VONAHI SECURITY
A Kaseya COMPANY

EBOOK

# The Network Penetration Testing Buyer's Guide

VONAHI SECURITY
A Kaseya COMPANY

# Table of **Contents**

# INTRODUCTION

Network security is paramount in the world of IT. However, cybercriminals are constantly innovating and looking for new ways to penetrate business networks to steal data or deploy ransomware. As businesses increasingly rely on digital infrastructure, safeguarding sensitive data and ensuring the integrity of network systems is vital.

That's why many organizations are choosing to do regular network penetration testing to locate and close security gaps before bad actors have the opportunity to exploit them.

This guide offers a comprehensive understanding of network penetration testing and insight into how to make a smart decision when choosing a network penetration testing solution. You will also learn about legal and ethical considerations around penetration testing and gain insight into other organizations' experiences from real-world case studies.

# UNDERSTANDING NETWORK PENETRATION TESTING

Network penetration testing, or pen testing, is sometimes referred to as ethical hacking.

In a network penetration test, testers simulate real-world cyberattacks to identify weaknesses in the network's defenses. The goal is to identify any problems and fix them before a real malicious hacker can take advantage. That's why it's considered the best way to evaluate security risks.

Network penetration testing has emerged as an essential tool to identify vulnerabilities & weaknesses in IT infrastructure before cybercriminals have the chance to exploit them.

# THE 8 MAIN TYPES OF PENETRATION TESTING

There are eight basic types of penetration testing to consider. A variety of factors can influence an organization's choice of the appropriate type of network penetration testing like the organization's specific goals, the level of knowledge available about the organization's network and the desired scope of the assessment. Many organizations employ a combination of these testing types to ensure a well-rounded evaluation of their network's security.

## 1. Black-box testing

**Objective:** In black-box testing, the tester has no prior knowledge of the network or system being tested. This simulates an external attacker's perspective.

**Methodology:** Testers perform the assessment without access to any internal documentation or system details. They rely on publicly available information & try to discover vulnerabilities just like a hacker would through reconnaissance & testing.

## 2. White-box testing

**Objective:** White-box testing is conducted with full knowledge of the network's architecture and system details. Testers aim to provide a comprehensive assessment of the network's security.

**Methodology:** Testers have access to internal network documentation, source code and system information. They can identify vulnerabilities more efficiently, making it useful for auditing, compliance and detailed security assessments.

## 3. Gray-box testing

**Objective:** Gray-box testing combines elements of both black-box and white-box testing. Testers have partial knowledge of the network, simulating an attacker with some insider information.

**Methodology:** Testers use a mix of external reconnaissance and internal system knowledge to assess the network. Gray-box testing is useful when an organization wants to test specific areas or systems while keeping some aspects unknown.

## 4. External testing

**Objective:** This type of testing focuses on assessing the security of the network and systems as they are exposed to the internet. It simulates attacks that originate from outside the organization's network perimeter and tries to uncover vulnerabilities that malicious actors might exploit to gain unauthorized access.

**Methodology:** Testers target the same devices, security measures and systems that a cybercriminal seeking entry from the web would, such as web servers, firewalls and VPNs, to identify vulnerabilities that could be exploited by an attacker without any internal access.

## 5. Internal testing

**Objective:** Internal testing evaluates the network's security from an insider's perspective, such as a disgruntled employee or a compromised system.

**Methodology:** Testers perform assessments from within the network, examining the security of internal systems, databases and applications. The goal is to identify vulnerabilities that could be exploited by someone with legitimate access.

## 6. Blind testing

**Objective:** Blind testing is designed to simulate the scenario of an external attacker with minimal information about the target network.

**Methodology:** Testers have limited knowledge about the network, and they need to gather information during the assessment. This type of testing helps evaluate the network's ability to detect and respond to unauthorized access attempts.

## 7. Targeted testing

**Objective:** Targeted testing concentrates on specific areas or systems within the network, often known to both the testers and the organization.

**Methodology:** Testers focus on specific vulnerabilities or systems that the organization is concerned about. It's typically more focused and efficient than broader assessments.

## 8. Full-scope testing

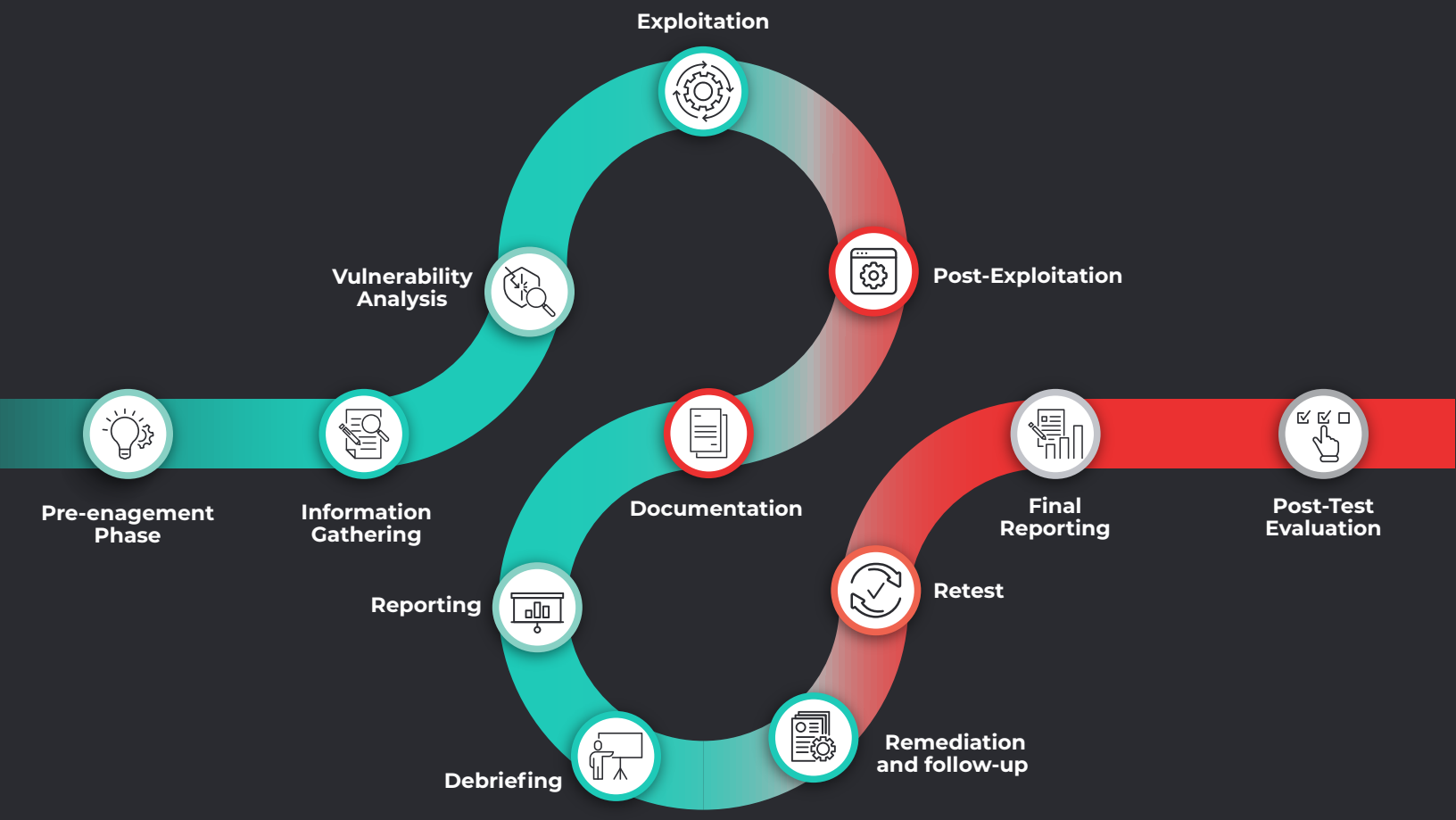
**Objective:** In full-scope testing, the assessment aims to cover the entire network, including all systems, applications and services.

**Methodology:** Testers perform a comprehensive evaluation, identifying vulnerabilities across the entire network. This type of testing is resource-intensive but provides a holistic view of the network's security.

# THE PENETRATION TESTING PROCESS

In network penetration tests, testers make multiple attempts to exploit security vulnerabilities with the ultimate goal of gaining access to data and systems. These attempts may include targeting patching deficiencies, authentication weaknesses, misconfigurations and even users (via man-in-the-middle attacks). After the testers score an initial compromise, they will then simulate the actions that bad actors might take like privilege escalation, lateral movement and enumeration of accessible resources to find sensitive data.

The process of a penetration test typically follows a structured methodology with several phases to ensure a thorough evaluation of an organization's cybersecurity defenses.

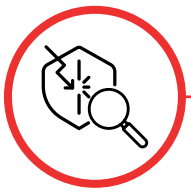


## PRE-ENGAGEMENT PHASE

- **Define scope:** Clearly define the scope of the penetration test, including determining which systems, networks and applications will be tested.
- **Set objectives:** Establish specific goals and objectives for the test, such as identifying vulnerabilities, assessing the effectiveness of security controls or testing incident response procedures. There may be several goals for a penetration test that can be accomplished together.
- **Obtain authorization:** Written authorization from the organization's management to conduct the test should be obtained to avoid any legal issues.

## INFORMATION GATHERING

- **Define scope:** Clearly define the scope of the penetration test, including determining which systems, networks and applications will be tested.
- **Set objectives:** Establish specific goals and objectives for the test, such as identifying vulnerabilities, assessing the effectiveness of security controls or testing incident response procedures. There may be several goals for a penetration test that can be accomplished together.
- **Obtain authorization:** Written authorization from the organization's management to conduct the test should be obtained to avoid any legal issues.



## VULNERABILITY ANALYSIS

- **Scan and enumeration:** At this stage, testers conduct scans and network enumeration to identify active hosts, services and potential vulnerabilities.
- **Vulnerability assessment:** Using automated tools and manual techniques, testers will aim to discover and assess vulnerabilities in systems and applications.

## EXPLOITATION

- **Attempt exploits:** Ethical hackers begin the test by attempting to exploit identified vulnerabilities and gaining unauthorized access to the designated systems or applications.
- **Escalation:** If initial access is achieved, testers may attempt to escalate privileges and gain deeper access within the environment.

## POST-EXPLOITATION

- **Maintain access:** TVesters may try to maintain access to the compromised system for further exploration.
- **Pivoting:** Testers may make lateral moves within the network to explore the vulnerabilities of other systems and assess the extent of a potential breach.

## DOCUMENTATION

- **Record findings:** The testers will carefully document all findings, including successful exploits, vulnerabilities, their severity and the steps taken to find them during the test.
- **Screenshots and logs:** Capturing screenshots and logs to provide evidence of successful compromises can help add context.

## REPORTING

- **Generate a detailed report:** A comprehensive report will be provided summarizing the test's findings, including a risk assessment, recommendations for mitigation and the potential impact of successful attacks.
- **Executive summary:** The report should also provide an executive-level summary of the findings for non-technical stakeholders.

## DEBRIEFING

- The testing team or representatives will connect with the organization's stakeholders to discuss the results of the test, answer questions and provide guidance on remediation steps.

## REMEDIATION AND FOLLOW-UP

- Testing experts will work with the organization to prioritize and address the vulnerabilities and weaknesses identified by the test.

## RE-TEST

- A company may choose to conduct follow-up tests to verify that vulnerabilities have been remediated effectively.

## FINAL REPORTING

- The company will be provided with a final report confirming the successful remediation of identified issues and a summary of the security improvements made.

## POST-TEST EVALUATION

- Conduct a post-test evaluation to assess the effectiveness of the penetration test process and identify areas for improvement.

# THE BENEFITS OF PENETRATION TESTING FOR IT INFRASTRUCTURE SECURITY

Network penetration testing is crucial for proactively identifying and mitigating security risks. It helps prevent data breaches and financial losses by fortifying an organization's defenses. Penetration tests allow organizations to assess their cybersecurity posture based on realistic attack scenarios. This enables them to address issues that could lead to a cyberattack or data breach if they followed a solely defensive approach to security.

**Network penetration testing offers businesses several benefits, including:**

- The opportunity to secure the environment and reduce exposure.
- Making it easy to prioritize the remediation of critical security weaknesses.
- Understanding how an attacker could gain access to sensitive data or systems.
- Meeting compliance and regulatory requirements.
- Testing and improving incident response procedures.
- Validating the effectiveness of security controls.
- Avoiding a costly security incident or data breach.
- Peace of mind gained from proactively addressing vulnerabilities.

# WHAT IS THE DIFFERENCE BETWEEN PENETRATION TESTING AND VULNERABILITY SCANNING?

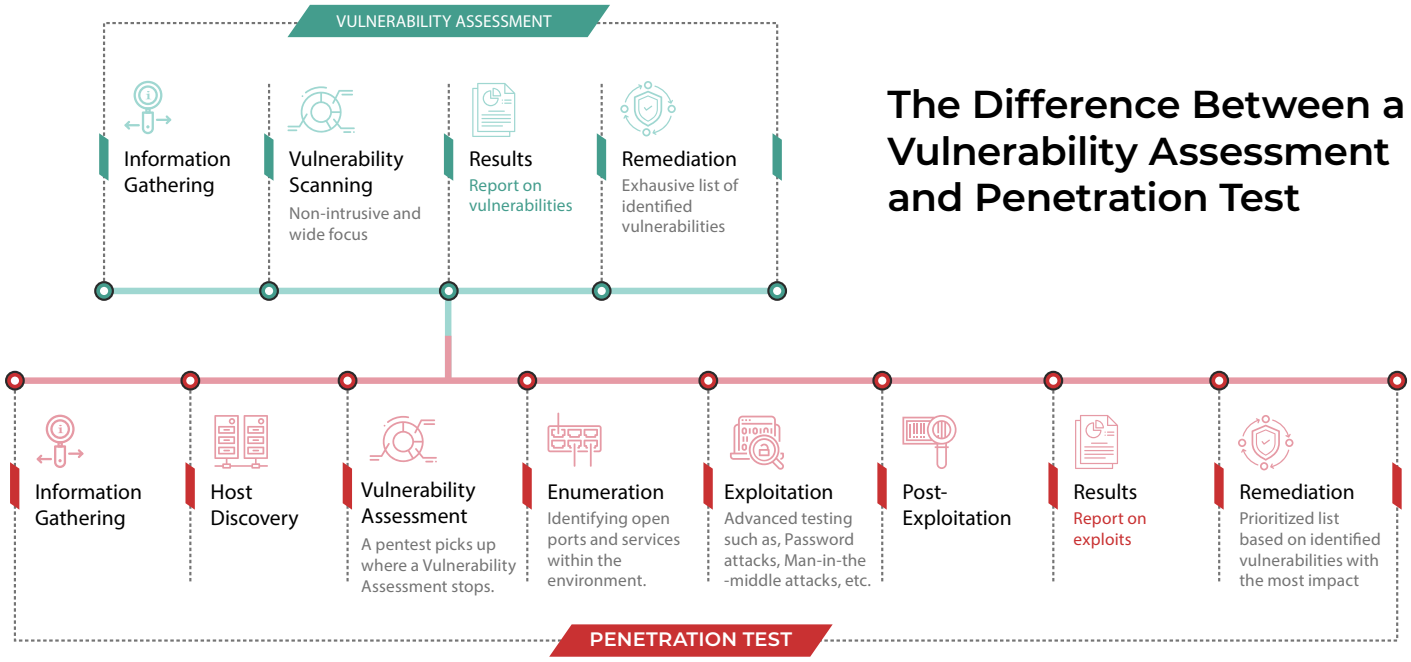
> Penetration testing and vulnerability scanning may sound similar, but they're not the same thing.

Vulnerability scanning is a more passive and automated process that identifies and lists known security vulnerabilities in a system or network. The primary purpose is to discover weaknesses in the target, without actively attempting to exploit them. It provides a snapshot of the system's security posture at a particular point in time.

Penetration testing is a proactive, simulated attack on a system or network to identify and exploit security vulnerabilities. It attempts to exploit vulnerabilities and provides tangible evidence of potential consequences. The primary goal of penetration testing is to determine the potential impact of a successful cyberattack and to help organizations understand how an attacker might breach their security, giving them insight into vulnerabilities that could lead to a genuine breach.

VONAHI SECURITY
A Kaseya COMPANY

# The Difference Between a Vulnerability Assessment and Penetration Test




| VULNERABILITY SCANNING | | PENETRATION TESTING |
|---|---|---|
| Identifying and prioritizing new known vulnerabilities | GOAL | Identifying unknown weaknesses and potential attack paths |
| Regularly scheduled (at least monthly) | FREQUENCY | Periodic. As needed or required |
| Finds internal and external vulnerabilities, misconfigurations, & system weaknesses, individual assets and applications | DEPTH | Simulates real-world attacks to show how vulnerabilities can be actively exploited and what's exposed |
| Non-intrusive<br>Starting point for testing security<br>Report on vulnerabilities<br>Use of security tools<br>Typically automated | APPROACH | Intrusive<br>Advanced security test<br>Report on exploits<br>Heavy use of security tools<br>Manual or automated |

# WHAT ARE THE MOST COMMON TYPES OF NETWORK PENETRATION TEST FINDINGS?

Penetration testing can reveal a wide range of security vulnerabilities and issues, and the findings will vary depending on the specific system, network or application being tested. However, some common pentest findings include:

**Weak or default passwords:** Penetration testers often discover weak, default or easily guessable passwords for user accounts, administrative access or critical systems.

**Unpatched software:** Outdated and unpatched software can lead to known vulnerabilities that attackers can exploit. This finding includes missing security patches and updates.

**Misconfigured security settings:** Improperly configured security settings, such as overly permissive access controls, misconfigured firewalls or unnecessary open ports can provide opportunities for attackers.

**Lack of encryption:** Failure to implement encryption for sensitive data in transit or at rest can expose data to eavesdropping or theft.

**Inadequate access control:** Weak access controls may allow unauthorized users to gain access to sensitive systems or data. This includes issues like missing or poorly configured authentication mechanisms.

**Egress Filtering Deficiencies:** Lack of egress filtering allows users to exfiltrate date to attacker-controlled servers on the public Internet.

**Buffer overflow vulnerabilities:** Buffer overflow issues can enable attackers to overwrite memory locations and potentially execute arbitrary code on a system.

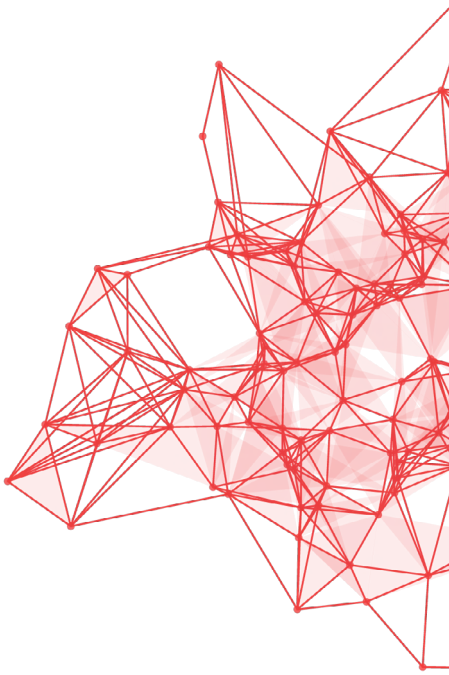
**Information disclosure:** This can include the exposure of sensitive information like system details, error messages or internal network configurations, which can aid attackers.

**Third-party vulnerabilities:** Dependencies on third-party libraries, frameworks or services may introduce vulnerabilities that can be exploited.

A penetration test will also reveal what attackers can actually do on the network once access has been obtained, such as what sensitive data they will be able to view. This is incredibly valuable information that organizations can obtain only through a penetration test.

**Cybercriminals will look for any vulnerability that they can exploit to sneak into a company's network. This includes some unexpected routes that would not be found by vulnerability scans like:**

- Shared local administrator credentials amongst workstations and servers.
- Weak Active Directory domain user account credentials as a result of a password-based attack.
- Disclosure of employee usernames and/or email addresses on devices like printers.
- Misconfigured all-in-one printers that contain privileged domain account credentials.
- Weak passwords amongst web services including printers, servers and remote management consoles.
- Misconfigured permissions associated with file shares and services, exposing sensitive data.



Using the results of a penetration test, IT professionals can identify ways to protect an organization's systems and data by reducing the number of attack vectors that cybercriminals can use to penetrate security.

VONAHI SECURITY
A Kaseya COMPANY

# 5 STEPS FOR ASSESSING AN ORGANIZATION'S PENETRATION TESTING NEEDS

Every organization's penetration testing needs are unique. These steps can help IT professionals ensure that they've taken the right steps to determine what their organization needs from a penetration testing solution.

## 1. Identify organizational goals and requirements

Define clear objectives for the test, like meeting compliance requirements, risk mitigation, improving incident response or overall security enhancement. There may be multiple objectives that can be achieved in the same test.

## 2. Assess network complexity and size for scalability

Determine the critical assets in your network, such as customer data, intellectual property, or financial information. Focus testing efforts on protecting these assets. The scalability of the chosen solution should match your network's complexity and size, especially if your organization is expanding.

## 3. Consider compliance and industry-specific regulations

Compliance is crucial. Ensure your chosen solution for penetration testing aligns with regulatory requirements in your industry, such as GDPR, HIPAA or PCI DSS.

## 4. Scope the testing engagement

Define the scope of your penetration testing project by specifying the systems, networks and applications to be tested. Clear scoping ensures a focused and effective assessment.

## 5. Set a budget and get quotes

Explore the cost factors associated with penetration testing, including initial testing, ongoing assessments and potential remediation costs. Weigh the cost-effectiveness of automated solutions against manual testing services. Request quotes from potential providers and compare them based on your budget and objectives.

> A small investment in a penetration testing solution now could lead to major savings and a major security boost down the road.

# EVALUATING NETWORK PENETRATION TESTING METHODS

In the ever-evolving landscape of network security, choosing the right network penetration testing solution or provider is very important. These factors should guide your decision.

### In-house vs. third-party testing

Decide whether to perform penetration testing in-house or hire a third-party provider. Consider factors like cost, expertise and objectivity. Advanced technology like automation makes it easy for businesses to save money by doing penetration testing in-house.

### Experience and certifications

Evaluate potential providers based on their qualifications, certifications and expertise in network penetration testing. Look for a provider with a proven track record. Seek references and case studies to gauge their capabilities.

### Testing methodologies and techniques

Evaluate the range of testing methodologies and techniques the provider employs to ensure thorough assessment and coverage. Ensure that the solution offers a wide range of testing methodologies, including external and internal assessments, to provide a holistic view of a network's security posture. It should cover vulnerabilities in systems, applications and configurations.

### Reporting and analysis

Comprehensive, easy-to-understand reporting is crucial for both accurately finding vulnerabilities and proving the value of testing to budget controllers. Look for detailed reports that clearly outline identified vulnerabilities, their severity and recommended remediation actions.

### Compliance alignment

Verify that the provider or solution aligns with industry standards and compliance requirements specific to the organization's sector. A network penetration testing solution should assist in meeting regulatory obligations and support your organization's compliance efforts.

### Ease of deployment

Streamlined deployment processes are essential. The solution should be user-friendly, easy to integrate with your existing network, and minimize operational disruptions.

### Ongoing support and guidance

Cyberthreats evolve rapidly, and bad actors discover and exploit new vulnerabilities every day. Choose a vendor or service provider with a reputation for innovation and excellent communication. This will ensure that they take a proactive approach in supporting and addressing emerging vulnerabilities and providing guidance to strengthen a company's network security over time.

The right penetration testing solution can significantly improve an organization's security posture. Although finding the right solution may seem like a daunting task, one penetration testing solution that offers all of the right features comes at a surprisingly affordable price.

# CASE STUDY
## W-Industries

Founded in 1984, W-Industries is a Texas-based leader in the energy industry specializing in control and safety systems. Cybersecurity is of paramount importance to the energy industry since it is a critical infrastructure sector that is often a target of threat actors and sabotage.

### The Challenge

Organizations like W-Industries face an ever-increasing tide of complex cybersecurity challenges in today's threat landscape, requiring frequent assessments of their cyber defenses. At the same time, the company uses many types of technology, complicating the testing process. For W-Industries, the whole process of manual penetration testing was cumbersome, alienating many non-technical staff members. Also, the glacial pace of traditional pen testing is time-consuming and expensive, which adds to the burden.

Commissioning a penetration test was a labor-intensive endeavor, requiring weeks, if not months, of vendor shopping and scheduling. The manual process involves a delay between a pen tester completing the testing and reporting on their findings, requiring a follow-up and leaving security gaps open for longer.

### The Solution

W-Industries considered their options for making the pen testing process smoother and faster, ultimately choosing the vPenTest platform. The platform could be installed in minutes and ready to begin testing immediately without hiring outside contractors.

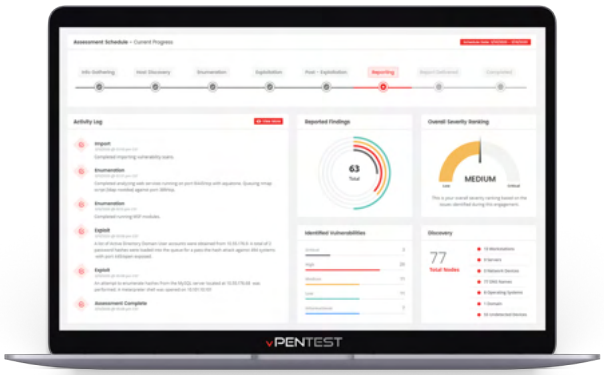
vPenTest's automatically generated, clear and detailed reports made it easy to demonstrate the company's risk and the value of testing to non-technical stakeholders. Third-party clients that allow W-Industries to host their content on-prem can trust that W-Industries maintains an excellent security posture via the reports vPenTest generates.

Best of all, the affordability and automated features made doing monthly pen tests easy, giving W-Industries a consistently accurate and comprehensive view of its security posture across all its digital assets. This gives W-industries an edge against cyberattacks, enabling the IT team to find and fix vulnerabilities before bad actors can exploit them.

"vPenTest helped us achieve a better security posture over our 20,000 hosts. The reports and the progress tracking vPenTest offers made it easier for us to secure cybersecurity insurance. Also, our customers felt more secure with our company as some of their resources existed in our tech infrastructure."

**IT Director**
W-Industries

# DISCOVER
## vPENTEST




**vPenTest is an automated network penetration testing tool that combines cutting-edge technology with ease of use. Some of its major advantages include:**

- The freedom to run internal and external network penetration testing on a monthly basis instead of annually to find and fix vulnerabilities before they become disasters.
- A cost savings of 50% compared to a traditional or manual network penetration test.
- Peace of mind knowing that vPenTest is backed by OSCP and OSCE-certified consultants with over 30 years of combined experience.


## LEARN MORE

Let us show you how easy it is to use our platform to proactively identify your risks to cyberattacks in real-time.

› Schedule a Demo

# HELLO WORLD.
# MEET AUTOMATED NETWORK PENTESTING.

VONAHI SECURITY
A Kaseya COMPANY


www.vonahi.io

info@vonahi.io

@vonahisec