venza®
Better Visibility. Better Defense.

Pen Testing & Vulnerability Scanning

Quick Reference Guide

Version: 1.0

Revised: June 2023

Contents

Introduction

When it comes to assessing the security of an organization's systems and networks, two commonly used methods are **penetration testing ("pen testing")** and **vulnerability scanning**.

While they share the goal of identifying weaknesses in a system, they differ in their approaches and objectives. This guide aims to provide a quick reference to understand the difference between pen testing and vulnerability scanning.

Penetration Testing Defined

Pen testing, often referred to as ethical or "white hat" hacking, involves simulating real-world attacks on a system or network to identify vulnerabilities and determine the potential impact of these vulnerabilities.

Here are key points to understand:

- **Objective** – The primary goal of penetration testing is to exploit vulnerabilities and gain unauthorized access to systems or sensitive data to assess the level of risk and evaluate the effectiveness of security measures.
- **Approach** – Pen testers use various techniques, tools, and methodologies to mimic real-world attacks, simulating the actions of an actual attacker.
- **Scope** – Pen testing can be performed from both internal and external perspectives. Internal pen testing involves assessing the security measures within a network, such as servers and workstations. External pen testing evaluates the security of systems accessible from the internet, such as websites or cloud infrastructure.

A pen test may involve attempting to gain unauthorized access to the hotel's reservation system, manipulating guest bookings, or exploiting vulnerabilities in the hotel's Wi-Fi network to intercept guest data.

Vulnerability Scanning Defined

Vulnerability scanning is a process that identifies and reports potential vulnerabilities within a system or network. It focuses on detecting security weaknesses, misconfigurations, or outdated software versions.

Consider the following aspects:

- **Objective** – Vulnerability scanning aims to identify known vulnerabilities that could potentially be exploited by an attacker. It provides a snapshot of the system's security posture at a specific moment.
- **Approach** – Vulnerability scanners automate the process of scanning systems or networks to discover vulnerabilities by comparing them against a database of known vulnerabilities and weaknesses.
- **Scope** – Vulnerability scanning can be performed both internally and externally. Internal vulnerability scanning assesses the security posture of systems within the network, while external vulnerability scanning focuses on systems exposed to the internet, such as public-facing web servers.

In the hospitality industry, a vulnerability scan could involve scanning a hotel's network for outdated software versions, unpatched systems, or misconfigured firewalls that could potentially provide an entry point for an attacker.

Differences

Pen testing and vulnerability scanning have key differences in several areas. They are summarized in the table below.

Area	Pen Testing	Vulnerability Scanning
Actor	Human (ethical hackers).	Automated tools or scanners.
Depth	In-depth analysis to determine the impact of vulnerabilities and potential chain of exploitation.	Surface-level identification of vulnerabilities without detailed analysis of the impact.

Focus	Emphasizes security flaws and human-centric vulnerabilities.	Emphasizes technical vulnerabilities and misconfigurations.
Methodology	Systematic and targeted approach to exploit vulnerabilities, escalate privileges, and gain unauthorized access.	Uses predefined signatures and patterns to identify vulnerabilities.
Real-Time	Has evolving capability to identify new vulnerabilities that may not be detected by scanners.	Limited ability to identify new or zero-day vulnerabilities not included in the scanner's database.
Target	Systems, networks, and devices within the organization's infrastructure.	Systems, networks, web applications, and devices connected to the network or exposed to the internet.

Commonalities

While pen testing and vulnerability scanning have many differences, they share significant similarities. These commonalities include:

- **Helping organizations improve security posture**. Both assist organizations to enhance their overall security posture by identifying weaknesses that could be exploited by attackers. By addressing these issues, organizations mitigate potential threats and improve their defenses.
- **Contributing to a comprehensive security assessment strategy**. While pen testing focuses on actively exploiting vulnerabilities through simulated attacks, vulnerability scanning provides a systematic and automated approach to identifying known vulnerabilities. Together, they provide a more comprehensive understanding of an organization's security landscape.

- **PCI DSS Compliance**. Pen testing and vulnerability scanning are explicitly required by PCI DSS for organizations handling payment card data. Requirement 11.2 mandates regular internal and external vulnerability scans to identify potential vulnerabilities, and Requirement 11.2.1 states that organizations must perform quarterly external vulnerability scans by an Approved Scanning Vendor (ASV). Additionally, Requirement 11.3 requires organizations to perform pen testing annually or after significant changes to the network or applications.

- **Requiring periodic assessments**. Both pen testing and vulnerability scanning necessitate regular and periodic assessments to ensure ongoing security. The threat landscape is constantly evolving, with new vulnerabilities emerging and systems being updated. Regular assessments help organizations stay ahead of potential risks.

- **Assisting in vulnerability identification**. Both methods are effective in identifying vulnerabilities before they are exploited by malicious actors. Pen testing leverages various techniques to identify and exploit vulnerabilities, while vulnerability scanning uses automated tools and databases to detect known vulnerabilities.

- **Providing reports with suggested remediation**. Both produce reports outlining identified vulnerabilities and suggesting remediation steps. These reports provide insights into the specific vulnerabilities discovered and offer guidance on how to mitigate or eliminate them.

- **Requiring follow-up actions**. Both pen testing and vulnerability scanning may necessitate follow-up actions to address identified vulnerabilities. It is not sufficient to merely identify vulnerabilities; organizations must take steps to remediate and mitigate these risks. Follow-up actions may include applying patches, updating configurations, enhancing security controls, or implementing additional safeguards to address the identified vulnerabilities.

By leveraging these commonalities, organizations can utilize both pen testing and vulnerability scanning as complementary approaches to protect against threats.

Conclusion

Pen testing and vulnerability scanning are each essential components of a comprehensive security assessment strategy.

While penetration testing aims to mimic real-world attacks and exploit vulnerabilities to evaluate risk and security effectiveness, vulnerability scanning focuses on identifying known weaknesses and misconfigurations.

Both methods play crucial roles in proactively securing systems and networks, allowing organizations in the hospitality industry, such as hotels, to identify and address potential vulnerabilities before they are exploited by malicious actors.

About VENZA

VENZA is a leading provider of security awareness data protection solutions that empower the hospitality industry to mitigate vulnerabilities and ensure compliance. VENZA supports over 2000 hotels globally, keeping guests and their data safe from breaches with 360-degree visibility for proactive management of risks. This allows property managers to focus on guest service and building trust in their brand.

Visit www.VENZAGroup.com or www.CyberTekMSSP.com for additional details.

Contact Us

Sales: sales@venzagroup.com

Customer Success: success@venzagroup.com