Pentesting Fundamentals

What is Penetration Testing?

Before teaching you the technical hands-on aspects of ethical hacking, you'll need to understand more about what a penetration tester's job responsibilities are and what processes are followed in performing pentests (finding vulnerabilities in a clients application or system).
The importance and relevancy of cybersecurity are ever-increasing and can be in every walk of life. News headlines fill our screens, reporting yet another hack or data leak.

Cybersecurity is relevant to all people in the modern world, including a strong password policy to protect your emails or to businesses and other organizations needing to protect both devices and data from damages.

A penetration test or pentest is an ethically-driven attempt to test and analyse the security defences to protect these assets and pieces of information. A penetration test involves using the same tools, techniques, and methodologies that someone with malicious intent would use and is similar to an audit.

According to Security Magazine, a cybersecurity industry magazine, there are over 2,200 cyber attacks every day - 1 attack every 39 seconds.

Penetration Testing Ethics

The battle of legality and ethics in cybersecurity, let alone penetration testing is always controversial. Labels like "hacking" and "hacker" often hold negative connotations, especially in pop culture, thanks to a few bad apples. The idea of legally gaining access to a computer system is a challenging concept to grasp -- after all, what makes it legal exactly?

Recall that a penetration test is an authorized audit of a computer system's security and defences as agreed by the owners of the systems. The legality of penetration is pretty clear-cut in this sense; anything that falls outside of this agreement is deemed unauthorized.

Before a penetration test starts, a formal discussion occurs between the penetration tester and the system owner. Various tools, techniques, and systems to be tested are agreed on. This discussion forms the scope of the penetration testing agreement and will determine the course the penetration test takes.

Companies that provide penetration testing services are held against legal frameworks and industry accreditation. For example, the National Cyber Security Centre (NCSC) has the CHECK accreditation scheme in the UK. This check means that only "[CHECK] approved companies can conduct authorized penetration tests of public sector and CNI systems and networks." (NCSC).

Ethics is the moral debate between right and wrong; where an action may be legal, it may go against an individual's belief system of right and wrong.

Penetration testers will often be faced with potentially morally questionable decisions during a penetration test. For example, they are gaining access to a database and being presented with potentially sensitive data. Or they are, perhaps, performing a phishing attack on an employee to test an organization's human security. If that action has been agreed upon during the initial stages, it is legal -- however ethically questionable.

Hackers are sorted into three hats, where their ethics and motivations behind their actions determine what hat category they are placed into. Let's cover these three in the table below:

Hat Category	**Description**	**Example**
White Hat	These hackers are considered the "good people". They remain within the law and use their skills to benefit others.	For example, a penetration tester performing an authorized engagement on a company.
Gray Hat	These people use their skills to benefit others often; however, they do not respect/follow the law or ethical standards at all times.	For example, someone taking down a scamming site.
Black Hat	These people are criminals and often seek to damage organizations or gain some form of financial benefit at the cost of others.	For example, ransomware authors infect devices with malicious code and hold data for ransom.

Rules of Engagement (ROE)
The ROE is a document that is created at the initial stages of a penetration testing engagement. This document consists of three main sections (explained in the table below), which are ultimately responsible for deciding how the engagement is carried out. The SANS institute has a great example of this document which you can view online here.

Section	Description
Permission	This section of the document gives explicit permission for the engagement to be carried out. This permission is essential to legally protect individuals and organizations for the activities they carry out.
Test Scope	This section of the document will annotate specific targets to which the engagement should apply. For example, the penetration test may only apply to certain servers or applications but not the entire network.
Rules	The rules section will define exactly the techniques that are permitted during the engagement. For example, the rules may specifically state that techniques such as phishing attacks are prohibited, but MITM (Man-in-the-Middle) attacks are okay.

****

Answer the questions below:

You are given permission to perform a security audit on an organization; what type of hacker would you be?
Answer: White Hat

You attack an organization and steal their data, what type of hacker would you be?
Answer: Black Hat

What document defines how a penetration testing engagement should be carried out?
Answer: Rules of Engagement

****

Penetration Testing Methodologies

Penetration tests can have a wide variety of objectives and targets within scope. Because of this, no penetration test is the same, and there are no one-case fits all as to how a penetration tester should approach it.

The steps a penetration tester takes during an engagement is known as the methodology. A practical methodology is a smart one, where the steps taken are relevant to the situation at hand. For example, having a methodology that you would

use to test the security of a web application is not practical when you have to test the security of a network.

Before discussing some different industry-standard methodologies, we should note that all of them have a general theme of the following stages:

Stage	Description
Information Gathering	This stage involves collecting as much publically accessible information about a target/organization as possible, for example, OSINT and research. Note: This does not involve scanning any systems.
Enumeration/Scanning	This stage involves discovering applications and services running on the systems. For example, finding a web server that may be potentially vulnerable.
Exploitation	This stage involves leveraging vulnerabilities discovered on a system or application. This stage can involve the use of public exploits or exploiting application logic.
Privilege Escalation	Once you have successfully exploited a system or application (known as a foothold), this stage is the attempt to expand your access to a system. You can escalate horizontally and vertically, where horizontally is accessing another account of the same permission group (i.e. another user), whereas vertically is that of another permission group (i.e. an administrator).
Post-Exploitation	This stage involves a few sub-stages: 1. What other hosts can be targeted (pivoting) 2. What additional information can we gather from the host now that we are a privileged user 3. Covering your tracks 4. Reporting

OSSTMM

The Open Source Security Testing Methodology Manual provides a detailed framework of testing strategies for systems, software, applications, communications and the human aspect of cybersecurity.

The methodology focuses primarily on how these systems and applications communicate, so it includes a methodology for:

1. Telecommunications (phones, VoIP, etc.)

2. Wired Networks
3. Wireless communications

Advantages	**Disadvantages**
Covers various testing strategies in-depth.	The framework is difficult to understand, very detailed, and tends to use unique definitions.
Includes testing strategies for specific targets (I.e. telecommunications and networking)	*Intentionally left blank.*
The framework is flexible depending upon the organization's needs.	*Intentionally left blank.*
The framework is meant to set a standard for systems and applications, meaning that a universal methodology can be used in a penetration testing scenario.	*Intentionally left blank.*

OWASP

The "Open Web Application Security Project" framework is a community-driven and frequently updated framework used solely to test the security of web applications and services.

The foundation regularly writes reports stating the top ten security vulnerabilities a web application may have, the testing approach, and remediation.

Advantages	**Disadvantages**
Easy to pick up and understand.	It may not be clear what type of vulnerability a web application has (they can often overlap).
Actively maintained and is frequently updated.	OWASP does not make suggestions to any specific software development life cycles.
It covers all stages of an engagement: from testing to reporting and remediation.	The framework doesn't hold any accreditation such as CHECK.
Specializes in web applications and services.	*Intentionally left blank.*

NIST Cybersecurity Framework 1.1

The NIST Cybersecurity Framework is a popular framework used to improve an organization's cybersecurity standards and manage the risk of cyber threats. This framework is a bit of an honourable mention because of its popularity and detail.

The framework provides guidelines on security controls & benchmarks for success for organizations from critical infrastructure (power plants, etc.) all through to commercial. There is a limited section on a standard guideline for the methodology a penetration tester should take.

Advantages	**Disadvantages**
The NIST Framework is estimated to be used by 50% of American organisations by 2020.	NIST has many iterations of frameworks, so it may be difficult to decide which one applies to your organisation.
The framework is extremely detailed in setting standards to help organisations mitigate the threat posed by cyber threats.	The NIST framework has weak auditing policies, making it difficult to determine how a breach occurred.
The framework is very frequently updated.	The framework does not consider cloud computing, which is quickly becoming increasingly popular for organisations.
NIST provides accreditation for organisations that use this framework.	*Intentionally left blank.*
The NIST framework is designed to be implemented alongside other frameworks.	*Intentionally left blank.*

NCSC CAF

The Cyber Assessment Framework (CAF) is an extensive framework of fourteen principles used to assess the risk of various cyber threats and an organisation's defences against these.

The framework applies to organisations considered to perform "vitally important services and activities" such as critical infrastructure, banking, and the likes. The framework mainly focuses on and assesses the following topics:

- Data security
- System security
- Identity and access control
- Resiliency
- Monitoring
- Response and recovery planning

Advantages	Disadvantages
This framework is backed by a government cybersecurity agency.	The framework is still new in the industry, meaning that organisations haven't had much time to make the necessary changes to be suitable for it.
This framework provides accreditation.	The framework is based on principles and ideas and isn't as direct as having rules like some other frameworks.
This framework covers fourteen principles which range from security to response.	*Intentionally left blank.*

****

Answer the questions below:

What stage of penetration testing involves using publicly available information?
Answer: Information Gathering

If you wanted to use a framework for pentesting telecommunications, what framework would you use? Note: We're looking for the acronym here and not the full name
Answer: OSSTMM

What framework focuses on the testing of web applications?
Answer: OWASP

****

Black Box, White Box, and Gray Box Penetration Testing

There are three primary scopes when testing an application or service. Your understanding of your target will determine the level of testing that you perform in your penetration testing engagement. In this task, we'll cover these three different scopes of testing.

Black-Box Testing
This testing process is a high-level process where the tester is not given any information about the inner workings of the application or service.

The tester acts as a regular user testing the functionality and interaction of the application or piece of software. This testing can involve interacting with the interface,

i.e. buttons, and testing to see whether the intended result is returned. No knowledge of programming or understanding of the programme is necessary for this type of testing.

Black-Box testing significantly increases the amount of time spent during the information gathering and enumeration phase to understand the attack surface of the target.

Grey-Box Testing
This testing process is the most popular for things such as penetration testing. It is a combination of both black-box and white-box testing processes. The tester will have some limited knowledge of the internal components of the application or piece of software. Still, it will be interacting with the application as if it were a black-box scenario and then using their knowledge of the application to try and resolve issues as they find them.

With Grey-Box testing, the limited knowledge given saves time, and is often chosen for extremely well-hardened attack surfaces.

White-Box Testing
This testing process is a low-level process usually done by a software developer who knows programming and application logic. The tester will be testing the internal components of the application or piece of software and, for example, ensuring that specific functions work correctly and within a reasonable amount of time.

The tester will have full knowledge of the application and its expected behaviour and is much more time consuming than black-box testing. The full knowledge in a White-Box testing scenario provides a testing approach that guarantees the entire attack surface can be validated.
****
Answer the questions below:

You are asked to test an application but are not given access to its source code - what testing process is this?
Answer: Black Box

You are asked to test a website, and you are given access to the source code - what testing process is this?
Answer: White Box
****

Practical: ACME Penetration Test

ACME has approached you for an assignment. They want you to carry out the stages of a penetration test on their infrastructure. View the site (by clicking the green button on this task) and follow the guided instructions to complete this exercise.

****

Answer the questions below:

Complete the penetration test engagement against ACME's infrastructure.

Answer: THM{PENTEST_COMPLETE}