FORTRA

A Simple Guide to Successful Penetration Testing

Table of Contents

Definition of Penetration Testing 03

History of Pen Testing 04

Assessing Your Security: The Benefits of Pen Testing 06

Putting on the White Hat: How to Become a Pen Tester 07

Rules of Engagement: Determining Your Pen Testing Scope 08

The 6 Stages of Penetration Tests 10

Conclusion 13

Glossary 14

The Five Ws of **Penetration Testing**

How effective are your existing security controls against a skilled adversary? The best way to find out is by running a penetration test. As this security practice becomes increasingly common, it can feel more difficult to ask, "what exactly is penetration testing?" This guide aims to not only answer this question, but to also explain how penetration testing began, who performs these assessments, why every organization benefits from them, and where to begin when incorporating penetration testing into your own security strategy.

Definition of **Penetration Testing**

A penetration test, often shortened to pen test, uses the same techniques as a hacker to assess of the security of an organization's IT environment. During these evaluations, security vulnerabilities are uncovered and safely exploited in order to determine and prioritize risk for the organization. Such vulnerabilities include unpatched devices, application flaws, misconfigurations, or even careless enduser behavior.

Penetration testing should also be defined in the context of what it is not. Penetration tests are often confused with vulnerability scans. Vulnerability scanners are automated tools that search for and report on which known vulnerabilities are present in an organization's IT infrastructure. Penetration tests continue the cybersecurity assessment by investigating if the vulnerability can be exploited, and the severity of that potential harm. Penetration tests also differ from Red Teaming, which is an offensive exercise which tests an organization's defenses by fully simulating a cyber-attack scenario. While all three of these practices are important to maintain security, the differences are worth noting.

Penetration testing is typically performed using a combination of manual and automated technologies to systematically compromise potential points of exposure. After an initial compromise, testers will often attempt to use the compromised device or system to launch subsequent exploits at other internal resources, ultimately trying to escalate their privileges to higher levels of security clearance and deeper access.

The end product of a penetration test is a report that shows where the infrastructure is vulnerable and prioritizes these vulnerabilities according to their level of risk. This gives organizations a path forward for remediation and provides proof of compliance for any industry best practices or regulations.

History of **Pen Testing**

At its core, penetration testing is simply thinking like an attacker. In this sense, the idea of penetration testing can be traced back to the fifth century B.C. In the military treatise attributed to Sun Tzu, *The Art of War*, it's written that "If you know the enemy and know yourself, you need not fear the result of a hundred battles."

When it comes to practice, pen testing has still been around for longer than you may expect. Since the 1960s, experts have been expressing the urgent need for prioritizing cybersecurity, recommending approaches like security testing. The brief timeline on the following page highlights key points in the development of modern penetration testing.

"IF YOU KNOW THE ENEMY AND KNOW YOURSELF, YOU NEED NOT FEAR THE RESULT OF A HUNDRED BATTLES."

SUN TZU, *THE ART OF WAR*

1964

01 A paper entitled "Program Management in Design and Development" is presented at the Third Annual Aerospace Reliability and Maintainability Conference, highlighting the idea of a Tiger Team, defined as "a team of undomesticated and uninhibited technical specialists, selected for their experience, energy, and imagination, and assigned to track down relentlessly every possible source of failure in a spacecraft subsystem or simulation."

1967

02 Renowned computer expert Willis Howard Ware presents "Security and Privacy in Computer Systems" at the Spring Joint Computer Conference, which touched upon the potential for individuals to hack into a network, even remotely.

1972

03 James Anderson is commissioned by the United States Airforce (USAF) to lead a Computer Security Technology Planning Study Panel. The subsequent two volume report included recommended security requirements, including suggestions for individuals or Tiger Teams testing systems for weaknesses and their ability to be penetrated.

1986

04 Penetration testing began to advance along with cyber-attacks throughout the 1980s, bringing about the passage of the Computer Fraud and Abuse Act. The ambiguous wording outlawing hacking "without authorization" presented issues to some ethical hackers over the coming years.

1992

05 The movie *Sneakers* brings wider awareness to the existence and practice of penetration testing.

1995

06 As modern penetration testing begins to emerge in the 1990s, cybersecurity researcher Dan Farmer and programmer Wietse Venema develop a vulnerability scanner, Security Administrator Tool for Analyzing Networks (SATAN), and publish a paper entitled "Improving the Security of Your Site by Breaking Into It".

2001

07 As more organizations become aware of cybersecurity risks, penetration testing tools develop further and become more commercially available.

2003

08 The first set of best practices for penetration testing are published by the Open Web Application Security Project (OWASP). The OWASP Web Security Testing Guide is still regularly updated and used today.

2009

09 A group of experts in the field of cybersecurity forms the Penetration Testing Execution Standard (PTES). This standard is made up of rules and guidelines that help businesses know what to expect and how to evaluate pen testing, should they conduct pen tests themselves or hire third-party services.

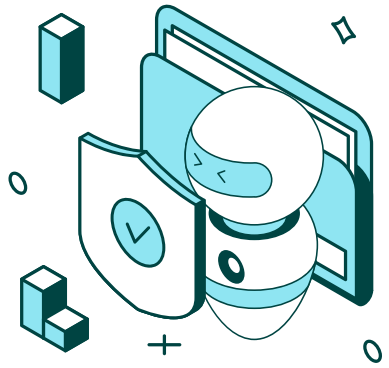
Today

10 Spending on enterprise security has exceeded $6 billion yearly and ondemand penetration testing is one of the standard methods to proactivel assess IT infrastructures.

Assessing Your Security:
The Benefits of Penetration Testing

When it comes to cybersecurity, ignorance is far from blissful—it can be dangerous and costly. Through penetration testing, you gain the visibility and insight needed to avert disaster. Pen tests empower you to proactively identify vulnerabilities before an attack occurs, giving you the chance to fix weaknesses and bolster your security.

While this summarizes the overall benefit of pen testing, there are many other advantages, including:



Intelligent Vulnerability Management

Vulnerability management programs aim to reduce risk and continually elevate the security of an IT environment by creating robust processes for identifying, classifying, remediating, and mitigating weaknesses in an IT environment. 62% of respondents to the 2023 Pen Testing Survey said a primary reason they pen tested was for vulnerability management support.

Adherence to Regulatory Requirements

Penetration testing helps organizations address regulatory requirements such as PCI-DSS, HIPAA, SOX, and GDPR. Reports from penetration reports allow you to illustrate ongoing due diligence to assessors, avoiding significant fines for non-compliance. In fact, 58% of respondents to the 2023 Pen Testing Survey said that a primary reason they pen tested was to help with compliance initiatives. Additionally 40% respondents listed internal or company specific mandates as a key reason for pen testing.

Avoiding the Costs of a Breach

Recovering from a security breach is costly in every sense of the word. In financial terms, organizations can end up paying thousands or millions of dollars to return to equilibrium. Operationally, a breach can dramatically affect productivity, sometimes even grinding the flow of business to a complete halt. And finally, breaches can severely damage or ruin the reputation of a business, making it difficult to retain customers and attract new ones. Penetration testing helps you reduce the risk of incidents that put your organization's finances, efficiency, and trustworthiness at stake by identifying and addressing risks before the attacks or security breaches occur.

Putting on the White Hat:
How to Become a Pen Tester

Cybersecurity experts are in short supply —according to the 2022 Cybersecurity Workforce Study by (ISC)2, there is a workforce gap of 3.4 million. Penetration testers are no exception. In fact, according to the 2023 Pen Testing Survey, internally hiring enough skilled personnel to perform pen tests (38%) and finding qualified third-parties (30%) were top challenges for penetration testing programs. While there are many reasons for the skills gap, a large factor is simply how challenging it is to become an expert.

So what does it take to become a pen tester? There isn't a pre-determined, required pathway, but penetration testers typically have a technical background in engineering, mathematics, physics, or computer science. Of course, there are exceptions, with many talented pen testers being completely self-taught. Additionally, pen testers often hold advanced certifications, like the Offensive Security Certified Professional (OSCP).

Certain personality traits lend themselves well to the profession. Someone who may thrive in the field is someone who can balance both being analytical and creative, giving them the ability to work through challenges effectively, even if it means thinking outside the box. They should also be patient and effective at managing frustration, as there is a lot of trial and error in the pen testing process.

However, this doesn't mean that experienced pen testers with advanced certifications are needed to run any type of pen test. Not every test requires an expert. Penetration testing tools that have automated features can be used by security team members who may not have an extensive pen testing background. These tools can be used for tests that are easy to run, but essential to perform regularly, like validating vulnerability scans, network information gathering, privilege escalation, or phishing simulations.

Even though there's a gap in the cybersecurity workforce, such tools can ensure that there isn't a gap in cybersecurity practices being implemented and they can help educate junior testers along the way.

Rules of Engagement: **Defining the Scope of a Penetration Test**

The scope of a penetration test should include what is tested, objectives, who will be involved in the testing process, and who needs to know a test is occurring. A common misconception of penetration tests is that each one tests an organization's entire infrastructure. This can sometimes make running a penetration test seem like too much of an undertaking—too costly and time consuming.

However, while some engagements of small businesses may be able to cover the whole IT environment, it's far more common to have a much narrower scope. In fact, too broad of a scope only allows pen testers to scratch the surface of a number of vulnerabilities, instead of gathering valuable intelligence gained by going more in-depth in fewer areas, with clear objectives in mind.

When determining the parameters of your penetration test, here are a few things to consider:

Objectives.

What insights are you hoping to gain from your pen test? If an outside attacker can get any sort of access? If an internal threat actor can escalate their privileges to root access? Getting a sense of your primary concerns can help lay the foundation for a well-defined engagement. Once this question is answered, it can help clarify both the type of access a pen tester should start out with, and what assets they should target.

Boundaries.

Where are the limits of where a penetration tester can go? There may be multiple reasons for why you want to draw lines that a tester should not cross. You may not want certain business areas disrupted, or there may be areas that are simply a low priority. Often, organizations run vulnerability scans to find out which areas are free of vulnerabilities, and which need further investigation.

Test Types.

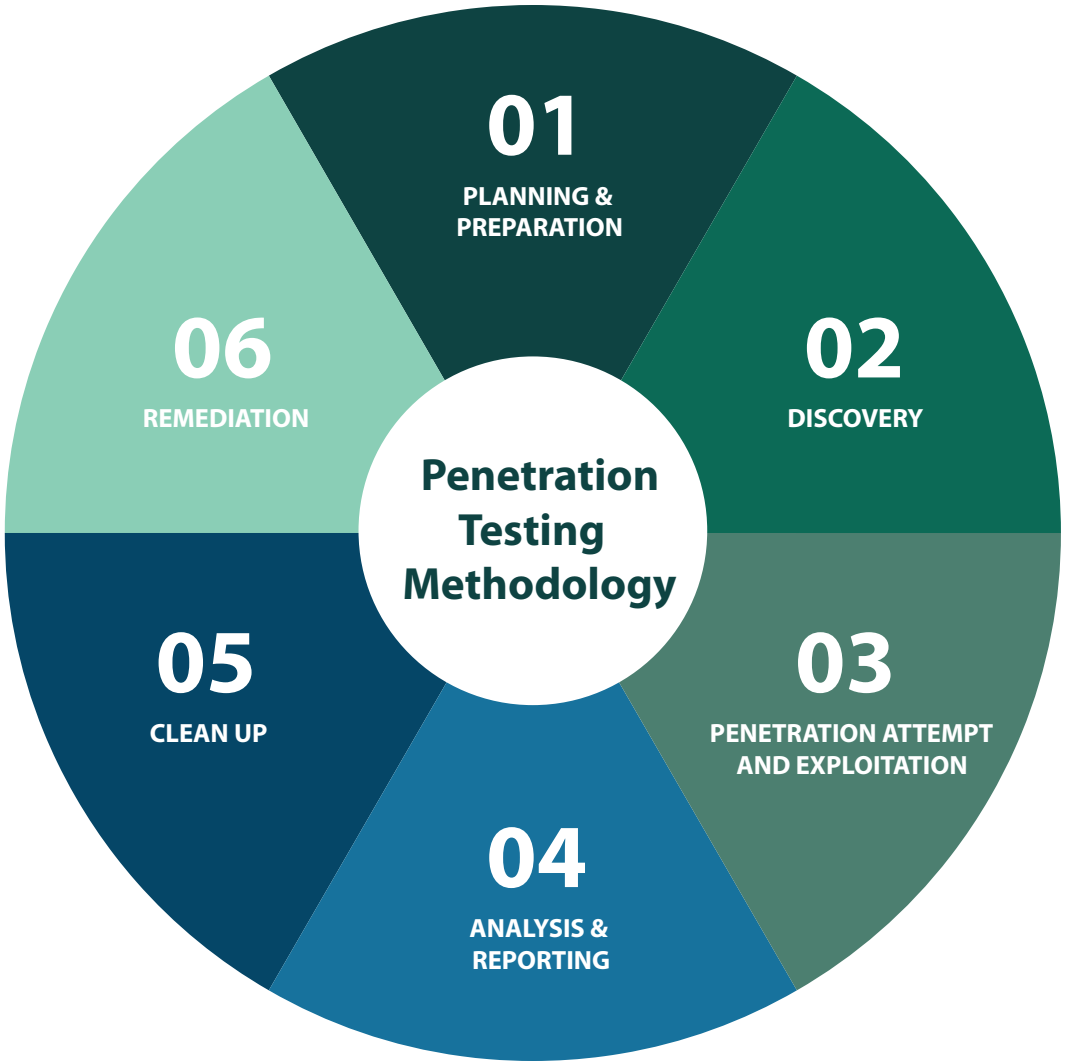
Once you have an idea of what assets you're concerned about, this can help determine what test types need to be run. Some of the most common ones include:

- **Network Security Tests** – These tests unveil vulnerabilities that could exist in your networks, as well as associated devices like routers, switches, and network hosts.
- **Web Application Tests** – These tests focus on the overall security and potential risks of web applications, including coding errors, broken authentication or authorization, and injection vulnerabilities.
- **Social Engineering Tests** – These tests show the security risk posed by employees within an organization by deploying phishing simulations, finding susceptible employees and evaluating the detection capabilities of defenses like spam filters.

Along the way, other questions may come up that can further refine your scope. Ultimately, taking the time to outline exactly what you want to get out of a penetration test ensures that you will get a complete picture of the security within the are you are testing, with an idea of what security controls are working, what is still needed, and what vulnerabilities should be fixed first.

The 6 Stages of a **Penetration Test**

A successful pen test is a multi-phased project that is both thorough and well thought out. While the scope of penetration tests often varies, the steps that should be followed for any engagement remain the same.



The 6 Stages of a **Penetration Test**

01 Planning and Preparation

As was discussed in the previous section, it is critical to determine and agree upon the scope of the test. The scope of a penetration test establishes what exactly will be tested and the objectives of that test. Talking through requirements and limitations explicitly defines the parameters of the process, which ensures that the engagement meets the needs of the organization.

02 Discovery

During this phase, reconnaissance is performed to gather as much information as possible on the target without actually exploiting it. This information can be used during the engagement to gain access or achieve other objectives. The type of information needed depends on the scope of the engagement. For example, an external pen test would require a way to gain initial access, while an internal pen test may instead be looking for ways that would help escalate privileges.

Additionally, approaches for the discovery phase vary, and techniques also depend on the vector being targeted (network, web, or client). However, most information gathering includes the use of automated tools to scan target assets for known vulnerabilities, which can then be investigated in depth.

03 Penetration Attempt and Exploitation

In order to determine risk, a pen test attempts to exploit vulnerabilities uncovered during the discovery phase. Sometimes, it's not possible to successfully exploit a seemingly critical vulnerability. On the other hand, a less severe vulnerability can be a crucial part of an attack chain which can launch subsequent exploits on other internal resources. Such chaining can end with gaining access to sensitive data or the capability to disrupt systems.

Penetration tests don't necessarily only put digital assets to the test. Organized social engineering campaigns with phishing emails can also be effective at gauging employee awareness, the impact of their behavior, and adherence to existing security controls.

The 6 Stages of a **Penetration Test**

04 Analysis and Reporting

Once exploitation is complete, the results should be examined, and conclusions should be written up in a report. The report should start with an overview of the penetration testing process, followed by an analysis of high-risk vulnerabilities. This analysis will also determine risk prioritization. Oftentimes, enough vulnerabilities are found that organizations may need to accept the risk incurred from less serious vulnerabilities to focus on fixing the most critical threats that could negatively impact business processes. The other contents of the report should include:

- Summary of successful penetration scenarios
- List of information gathered during penetration testing
- List and description of vulnerabilities found
- Detailed description of procedures
- Suggestions and techniques to resolve vulnerabilities

05 Clean Up

Though a detailed and exact list of actions performed during the penetration test should be recorded for the organization's report, it also benefits the penetration testers, by keeping track of what they have done during the test in order to clean up the environment once a test is complete. Compromised hosts should be restored to their original state, so that they don't negatively impact the organization's operations.

06 Remediation

Once clean up is completed, an organization can go about the business of addressing weaknesses according to the criticality of the vulnerability. This may include implementing patches, putting compensating controls in place to protect weaknesses that cannot be easily remediated, or even investing in new solutions that can streamline security and improve efficiency. It is also best practice to validate remediated vulnerabilities by re-testing to ensure they were properly mitigated.

Conclusion:
Incorporating Penetration Testing into Your Security Strategy

Organizations don't need to start out with a fully developed penetration testing program. Instead, they can start small, either incorporating basic tests with a pen testing tool or contracting a third-party, discussing which areas are the most essential in their consultation before the test begins. Once you have started incorporating penetration tests, the program can begin to evolve.

Most importantly, once you have started penetration testing, you should keep up the habit. One should think of a penetration test as the equivalent of a checkup with your doctor, or even maintaining your car. At first, it seems harmless to skip an appointment, but over time, problems can begin to accumulate, ultimately resulting in even bigger issues. Consistently testing the effectiveness of your security controls is vital to ensure that you can keep up with how an attacker might approach your organization. Ultimately, regular pen testing ensures your security improves over time and remains strong.

Glossary

As with all aspects of cybersecurity, there is a lot of jargon often thrown around when discussing penetration testing. While by no means a comprehensive list, here are a few key terms worth remembering.

Adversary – A person or group that intends to launch a cyber-attack against an IT infrastructure, for the purposes of stealing data, extorting money, or disrupting production. In an adversary simulation, a cybersecurity expert will emulate this role in order to test the strength of an environment's defenses.

Attack Chain – The act of pivoting from one attack into launching another in order to achieve a goal, typically for gaining control of the entire domain.

Exploit – An exploit is a piece of code that takes advantage of a known or unknown vulnerability located within an asset.

External Threat – The risk of an outside attack that begins outside of the security perimeter and is committed by an individual or group that is seeking to gain access to the environment's data or functionality.

Insider Threat – The risk of an attack initiated from inside the security perimeter, either purposefully or accidentally, by those that already have access of some kind, like an employee, contractor, or someone who has stolen credentials.

Patch – A release of changes to a computer program or its supporting data designed to fix bugs or other issues.

Phishing Simulation – A type of social engineering testing that imitates phishing campaigns. Pen testers deploy a number of phish emails of varying difficulty levels, and monitor whether any are opened, clicked, or have credentials entered.

Privilege Escalation – Typically achieved by exploiting a security weakness, the act of gaining additional access, resources, and control within a domain.

Remediation – Measures taken to correct or compensate for uncovered security weaknesses or vulnerabilities. Retest exploited systems after a penetration test to verify that remediation measures or compensating controls are effective and working.

Vulnerability – A weakness within an asset. Some vulnerabilities have the potential to be used by threat actors to gain access to an environment, or for some other malicious purposes. Not every vulnerability can be exploited.

Vulnerability Management Program – A comprehensive approach to the security stance of an entire infrastructure, often consisting of processes such as asset analysis, vulnerability scanning, penetration testing, patch management, and new process implementation.

FORTRA

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

fta-cs-gd-1023-r2-vm