In a **gray box test**, some information is provided and some hidden.
- In the case of a network penetration test, the organization provides the names of the application running behind an IP; however, it doesn't disclose the exact version of the services running.
- In the case of a web application penetration test, some extra information, such as test accounts, back end server, and databases, is provided.



Categories of Penetration Test

Knowledge Type	Network Knowledge	Benefits
Black-Box (Covert)	No knowledge of the infrastructure	- More adversarial approach- Focused on the impact an adversary can cause
White-Box (Overt)	Almost complete knowledge of infrastructure (IPs, diagrams, etc.)	- Faster- Cheaper- More comprehensive evaluation of the network
Grey-Box	Some infrastructure knowledge	- Customer decided blend of speed vs adversarial simulation

Types of Penetration Tests

There are several types of penetration tests; however, the following are the ones most commonly performed:

- Network Penetration Test
- Web Application Penetration Test
- Mobile Application Penetration Test
- Social Engineering Penetration Test
- Physical Penetration Test

Penetration Testing Methodologies and Standards

Penetration Testing Methodologies and Standards

1. OSSTMM : Open-Source Security Testing Methodology Manual. It is one of the most widely used and recognized standards of penetration testing
2. OWASP: Open Web Application Security Project.
3. NIST: National Institute of Standards and Technology (NIST) offers very specific penetration testing guidelines for pen-testers to help them improve the accuracy of the test.

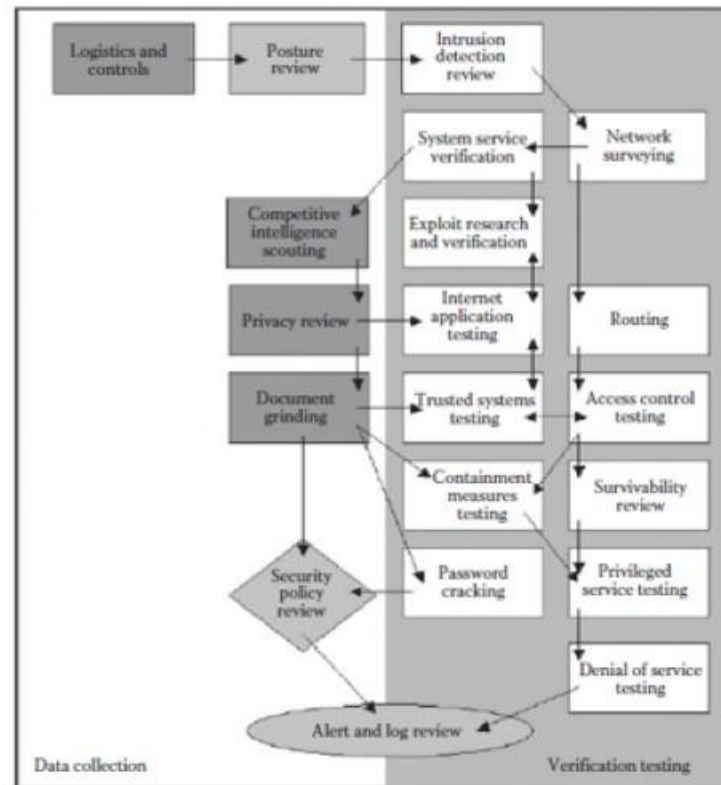
Penetration Testing Methodologies and Standards

4. PTES: PTES or Penetration Testing Execution Standards is a pentest methodology designed by a team of information security professionals.
5. ISSAF: The Information System Security Assessment Framework (ISSAF) is a pentesting guide supported by the Open Information Systems Security Group

Chapter
01

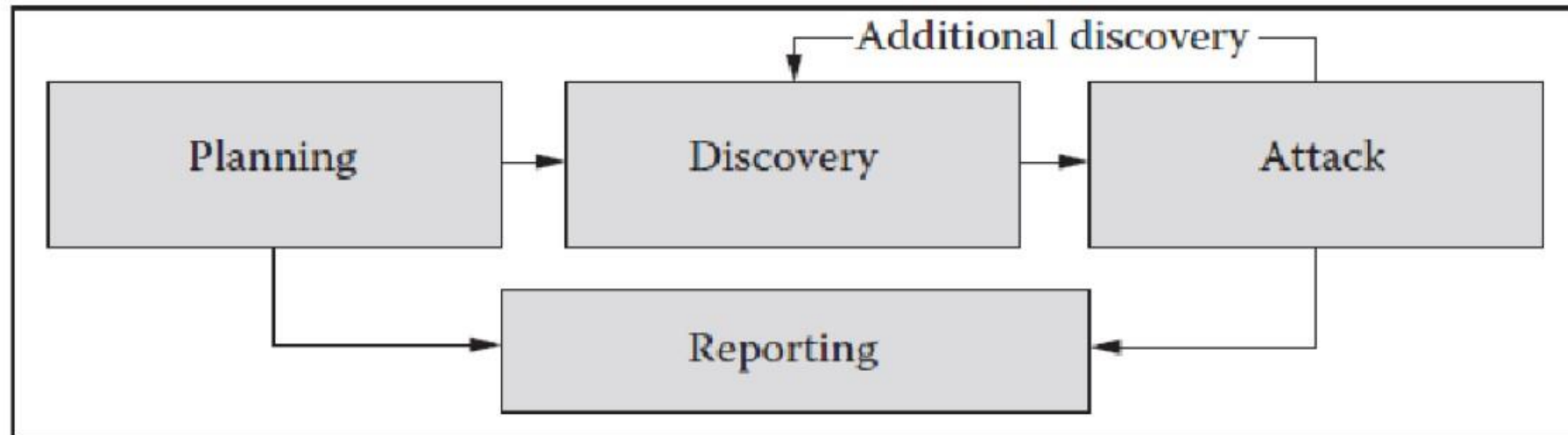
Penetration Testing Methodologies and Standards

OSSTMM



NIST





Methodology

Planning – In this phase, we plan how the assessments would be carried out.

Discovery – In this phase, the targets discovery, target enumeration, and vulnerability assessments are performed.

Attacking–In the attacking phase, the vulnerabilities that were found in the previous phase are attempted to be exploited. Once a system is exploited, an attempt to escalate privileges is made, the attacking phase contains two more steps, namely, system browsing and “Installing Additional Tools”.

During this process if a new target is discovered we move back towards the discovery phase.

Reporting–In the reporting phase the vulnerabilities that were discovered are documented.

Phases of Penetration Testing

Phases of Penetration Testing

- Reconnaissance and Information Gathering
- Network Enumeration and Scanning
- Vulnerability Testing and Exploitation
- Reporting

Reconnaissance and Information Gathering

Purpose: To discover as much information about a target (individual or organization) as possible without actually making network contact with said target.

Methods:

- Organization info discovery via WHOIS
- Google search
- Website browsing

Network Enumeration and Scanning

Purpose: To discover existing networks owned by a target as well as live hosts and services running on those hosts.

Methods:

- Scanning programs that identify live hosts, open ports, services, and other info (Nmap, autoscan)
- DNS Querying
- Route analysis (traceroute)

Vulnerability Testing and Exploitation

Purpose: To check hosts for known vulnerabilities and to see if they are exploitable, as well as to assess the potential severity of said vulnerabilities.

Methods:

- Remote vulnerability scanning (Nessus, OpenVAS)
- Active exploitation testing
- Login checking and bruteforcing
- Vulnerability exploitation (Metasploit, Core Impact)
- Oday and exploit discovery (Fuzzing, program analysis)
- Post exploitation techniques to assess severity (permission levels, backdoors, rootkits, etc)

Reporting

Purpose: To organize and document information found during the reconnaissance, network scanning, and vulnerability testing phases of a pentest.

Methods:

- Documentation tools (Dradis)
- Organizes information by hosts, services, identified hazards and risks, recommendations to fix problems

Report Writing

- Your report should be simple, clear, and understandable.
- Presentation of the report is also important. Headers, footers, appropriate fonts, well-spaced margins, etc., should be created/selected properly and with great care. For example, if you are using a red font for the heading, every heading in the document should be in that style.
- The report should be well organized.
- Correct spelling and grammar is important too. A misspelled word leaves a very negative impact upon the person who is reading your report. So, you should make sure that you proofread your report and perform spell-checks before submitting it to the client.

Understanding the Audience

Understanding the Audience

Understanding the audience that would be reading your penetration testing report is a very crucial part of the penetration test. We can divide the audience into three different categories:

1. Executive class
2. Management class
3. Technical class

Executive Class

This category includes the CEOs of the company. Since they have a very tedious schedule and most of the times have less technical knowledge, they would end up reading a very small portion of the report, specifically the executive summary, remediation report, etc.,

Management Class

Next, we have the management class, which includes the CISOs and CISSPs of the company.

Since they are the ones who are responsible for implementing the security policy of the company, they would probably be a bit more interested in reading about overall strengths and weaknesses, the remediation report, the vulnerability assessment report, etc.

Certified Information Systems Security Professional (CISSP)

chief information security officer (CISO)

Technical Class

This class includes the security manager and developers, who would be interested in reading your report thoroughly. They would investigate your report as they are responsible for patching the weaknesses found and for making sure that the necessary patches are implemented.

How to Become a Penetration Tester

How to Become a Penetration Tester

- Stay up to date on recent developments in computer security, reading newsletters and security reports are a good way to do this.
- Penetration Testing Certifications
 - Certified Ethical Hacker (CEH)
 - GIAC Certified Penetration Tester (GPEN)

Vulnerability Assessments versus Penetration Test

Vulnerability Assessments versus Penetration Test

Oftentimes, a vulnerability assessment is confused with a penetration test; however, these terms have completely different meanings.

- **In a vulnerability assessment**, our goal is to figure out all the vulnerabilities in an asset and document them accordingly.

Vulnerability Assessments versus Penetration Test

- **In a penetration test**, however, we need to simulate as an attacker to see if we are actually able to exploit a vulnerability and document the vulnerabilities that were exploited and the ones that turned out to be false-positive.

Vulnerability Assessments versus Penetration Test

Vulnerability assessment	Areas of Differences	Penetration testing
Discovery of weaknesses and vulnerabilities	Depth	Exploration of their depth and exploitation
Automated methods	Automation	Combined methods
Some security knowledge needed	Expertise	Requires specialization, expertise and know-how



Thank You