Penetration Testing Overview

IT is an integral part of nearly every company. The amount of critical and confidential data stored in IT systems is constantly growing, as is dependence on the uninterrupted functioning of the IT systems in use. Therefore, attacks against corporate networks, disruption of system availability, and other ways of causing significant damage to a company (such as ransomware attacks) are becoming increasingly common. Important company information obtained through security breaches and cyber-attacks may be sold to competitors, leaked on public forums, or used for other nefarious purposes. System failures are deliberately triggered because they are increasingly difficult to counteract.

A `Penetration Test` (`Pentest`) is an organized, targeted, and authorized attack attempt to test IT infrastructure and its defenders to determine their susceptibility to IT security vulnerabilities. A pentest uses methods and techniques that real attackers use. As penetration testers, we apply various techniques and analyses to gauge the impact that a particular vulnerability or chain of vulnerabilities may have on the confidentiality, integrity, and availability of an organization's IT systems and data.

- `A pentest aims to uncover and identify ALL vulnerabilities in the systems under investigation and improve the security for the tested systems.`

Other assessments, such as a `red team assessment`, may be scenario-based and focus on only the vulnerabilities leveraged to reach a specific end goal (i.e., accessing the CEO's email inbox or obtaining a flag planted on a critical server).

Risk Management

In general, it is also a part of `risk management` for a company. The main goal of IT security risk management is to identify, evaluate, and mitigate any potential risks that could damage the confidentiality, integrity, and availability of an organization's information systems and data and reduce the overall risk to an acceptable level. This includes identifying potential threats, evaluating their risks, and taking the necessary steps to reduce or eliminate them. This is done by implementing the appropriate security controls and policies, including access control, encryption, and other security measures. By taking the time to properly manage the security risks of an organization's IT systems, it is possible to ensure that the data is kept safe and secure.

However, we can eliminate not every risk. There's still the nature of the inherent risk of a security breach that is present even when the organization has taken all reasonable steps to manage the risk. Therefore, some risks will remain. Inherent risk is the level of risk that is present even when the appropriate security controls are in place. Companies can accept, transfer, avoid and mitigate risks in various ways. For example, they can purchase insurance to cover certain risks, such as natural disasters or accidents. By entering into a contract, they can also transfer their risks to another party, such as a third-party service provider. Additionally, they can implement preventive measures to reduce the likelihood of certain risks occurring, and if certain risks do occur, they can put in place processes to minimize their impact. Finally, they can use financial instruments, such as derivatives, to reduce the economic consequences of specific risks. All of these strategies can help companies effectively manage their risks.

During a pentest, we prepare detailed documentation on the steps taken and the results achieved. However, it is the client's responsibility or the operator of their systems under investigation to rectify the vulnerabilities found. Our role is as trusted advisors to report vulnerabilities, detailed reproduction steps, and provide appropriate remediation recommendations, but we do not go in and apply patches or make code changes, etc. It is important to note that a pentest is not monitoring the IT infrastructure or systems but a momentary snapshot of the security status. A statement to this regard should be reflected in our penetration test report deliverable.

Vulnerability Assessments

`Vulnerability analysis` is a generic term that can include vulnerability or security assessments and penetration tests. In contrast to a penetration test, vulnerability or security assessments are performed using purely automated tools. Systems are checked against known issues and security vulnerabilities by running scanning tools like Nessus, Qualys, OpenVAS, and similar. In most cases, these automated checks cannot adapt the attacks to the configurations of the target system. This is why manual testing conducted by an experienced human tester is essential.

On the other hand, a pentest is a mix of automated and manual testing/validation and is performed after extensive, in most cases, manual information gathering. It is individually tailored and adjusted to the system being tested. Planning, execution, and selection of the tools used are much more complex in a pentest. Both penetration tests and other security assessments may only be carried out after mutual agreement between the contracting company and the organization that employs the penetration tester. This is because individual tests and activities performed during the pentest could be treated as criminal offenses if the tester does not have explicit written authorization to attack the customer's systems. The organization commissioning the penetration test may only request testing against its' own assets. If they are using any third parties to host websites or other infrastructure, they need to gain explicit written approval from these entities in most cases. Companies like Amazon no longer require prior authorization for testing certain services per this policy, if a company is using AWS to host some or all of their infrastructure. This varies from provider to provider, so it is always best to confirm asset ownership with the client during the scoping phase and check to see if any third parties they use require a written request process before any testing is performed.

A successful pentest requires a considerable amount of organization and preparation. There must be a straightforward process model that we can follow and, at the same time, adapt to the needs of our clients, as every environment we encounter will be different and have its own nuances. In some cases, we may work with clients who have never experienced a pentest before, and we have to be able to explain this process in detail to make sure they have a clear understanding of our planned activities, and we help them scope the assessment accurately.

In principle, employees are not informed about the upcoming penetration tests. However, managers may decide to inform their employees about the tests. This is because employees have a right to know when they have no expectation of privacy.

Because we, as penetration testers, can find personal data, such as names, addresses, salaries, and much more. The best thing we can do to uphold the Data Protection Act is to keep this information private. Another example would be that we get access to a database with credit card numbers, names, and CVV codes. Accordingly, we recommend that our customers improve and change the passwords as soon as possible and encrypt the data on the database.

Testing Methods

An essential part of the process is the starting point from which we should perform our pentest. Each pentest can be performed from two different perspectives:

- `External` or `Internal`

External Penetration Test

Many pentests are performed from an external perspective or as an anonymous user on the Internet. Most customers want to ensure that they are as protected as possible against attacks on their external network perimeter. We can perform testing from our own host (hopefully using a VPN connection to avoid our ISP blocking us) or from a VPS. Some clients will not care about stealth, while others will request that we proceed as quietly as possible and approach the target systems to avoid being banned by the firewalls and IDS/IPS systems and avoid triggering an alarm. They may ask for a stealthy or "hybrid" approach where we gradually become "noisier" to test their detection capabilities. Ultimately our goal here is to access external-facing hosts, obtain sensitive data, or gain access to the internal network.

Internal Penetration Test

In contrast to an external pentest, an internal pentest is when we perform testing from within the corporate network. This stage may be executed after successfully penetrating the corporate network via the external pentest or starting from an assumed breach scenario. Internal pentests may also access isolated systems with no internet access whatsoever, which usually requires our physical presence at the client's facility.

Types of Penetration Testing

No matter how we begin the pentest, the type of pentest plays an important role. This type determines how much information is made available to us. We can narrow down these types to the following:

Type	Information Provided
`Blackbox`	`Minimal`. Only the essential information, such as IP addresses and domains, is provided.
`Greybox`	`Extended`. In this case, we are provided with additional information, such as specific URLs, hostnames, subnets, and similar.
`Whitebox`	`Maximum`. Here everything is disclosed to us. This gives us an internal view of the entire structure, which allows us to prepare an attack using internal information. We may be given detailed configurations, admin credentials, web application source code, etc.
`Red-Teaming`	May include physical testing and social engineering, among other things. Can be combined with any of the above types.
`Purple-Teaming`	It can be combined with any of the above types. However, it focuses on working closely with the defenders.

The less information we are provided with, the longer and more complex the approach will take. For example, for a blackbox penetration test, we must first get an overview of which servers, hosts, and services are present in the infrastructure, especially if entire networks are tested. This type of recon can take a considerable amount of time, especially if the client has requested a more stealthy approach to testing.

Types of Testing Environments

Apart from the test method and the type of test, another consideration is what is to be tested, which can be summarized in the following categories:

Network	Web App	Mobile	API	Thick Clients
IoT	Cloud	Source Code	Physical Security	Employees
Hosts	Server	Security Policies	Firewalls	IDS/IPS

It is important to note that these categories can often be mixed. All listed test components may be included depending on the type of test to be performed. Now we'll shift gears and cover the Penetration Process in-depth to see how each phase is broken down and depends on the previous one.

Previous Next

Mark Complete & Next

Table of Contents

Using Academy Effectively
- Introduction to the Penetration Tester Path
- Academy Modules Layout
- Academy Exercises & Questions

Background & Preparation
- Penetration Testing Overview
- Laws and Regulations
- Penetration Testing Process

Penetration Testing Phases - Assessment Specific Stages
- Pre-Engagement
- Information Gathering
- Vulnerability Assessment
- Exploitation
- Post-Exploitation
- Lateral Movement

Penetration Testing Phases - Project Closeout
- Proof-of-Concept
- Post-Engagement

Preparing for Real-World Pentests
- Practice

My Workstation

OFFLINE

Start Instance

1 / 1 spawns left