GUIDE | **CYBERSECURITY**

Resultant

Vulnerability Assessments and Penetration Testing

A GUIDE TO UNDERSTANDING VULNERABILITY ASSESSMENTS AND PENETRATION TESTS.

Often used interchangeably, confusion about the difference between a vulnerability assessment and penetration test is prevalent. Understanding which test to undergo requires knowing what you need, the right questions to ask, and which test coincides with your answers.

CONTENTS

INTRODUCTION

When organizations begin developing a strategy to analyze their security posture, a vulnerability assessment or penetration test frequently tops the to-do list. Often used interchangeably, confusion about the difference between the two is prevalent.

Understanding the right activity to undertake and what to expect is a hurdle for many organizations. It requires knowing what you need, the right questions to ask, and which test coincides with your answers.

In this guide, we will discuss how to select the right security testing method to meet your goals by understanding the differences between a vulnerability assessment and a penetration test.

Security Testing 101 – Definitions

WHAT IS A VULNERABILITY ASSESSMENT?

A vulnerability assessment is the process of discovering, documenting, and quantifying the current security vulnerabilities found within an environment. A vulnerability assessment is intended to be a comprehensive evaluation of the security of your vital infrastructure, endpoints, and IT assets. It gives insight into system weaknesses and recommends the appropriate remediation procedures to either eliminate the issue or reduce the weakness to an acceptable level of risk.

Vulnerability assessments typically follow a structured methodology, which should include the:

- Identification and cataloging of assets (systems, infrastructure, resources, etc.) in an environment;
- Discovery and prioritization of the security vulnerabilities or potential threats to each asset; and
- Reporting on the recommended remediation or mitigation of vulnerabilities to reach an acceptable risk level.

WHAT IS A PENETRATION TEST?

A penetration test attempts to simulate the actions of an external or internal attacker who is trying to breach the information security of an organization. The individual performing the test uses a combination of tools and techniques and attempts to bypass the existing security controls of the target organization. The goal is to gain access to sensitive systems and information.

The methodology followed by penetration testers is inherently less structured to allow for rapid adjustment while testing the environment. However, most penetration methodologies typically follow these key steps:

- Determination of the scope and testing objectives;
- Targeted information gathering and reconnaissance;
- Identification and exploitation of weakness to gain and escalate access;
- Demonstrate completion of the testing objective; and
- Clean up and reporting.

Why Undergo a **Security Test?**

VULNERABILITY ASSESSMENT

The primary goal of a vulnerability assessment is to identify, catalog, and prioritize the population of vulnerabilities present within an environment. The intent is to remediate the identified issues to an acceptable risk level.

The objective of a vulnerability assessment focuses on creating a list of identified vulnerabilities and establishing a plan to remediate findings. Overall, the focus of the assessment is about breadth, rather than depth, identifying issues across the environment and prioritizing them for remediation based on multiple risk factors.

PENETRATION TESTING

The primary goal of a penetration test can be customized based on the organization and environment undergoing the test. A penetration test typically requires achieving some level of insider access in order to demonstrate control of a key system or asset on the internal network.

Penetration tests are robust as they simulate the activities of a real attacker and test an organization's current maturity levels within their security monitoring, network detection, access controls, and security response procedures. Overall, the focus of a penetration test is to demonstrate success against the testing objective. The testing objective could be breaching an organization's border security controls, gaining administrative rights to a key system, or even remaining active on the network for a period of time without detection by the organization's security team.

A SCENARIO: **PENETRATION TEST VERSUS VULNERABILITY ASSESSMENT**

Consider this non-technical scenario that demonstrates the primary difference between the two security tests:

> **Imagine a military General giving orders to one of his officers:**
>
> "Take the compound and save the hostage."
>
> The officer assembles his team, conducts reconnaissance of the compound and surrounding area, establishes a plan of action, and successfully executes the mission by breaching a weakness in a wall on the southern end of the compound.
>
> **Now imagine that during the debrief, the General asked about the security weaknesses and enemy activities on the northern end of the compound.**
>
> To the officer, this is an irrelevant question; the aim was not to assess the security weaknesses of the compound, the objective was to take the compound and save the hostage.

"Take the compound and save the hostage."

This scenario is a example of the difference between a penetration test (the officer's mission) and a vulnerability assessment (the General's follow up question). A penetration test will not attempt to identify all the vulnerabilities within the environment; the attacker will typically take the path of least resistance to avoid detection and complete the objective of the test.

Value and Timing
of Security Tests

As part of an organization's overall Threat and Vulnerability Management Program, both vulnerability assessments and penetration testing should be performed periodically to ensure the state of operations within an organization is continuously improving.

VULNERABILITY ASSESSMENT

Vulnerability assessments often provide the most value when used by organizations that do not have an in-house security team. An organization may recognize issues within its environment but is in need of outside technical expertise to identify and address the weaknesses. A vulnerability assessment can help organizations understand the problem and establish a plan to remediate the identified vulnerabilities.

PENETRATION TESTING

Penetration testing can provide an organization with a significant value as it relates to understanding the current state of its security operations. However, penetration tests require a higher level of security maturity to realize their full value. As a result, penetration testing should be conducted by an organization with at least a moderate level of maturity of its security operations. A moderate level of security encompasses an investment in security tools and processes and a team to manage its security operations. This level of maturity allows the organization to test not only the technical security of its environment, but its people, and the incident response procedures that support security operations.

Expected **Outcomes**

VULNERABILITY ASSESSMENT

A vulnerability assessment's core deliverables should include a technical report highlighting discovered vulnerabilities, their risk ranking, and recommended remediation activities. The report should also be accompanied by an executive summary to translate the results of the test into business-focused objectives for a non-technical audience.

A second primary deliverable should be a comprehensive list of the identified vulnerabilities in a matrix format. The document can be used by the organization to facilitate tracking and remediation of vulnerabilities discovered in the assessment.

VULNERABILITY ASSESSMENT COMMON DELIVERABLES:

- Technical Report
- Risk Ranking
- Remediation Activities
- Vulnerability Matrix

PENETRATION TESTING

A penetration test's core deliverables should include a targeted, technical report that focuses on narrating the path of the attacker, documenting vulnerabilities discovered as part of the assessment, and providing the organization with recommended remediation activities to prevent similar future attacks. The depth of the report depends on the methods of the attacker, how long it took to achieve the objective, and the systems compromised to complete the objective of the assessment.

PENETRATION TEST COMMON DELIVERABLES:

- Targeted Technical Report
- Remediation Activities

SUMMARY

If you are reading this and wondering who is responsible for security within your company, what tools you utilize to protect and monitor your environment, and what you would do in the event of a security incident, a vulnerability assessment is likely the right option for you.

Most organizations will achieve the highest return on investment by first conducting a vulnerability assessment to identify the current population of security issues within its environment. Once these matters have been remediated by the organization and the maturity level of security operations has increased; a penetration test can ensure the new environment is operating as expected.

	VULNERABILITY ASSESSMENT	PENETRATION TESTING
OVERVIEW	Automated vulnerability scanning coupled with manual analysis to validate and prioritize weaknesses.	Advanced, automated, and manual-testing techniques to identify and utilize weaknesses in the environment.
GOAL AND FOCUS	Creates a listing of validated, risk-ranked, and prioritized vulnerabilities within the environment to support remediation efforts. Discovers and documents as many vulnerabilities as possible. Focuses on breadth over depth.	Determines whether an organization's current level of security maturity can withstand an intrusion attempt from an advanced attacker with specific goals. Achievement of a specific testing goal (take control of an internal asset, demonstrate control of the network, gain physical access to a restricted area) by any means. Focuses on depth over breadth.
CLIENT MATURITY LEVEL	**Low to Medium.** The organization recognizes there are known issues in the environment and is looking for assistance in identification and remediation activities. There is awareness of the technical vulnerabilities present in the environment, with actionable remediation advice to address each weakness.	**High** The organization has established security teams, monitoring, and response procedures which would be assessed. Ultimately, the organization believes its defenses are strong and is looking to test that understanding. Assessment of the organization's current security maturity to prevent, identify, block, and respond to a real-life attack simulation.
DELIVERABLES	A comprehensive technical report that includes all identified vulnerabilities, risk rankings, and recommended remediation activities.	A targeted summary narrative that includes the successful attack vector and recommended remediation activities to close that attack vendor.

ABOUT RESULTANT

Our team believes solutions are more valuable, transformative, and meaningful when reached together. Through outcomes built on solutions rooted in data analytics, technology, and management consulting, Resultant serves as a true partner by solving problems with our clients, rather than for them.

Learn more about Resultant cybersecurity services.

VISIT **RESULTANT.COM.**