# Vulnerability Scanning & Penetration Testing

## Essential Knowledge for Modern Business Leaders

By Ray Hutchins and Mitch
Tanenbaum Last updated: Feb 2023

**AI Statement:** This document was written by a human being ***and not AI***. While we may use AI for aspects of our research, we find that AI is (thus far) incapable of writing a document of this kind.

## Contents

## Overview

Understanding vulnerability scanning and penetration testing is important for business leaders because these technical security assessments play a critical role in protecting the security and integrity of an organization's systems and data and are required by a variety of regulations and laws. By identifying and mitigating vulnerabilities, these assessments help organizations reduce the risk of cyber attacks and minimize the impact of successful attacks.

Reasons why vulnerability scanning and penetration testing are important for business leaders:

1. **Risk mitigation**: Vulnerability scanning and penetration testing help organizations identify and prioritize areas of risk, allowing them to focus their resources on mitigating the most critical vulnerabilities.
2. **Compliance**: Some industries are required by law, contract or regulation to conduct regular security assessments, and failure to comply can result in significant fines, loss of contracts and reputational damage.
3. **Protecting sensitive information**: Vulnerability scanning and penetration testing help organizations identify and address potential threats to sensitive information, such as customer data and intellectual property.
4. **Maintaining business continuity**: By identifying and mitigating vulnerabilities, organizations can reduce the risk of data breaches and system disruptions, which can have a significant impact on business operations.
5. **Enhancing brand reputation**: Demonstrating a commitment to security can enhance an organization's brand reputation and build customer trust.
6. **Increasing company valuation**: Companies that secure their data are worth more than companies that do not. Please see our valuation position paper for more info.
7. Conducting these tests are likely required in order to obtain and maintain cyber risk insurance.

For business leaders who are responsible for risk reduction and company valuation, these tests help organizations ensure the security of their systems and data, meet regulatory requirements, and protect their bottom line.

## Differences Between Vulnerability Scanning and Penetration Testing

Vulnerability scanning and penetration testing are both security assessments that aim to identify weaknesses in a system, network, or application. However, there are several key differences between the two:

### Vulnerability scanning:

- Automated process that uses software to identify known vulnerabilities in a system, network or application.
- Usually fast and can cover a large number of system, device or application components.
- The results of a vulnerability scan can be used to identify potential security risks, but they do not provide information on the potential impact of a vulnerability. They do not attempt to compromise any systems or identify data which is at risk.

## Penetration testing:

- Involves automated plus manual testing performed by security experts who use a variety of techniques to attempt to ***exploit vulnerabilities*** in a system, network or application.
- More thorough and provides more information on the potential impacts of vulnerabilities.
- Takes more time and resources to perform than vulnerability scanning, so it costs more.

In conclusion, while vulnerability scanning is a useful tool for identifying potential vulnerabilities, it should not be relied upon as the sole method of security assessment. Penetration testing provides a more comprehensive evaluation of a system's security, but is typically more time-consuming and resource-intensive.

## What does a vulnerability scan include?

A vulnerability scan typically includes the following elements:

1. Target Discovery: The process of identifying all systems, devices, and applications on a network to be scanned.
2. Port Scanning: A technique used to identify open ports and services on target systems, which can indicate potential vulnerabilities.
3. Vulnerability Assessment: The process of using software or tools to identify known vulnerabilities in the systems and applications being scanned. This may include checking for missing security patches, misconfigured systems, or known exploits.
4. Threat Intelligence: The use of external information sources to gather information on known security threats and vulnerabilities.
5. Reporting: The production of a detailed report outlining the results of the vulnerability scan, including a list of all identified vulnerabilities, their severity, and recommended remediation steps.

The specific elements included in a vulnerability scan can vary depending on the type of scan being performed, the tools and software used, and the goals and objectives of the scan.

## What does a Pen Test Include?

A penetration test, also known as a pen test, typically includes the following elements:

1. Planning and Preparation: The process of defining the scope and objectives of the test, identifying the systems and applications to be tested, and obtaining necessary approvals and permissions.
2. Reconnaissance: The process of gathering information about the target systems and applications, including identifying open ports, services, and vulnerabilities.
3. Threat Modeling: The process of analyzing the information gathered during reconnaissance to identify potential attack vectors and determine the most likely methods of exploitation.
4. Exploitation: The process of attempting to exploit vulnerabilities in the target systems and applications to gain unauthorized access or elevate privileges.
5. Post-Exploitation: The process of gathering information and data from the target systems and applications after a successful exploitation.
6. Reporting: The production of a detailed report outlining the results of the penetration test, including a list of all identified vulnerabilities and their potential impact, and recommended remediation steps.

**NOTE**: Penetration testing can take many different forms and the specific elements included in a test can vary depending on the type of test being performed, the tools and techniques used, and the goals and objectives of the test.

## Difference Between a Network Penetration Test and a Web Application Penetration Test

A network penetration test and a web application penetration test are both forms of penetration testing, but they have different focuses and objectives:

### Network Penetration Test:

- Focuses on identifying vulnerabilities in a network infrastructure, such as servers, routers, switches, and firewalls.
- Tests the security of the network perimeter, internal network security, and network-level authentication and authorization systems.
- Aims to identify weaknesses that could allow an attacker to gain unauthorized access to sensitive data or compromise the network as a whole.

### Web Application Penetration Test:

- Focuses on identifying vulnerabilities in web-based applications, such as e-commerce sites, web portals, and web-based APIs.
- Tests the security of the application's code, the application server, and the database server.
- Aims to identify weaknesses that could allow an attacker to inject malicious code, steal sensitive data, access data in excess of the role’s permissions or compromise the application and its users.

In summary, both network penetration tests and web application penetration tests are important tools for improving the security of an organization's systems and data. The choice between the two depends on the specific security needs and goals of the organization, as well as the types of systems and applications in use.

## Difference Between an Internal Vulnerability Scan and An External Vulnerability Scan

An internal vulnerability scan and an external vulnerability scan are two types of security assessments that are used to identify security weaknesses in an organization's network. The main difference between these two scans is their *scope and focus*.

**Internal vulnerability** scans focus on identifying vulnerabilities within an organization's internal network and infrastructure, including servers, workstations, and other connected devices. **External vulnerability scans**, on the other hand, focus on identifying vulnerabilities in an organization's external network and infrastructure, such as web applications, internet-facing servers, and public-facing IP addresses.

These scans are typically conducted by security professionals, using tools and techniques designed to assess security from an internal or external perspective.

Both internal and external vulnerability scans are important components of a comprehensive security program and should be used together to get a complete picture of an organization's security posture.

## Difference Between an Internal Penetration Test and an external Penetration Test?

An internal penetration test and an external penetration test are both types of security assessments that are designed to identify and exploit vulnerabilities in an organization's network and systems. The main difference between these two tests is the scope and focus of the assessment.

An **internal penetration test** focuses on identifying vulnerabilities within an organization's *internal* network and infrastructure, including servers, workstations, and other connected devices. The objective of an internal penetration test is to simulate an attack by an attacker who has already gained access to an organization's internal network, either through a successful external attack or through internal means.

An **external penetration test** (sometimes referred to as a test of publicly facing or publicly exposed IP addresses) focuses on identifying vulnerabilities in an organization's *external* network and infrastructure. The objective of an external penetration test is to simulate an attack by an attacker who is outside of an organization's network, attempting to gain access through the organization's external perimeter.

Both internal and external penetration tests are important components of a comprehensive security program and should be used together to get a complete picture of an organization's security posture.

## What is a Mobile Device Penetration Test?

A mobile penetration test is a security assessment of mobile devices, such as smartphones and tablets, and the systems and applications that run on them. While we are calling it a “mobile device” test here, in reality, It can also be a test of IoT devices such as printers, cameras, security systems, appliances, etc. The objective of this testing is to identify and exploit vulnerabilities in the security of these devices and their associated systems. This type of test is designed to simulate an attack by a malicious actor, and to identify potential weaknesses in the security of mobile devices and the data they contain.

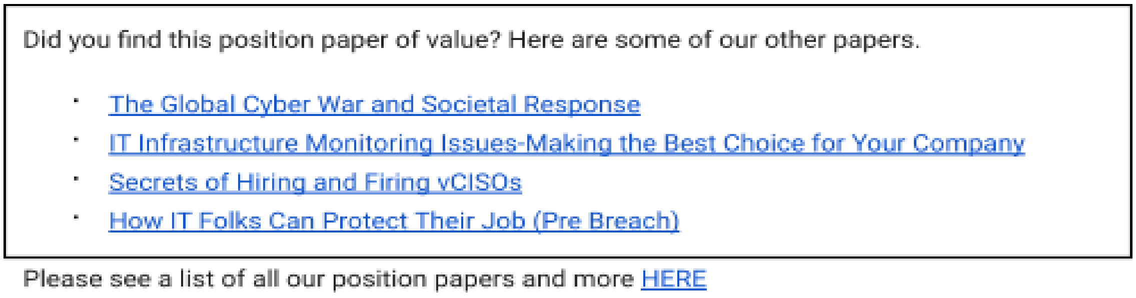
This type of penetration test can include a variety of techniques, such as network and application-layer testing, code analysis, and social engineering. The test may also include a review of the device's operating system and any installed applications, as well as any security measures that have been put in place, such as encryption and device-level authentication.

Mobile penetration testing is important for organizations that use mobile devices and other IT related equipment for business purposes, as these devices are often used to access sensitive information, including customer data and intellectual property. By identifying and mitigating vulnerabilities in mobile devices and their associated systems, organizations can reduce the risk of data breaches and protect against potential threats to their sensitive information.

## How We Can Help You

Our company provides a full range of vulnerability and penetration testing services. Over the years we have vetted and assembled a strong, trusted team of testers who are U.S. citizens and typically trained by the military. We can provide much more detail on how tests are performed, issues which are directly addressed, and pricing.

Please call or email us to learn more:
Raymond Hutchins
Mitch Tanenbaum
Partners
Turnkey Cybersecurity & Privacy Solutions, LLC
CyberCecurity, LLC
303-887-5864
rh@cybercecurity.com
mitch@cybercecurity.com



Did you find this position paper of value? Here are some of our other papers.

- The Global Cyber War and Societal Response
- IT Infrastructure Monitoring Issues-Making the Best Choice for Your Company
- Secrets of Hiring and Firing vCISOs
- How IT Folks Can Protect Their Job (Pre Breach)

Please see a list of all our position papers and more HERE

## About the Authors

Ray Hutchins and Mitch Tanenbaum own and operate two cybersecurity companies:

- CyberCecurity, LLC
- Turnkey Cybersecurity and Privacy Solutions, LLC

These are veteran-owned, mission-oriented companies providing defensive governance, strategic and operational guidance, and boots-on-the-ground support to organizations that acknowledge the cyberwar and are ready to actively support and engage in risk reduction and value creation.

Ray’s and Mitch’s wide range of cyberwar experiences with defending organizations all over the world and their ability to articulate this complex technical environment to leaders has established them as “global cyberwar” authorities. Please learn more about Ray and Mitch here:

https://www.cybercecurity.com/about/