VONAHI
SECURITY
A Kaseya COMPANY

2024 REPORT

Top 10 Critical Pentest Findings

HELLO WORLD.
Focus on what's most important.

In today's interconnected digital world, technological progress brings significant cybersecurity risks. CISOs and IT departments face the challenge of protecting their networks against an increasing array of cyber threats.

Cybercrime continues to increase by 15% year over year; the global annual cost of cybercrime is said to reach 8 trillion in 2023. By 2025 cybercrime will cost the entire world 10.5 trillion annually.

This is exactly why compliance and cyber insurance requirements have become significantly more demanding. The industry now recognizes that a mere vulnerability scan is insufficient; understanding the exact vectors through which attackers could infiltrate and exploit a network is paramount. Yet, standard penetration testing is often too manual, slow, infrequent (typically performed once a year), and expensive, particularly for SMBs. This makes it impractical for organizations to incorporate quality network penetration testing on a quarterly or monthly basis to meet security best practices.

At Vonahi Security, we're pioneering a paradigm shift in network penetration testing. Our vPenTest platform leverages automation to revolutionize this critical security service. This innovation not only slashes costs and streamlines processes but also enables monthly, real-time assessments of network vulnerabilities—without the necessity for additional staffing or outsourcing it to a 3rd party. In doing so, we empower organizations to stay a step ahead in the ever-evolving cybersecurity battleground.

After completing over 10,000 automated network pentests in 2023, Vonahi has identified the Top 10 Critical Internal Network Pentest Findings at over 1,200 organizations. We hope this resource can help your organization stay vigilant and one step ahead of the bad guys.

Alton Johnson
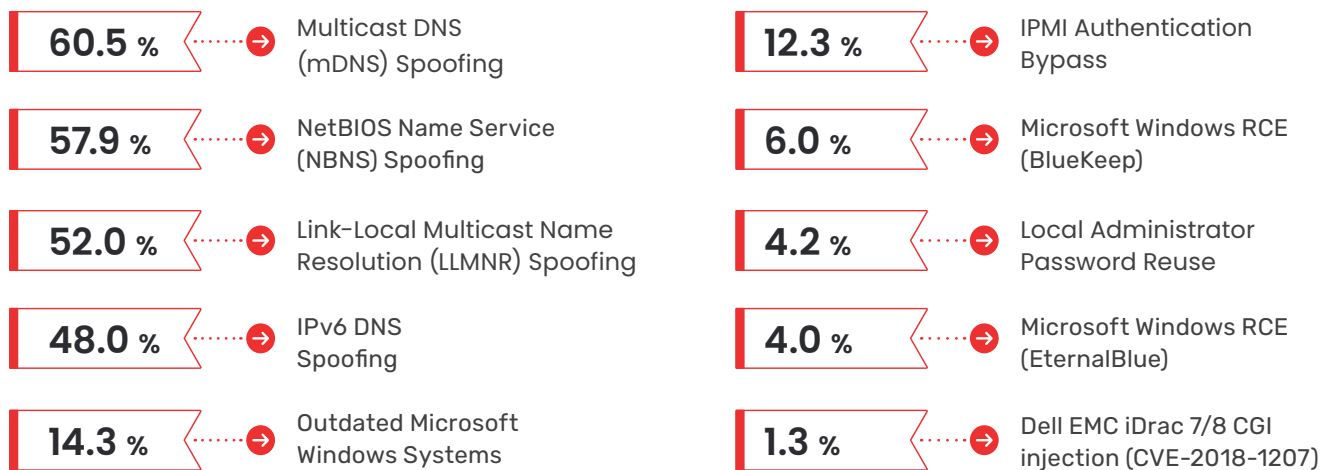Founder & Principal Security Consultant
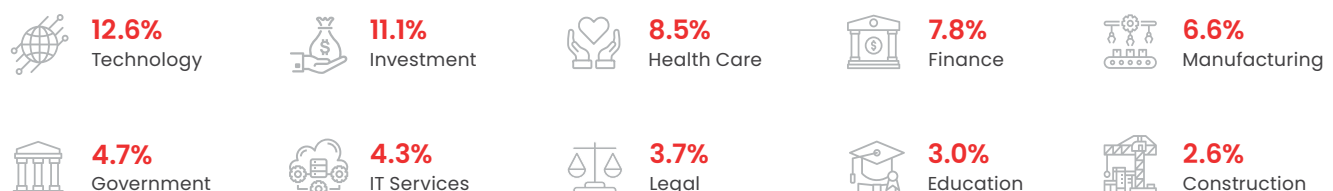Vonahi Security

Table of **Content**

OVERVIEW

Vonahi Security has provided over 10,000 organizations with a full-scale automated network penetration test since 2019 using our SaaS platform. This report shows the top 10 critical internal network pentest findings based on the most recent 3,000 security tests performed globally, as delivered by our vPenTest platform.

TOP 10 CRITICAL INTERNAL PENTEST FINDINGS BASED ON % OF OCCURRENCE

60.5 % → Multicast DNS (mDNS) Spoofing

57.9 % → NetBIOS Name Service (NBNS) Spoofing

52.0 % → Link-Local Multicast Name Resolution (LLMNR) Spoofing

48.0 % → IPv6 DNS Spoofing

14.3 % → Outdated Microsoft Windows Systems

12.3 % → IPMI Authentication Bypass

6.0 % → Microsoft Windows RCE (BlueKeep)

4.2 % → Local Administrator Password Reuse

4.0 % → Microsoft Windows RCE (EternalBlue)

1.3 % → Dell EMC iDrac 7/8 CGI injection (CVE-2018-1207)

TOP 10 CRITICAL INTERNAL PENTEST FINDINGS BY INDUSTRIES

12.6% Technology

11.1% Investment

8.5% Health Care

7.8% Finance

6.6% Manufacturing

4.7% Government

4.3% IT Services

3.7% Legal

3.0% Education

2.6% Construction

DEFINITIONS

PENTEST FINDINGS

The vulnerabilities that were successfully exploited by our automated pentesting platform, vPenTest, while performing an assessment in a non-disruptive manner on internal and external networks. PenTest findings will be referred to as "Findings" throughout the report.

THREAT SEVERITY RANKING

To assist organizations with prioritizing findings, the pentest findings and observations are categorized with threat severity rankings based on the Common Vulnerability Scoring System. The CVSS provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. CVSS is currently at version 3.1.

Severity	Description
Critical CVSS 9.0-10.0	A critical threat ranking requires immediate remediation or mitigation. Exploitation of these vulnerabilities typically require a minimal amount of effort by the adversary, but pose a significant threat to the confidentiality, integrity, and/or availability of the organization's systems and data. A successful compromise of findings of this ranking lead to access to multiple systems and/or several pieces of sensitive information.
High CVSS 7.0-8.9	A high threat ranking requires immediate remediation or mitigation. Exploitation of these vulnerabilities typically require a minimal amount of effort by the adversary, but pose a significant threat to the confidentiality, integrity, or availability of the organization's systems or data. A successful compromise of findings of this ranking lead to access to a single access or limited sensitive information.
Medium CVSS 4.0-6.9	A medium threat ranking requires remediation or mitigation within a short and reasonable amount of time. These findings typically lead to a compromise of non-privileged user accounts on systems and/or applications or denote a denial-of-service (DoS) condition of the host, service, or application.
Low CVSS 0.1-3.9	A low threat ranking requires remediation or mitigation once all higher prioritized findings have been remediated. These findings typically leak information to unauthorized or anonymous users and may lead to more significant attacks when combined with other attack vectors.
Informational CVSS 0	An information threat ranking does not pose a significant threat to the environment and may just be findings that could potentially disclose valuable information, but does not expose the organization to any technical attacks. Findings rated as informational may be useful for an attacker performing information gathering on the organization to leverage in other attacks, such as social engineering or phishing.

01 MULTICAST DNS (MDNS) SPOOFING

Multicast DNS (mDNS) is a protocol used within small networks to resolve a domain name system (DNS) name when a local DNS server does not exist.

When a system attempts to resolve a DNS name, the system proceeds with the following steps:

1. The system checks its local host file to determine if an entry exists to match the DNS name in question with an IP address.

2. On small networks where no DNS Server is configured, the system then uses mDNS to send an IP multicast query message to the systems on the local subnet that asks the host having that name to identify itself. Attackers can take advantage of this by answering this request and impersonating a system on the network.

RECOMMENDATIONS

➤ The most effective method for preventing exploitation is to disable mDNS altogether if it is not being used. Depending on the implementation, this can be achieved by disabling the Apple Bonjour or avahi-daemon service.

CVSS3.1: 9.8

SECURITY IMPACT

Since the mDNS queries are sent to systems on the local subnet, any system can respond to these queries with the IP address of the DNS name in question. This can be abused by malicious attackers since an attacker can respond to all of these queries with the IP address of the attacker's system. Depending on the service that the victim was attempting to communicate with (e.g. SMB, MSSQL, HTTP, etc.), an attacker may be able to capture sensitive cleartext and/or hashed account credentials. Hashed credentials can, many times, be recovered in a matter of time using computing modern-day computing power and brute-force techniques.

REFERENCES

Multicast DNS

REPRODUCTION STEPS

On a system configured with mDNS, attempt to interact with a DNS name that is known to be invalid (e.g. test123.local). On another system, use a network packet analyzer, such as Wireshark, to inspect the mDNS traffic on the internal network environment by filtering for UDP queries over port 5353.

02 NETBIOS NAME SERVICE (NBNS) SPOOFING

NetBIOS Name Service (NBNS) is a protocol used amongst workstations within an internal network environment to resolve a domain name system (DNS) name when a DNS server doesn't exist or can't be helpful.

When a system attempts to resolve a DNS name, the system proceeds with the following steps:

1. The system checks its local host file to determine if an entry exists to match the DNS name in question with an IP address.

2. If the system does not have an entry in its local hosts file, the system then sends a DNS query to its configured DNS server(s) to attempt retrieving an IP address that matches the DNS name in question.

3. If the configured DNS server(s) cannot resolve the DNS name to an IP address, the system then sends an NBNS broadcast packet on the local network to seek assistance from other systems.

CVSS3.1: 9.8

SECURITY IMPACT

Since the NBNS queries are broadcasted across the network, any system can respond to these queries with the IP address of the DNS name in question. This can be abused by malicious attackers since an attacker can respond to all of these queries with the IP address of the attacker's system. Depending on the service that the victim was attempting to communicate with (e.g. SMB, MSSQL, HTTP, etc.), an attacker may be able to capture sensitive cleartext and/or hashed account credentials. Hashed credentials can, many times, be recovered in a matter of time using modern-day computing power and brute-force techniques.

RECOMMENDATIONS

The following are some strategies for preventing the use of NBNS in a Windows environment or reducing the impact of NBNS Spoofing attacks:

➤ Configure the UseDnsOnlyForNameResolutions registry key in order to prevent systems from using NBNS queries (NetBIOS over TCP/IP Configuration Parameters). Set the registry DWORD to 1.

➤ Disable the NetBIOS service for all Windows hosts in the internal network. This can be done via DHCP options, network adapter settings, or a registry key.

REFERENCES

NTLM Challenge Response is 100% Broken (Yes, this is still relevant)

How to disable NetBIOS over TCP/IP by using DHCP server options

Disabling NetBIOS over TCP/IP Via Registry

NetBIOS over TCP/IP Configuration Parameters

REPRODUCTION STEPS

On a system configured with NBNS, attempt to interact with a DNS name that is known to be invalid (e.g. test123.local). On another system, use a network packet analyzer, such as Wireshark, to inspect the broadcasted traffic on the internal network environment.

03 LINK-LOCAL MULTICAST NAME RESOLUTION (LLMNR) SPOOFING

Link-Local Multicast Name Resolution (LLMNR) is a protocol used amongst workstations within an internal network environment to resolve a domain name system (DNS) name when a DNS server does not exist or cannot be helpful.

When a system attempts to resolve a DNS name, the system proceeds with the following steps:

1. The system checks its local host file to determine if an entry exists to match the DNS name in question with an IP address.

2. If the system does not have an entry in its local hosts file, the system then sends a DNS query to its configured DNS server(s) to attempt retrieving an IP address that matches the DNS name in question.

3. If the configured DNS server(s) cannot resolve the DNS name to an IP address, the system then sends an LLMNR broadcast packet on the local network to seek assistance from other systems.

SECURITY IMPACT

Since the LLMNR queries are broadcasted across the network, any system can respond to these queries with the IP address of the DNS name in question. This can be abused by malicious attackers since an attacker can respond to all of these queries with the IP address of the attacker's system. Depending on the service that the victim was attempting to communicate with (e.g. SMB, MSSQL, HTTP, etc.), an attacker may be able to capture sensitive cleartext and/or hashed account credentials. Hashed credentials can, many times, be recovered in a matter of time using modern-day computing power and brute-force techniques.

RECOMMENDATIONS

The most effective method for preventing exploitation is to configure the Multicast Name Resolution registry key in order to prevent systems from using LLMNR queries.

➤ **Using Group Policy:** Computer Configuration\Administrative Templates\Network\DNS Client \Turn off Multicast Name Resolution = Enabled (To administer a Windows 2003 DC, use the Remote Server Administration Tools for Windows 7)

➤ **Using the Registry for Windows Vista/7/10 Home Edition only:** HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\ Windows NT\DNSClient \EnableMulticast

REFERENCES

Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay

REPRODUCTION STEPS

On a system configured with LLMNR, attempt to interact with a DNS name that is known to be invalid (e.g. test123.local). On another system, use a network packet analyzer, such as Wireshark, to inspect the broadcasted traffic on the internal network environment.

04 IPV6 DNS SPOOFING

IPv6 DNS spoofing is possible due to the possibility of deploying a rogue DHCPv6 server on the internal network. Since Microsoft Windows systems prefer IPv6 over IPv4, IPv6-enabled clients will prefer to obtain IP address configurations from a DHCPv6 server when one is available.

During an attack such as the one performed during this assessment, an IPv6 DNS server was assigned to IPv6-enabled clients; however, the IPv6-enabled clients retained their pre-existing IPv4 address configurations - IP address, default gateway, and subnet mask.

RECOMMENDATIONS

Disable IPv6 unless it is required for business operations. As disabling IPv6 could potentially cause an interruption in network services, it is strongly advised to test this configuration prior to mass deployment. An alternative solution would be to implement DHCPv6 guard on network switches. Essentially, DHCPv6 guard ensures that only an authorized list of DHCP servers are allowed to assign leases to clients.

CVSS3.1: 10.0

SECURITY IMPACT

By deploying a rogue DHCPv6 server, an attacker is able to intercept DNS requests by reconfiguring IPv6-enabled clients to use the attacker's system as the DNS server. Such an attack could potentially lead to the successful capture of sensitive information, including user credentials and other information. Resolving all DNS names to an attacker's system results in the victim's system communicating with services such as SMB, HTTP, RDP, MSSQL, etc. all hosted on the attacker's system.

REFERENCES

Taking Over IPv6 Networks

REPRODUCTION STEPS

Leveraging the "mitm6" tool within Kali Linux, a user is able to quickly deploy a DHCPv6 server within the local network and assign five minute leases (by default) to IPv6-enabled clients.

05 OUTDATED MICROSOFT WINDOWS SYSTEMS

An outdated Microsoft Windows system raises several concerns as the system is no longer receiving updates by Microsoft. This could be a prime target for an attacker as these systems typically do not contain the latest security updates, oftentimes leaving them vulnerable to significant threats.

RECOMMENDATIONS

Replace outdated versions of Microsoft Windows with operating systems that are up-to-date and supported by the manufacturer.

REPRODUCTION STEPS

Use an operating system identification scanner, such as Nmap or Metasploit, to scan the affected targets to identify their specific versions. Alternatively, a network administrator can check the operating system version by logging into the system and viewing the operating system version through the system properties.

CVSS3.1: 9.8

SECURITY IMPACT

An exploited Microsoft Windows system could potentially result in an attacker gaining unauthorized access to the affected system(s). Additionally, depending on the similarities in configurations between the compromised system(s) and other systems within the network, an attacker may be able to pivot from this system to other systems and resources within the environment.

REFERENCES

Update Software - Techniques Addressed by Mitigation

What does it mean if Windows isn't supported?

06 IPMI AUTHENTICATION BYPASS

Intelligent Platform Management Interface (IPMI) is a hardware solution that allows network administrators to centrally control and manage servers. When setting up a server with IPMI, some servers may contain vulnerabilities that allow for an attacker to remotely bypass the authentication process, resulting in extracting the password hash. In some cases, an attacker may also be able to identify the cleartext password if the hash if the password is still default or weak.

CVSS3.1: 10.0

SECURITY IMPACT

By extracting the cleartext password, an attacker may be able to gain remote access to the service. This access may be to the service's Secure Shell (SSH), Telnet, or even web interfaces. Successful access could result in the manipulation of configurations that may negatively impact the availability of services provided by the compromised server.

RECOMMENDATIONS

Since there is no patch available for this particular vulnerability, it is recommended to perform one or more of the following actions.

➤ Restrict IPMI access to a limited number of systems - systems which require access for administration purposes.

➤ Disable the IPMI service if it is not required for business operations.

➤ Change the default administrator password to one that is strong and complex.

➤ Only use secure protocols, such as HTTPS and SSH, on the service to limit the chances of an attacker from successfully obtaining this password in a man-in-the-middle attack.

REFERENCES

What Is IPMI And Why You Should Care

IPMI Cipher Suite Zero Authentication Bypass

IPMI Cipher Zero Vulnerability: Finding and Fixing

REPRODUCTION STEPS

Leveraging the Metasploit framework, configure and run the following module against the affected service:.

➤ auxiliary/scanner/ipmi/ipmi_dumphashes

07 MICROSOFT WINDOWS RCE (BLUEKEEP)

During testing, systems were identified that are vulnerable to CVE-2019-0708 (BlueKeep), which is a vulnerability that exists in Microsoft Windows systems. This vulnerability is extremely valuable to an attacker due to the availability of tools and code that could take advantage of this weakness. Successful exploitation of this vulnerability typically results in full access to the exploited system(s).

RECOMMENDATIONS

It is recommended to apply security updates on the affected system. Furthermore, the organization should evaluate its patch management program to determine the reason for the lack of security updates. As this vulnerability is a commonly exploited vulnerability and could result in significant access, it should be remediated immediately.

REPRODUCTION STEPS

➤ Using a tool such as Metasploit, use the following module: **exploit/windows/rdp/cve_2019_0708_bluekeep_rce**

Provide the necessary IP address information about the source and target, and type "exploit" to launch the exploit. It should be noted that exploitation of this issue could potentially cause an impact on the availability of the remote system.

CVSS3.1: 9.8

SECURITY IMPACT

By exploiting the BlueKeep vulnerability, an attacker could gain full control over the affected system. This typically leads to additional attacks within the organization, including extraction of cleartext passwords and hashes, along with lateral movement within the network. Since exploitation of this vulnerability does not require privilege escalation on the affected system, an attacker would typically have as much access as they need on the compromised system to start enumerating the system.

REFERENCES

Remote Desktop Services Remote Code Execution Vulnerability

08 LOCAL ADMINISTRATOR PASSWORD REUSE

CVSS3.1: 9.0

As part of the internal penetration test, it was found that many systems have the same local administrator password. This was confirmed by successfully compromising a local administrator account and discovering its access across a number of systems within the internal network environment.

SECURITY IMPACT

Using the same local administrator credentials across multiple systems significantly increases the chances of a successful and widespread compromise within the organization. If an attacker successfully compromises the credentials to one of the affected systems, then they essentially have local administrator privileges across multiple other systems within the environment. This level of access across a number of systems could lead to a significant compromise of systems and resources within the environment.

RECOMMENDATIONS

Use a solution such as Microsoft Local Administrator Password Solution (LDAPS) to ensure that the local administrator password across multiple systems are not consistent.

REPRODUCTION STEPS

Using the compromised user account credentials, attempt to login to multiple systems.

REFERENCES

Microsoft security advisory: Local Administrator Password Solution (LAPS) now available

09 MICROSOFT WINDOWS RCE (ETERNALBLUE)

CVSS3: 9.8

During testing, systems were identified that are vulnerable to MS17-010 (EternalBlue), which is a vulnerability that exists in Microsoft Windows systems. This vulnerability is extremely valuable to an attacker due to the availability of tools and code that could take advantage of this weakness. Successful exploitation of this vulnerability typically results in full access to the exploited system(s).

SECURITY IMPACT

By exploiting the EternalBlue vulnerability, an attacker could gain full control over the affected system. This typically leads to additional attacks within the organization, including extraction of cleartext passwords and hashes, along with lateral movement within the network. Since exploitation of this vulnerability does not require privilege escalation on the affected system, an attacker would typically have as much access as they need on the compromised system to start enumerating the system.

RECOMMENDATIONS

It is recommended to apply security updates on the affected system. Furthermore, the organization should evaluate its patch management program to determine the reason for the lack of security updates. As this vulnerability is a commonly exploited vulnerability and could result in significant access, it should be remediated immediately.

REFERENCES

Microsoft Security Bulletin MS17-010 - Critical

REPRODUCTION STEPS

➤ Leveraging a tool such as Metasploit, use the *smb_ms17_010* module to scan for this vulnerability.

10 DELL EMC IDRAC 7/8 CGI INJECTION (CVE-2018-1207)

CVSS3.1: 9.8

Dell EMC iDRAC7/iDRAC8 is running a version prior to 2.52.52.52, making it vulnerable to a command injection issue tracked as CVE-2018-1207.

SECURITY IMPACT

The vulnerability allows unauthenticated attackers to execute commands with root privileges, thereby giving them complete control over the iDrac device.

RECOMMENDATIONS

Upgrade the firmware to the latest possible version.

REFERENCES

Dell EMC iDRAC Response to Common Vulnerabilities and Exposures CVE-2018-1207, CVE2018-1211, and CVE-2018-1000116 [20 March 2018]

REPRODUCTION STEPS

➤ Log into the iDRAC web interface

➤ Go to **Overview** > **iDRAC Settings** > **Update and Rollback**. The **Firmware Update** page is displayed.

➤ Click on the **Update** tab. The firmware version is now displayed. Only versions prior to 2.52.52.52 are vulnerable.

ANALYSIS

We have observed that the root cause of critical pentest findings continue to be configuration weaknesses and patching deficiencies. Most concerningly, the top 3 findings, **identified for over half of all assessments**, are capable of completely bypassing an organization's security, using off the shelf tools and simple techniques that are undetectable by most IT teams.

CONFIGURATION WEAKNESSES

Configuration weaknesses are typically due to improperly hardened services within systems deployed by administrators, and contain issues such as weak/default credentials, unnecessarily exposed services or excessive user permissions. Although some of the configuration weaknesses may be exploitable in limited circumstances, the potential impact of a successful attack will be relatively high.

PATCHING DEFICIENCIES

Patching deficiencies still prove to be a major issue for organizations and are typically due to reasons such as compatibility and, oftentimes, configuration issues within the patch management solution. Successful access may lead to confidential data and/or systems

Attackers take advantage of these configuration and patching deficiencies by leveraging many publicly available tools that require a relatively low level of knowledge to execute. These exploited weaknesses typically result in limited or escalated privileges within environments and usually lead to gaining unauthorized access to many critical areas within an organization.

> These two major issues alone prove the need for frequent penetration testing. While once-a-year testing has been the usual approach for penetration testing, ongoing testing provides a significant amount of value in identifying significant gaps closer to real-time.

Vulnerability scanning is also a fairly routine assessment within many organizations, but these solutions lack the ability to provide the organization with a true understanding of how security risks can be used to establish a significant compromise. For example, Tenable's Nessus scanner correctly identifies the existence of LLMNR in an environment, but only ranks the finding as informational. Quarterly or monthly network penetration testing using Vonahi's vPenTest provides not only the visibility into the issue, but also provides the context of how it can be used in an attack chain that could devastate your environment.

vPENTEST

vPenTest is a leading, fully automated network penetration testing platform that proactively helps reduce security risks and breaches across an organization's IT environment. It removes the hassles of finding a qualified network penetration tester and provides quality deliverables that communicate what vulnerabilities were identified, what risk they present to the organization along with how to remediate those vulnerabilities from a technical and strategic standpoint. Best of all, it can help bolster the organization's compliance management capabilities.

KEY FEATURES & BENEFTIS

COMPREHENSIVE ASSESSMENTS MADE EASY

vPenTest offers the ability to run both an internal and external network penetration test, ensuring that all potential entry points are thoroughly examined in your network infrastructure.

REAL-WORLD SIMULATION

Our platform simulates real-world cyberthreats, providing you with valuable insights into your security posture and readiness against malicious actors.

TIMELY AND ACTIONABLE REPORTING

The automated testing is followed by detailed, yet easy-to-understand reports, highlighting vulnerabilities, their potential impact and recommended actions for mitigation.

ONGOING PENETRATION TESTING

vPenTest allows you to set monthly testing intervals without breaking the bank, ensuring that your security posture remains proactive and responsive to new threats.
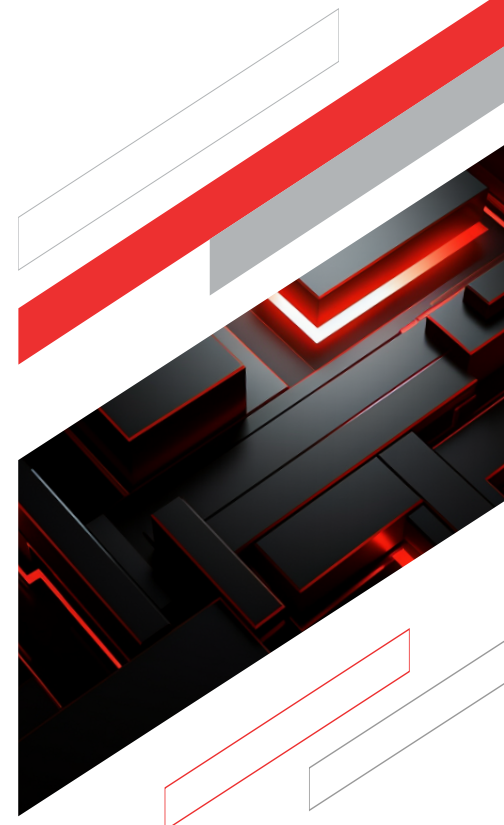
EFFICIENT INCIDENT RESPONSE

By identifying vulnerabilities proactively, you are better prepared to respond to potential security incidents efficiently and effectively.

COMPLIANCE ALIGNMENT

Our solution aligns with regulatory compliance requirements, such as SOC2, PCI DSS, HIPAA, ISO 27001, as well as cyber insurance requirements for network penetration testing.

INDUSTRY RECOGNITION & CERTIFICATIONS

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations

Gartner®

Gartner® recognizes Vonahi Security in their Hype Cycle™ for Security Operations Three Years in a Row in the Automated Penetration Test and Red Teaming Tool category.

TAKE YOUR SECURITY TO THE NEXT LEVEL IN 3 EASY STEPS:

01

Check Out Our Website

Visit our website and learn more about why 10K organizations love vPenTest.

➤ www.vonahi.io

02

Check Out Our G2 Reviews

See why we're a High Performer on G2 with over 100 product reviews from organizations and IT teams from all around the world.

➤ See G2 Product Reviews

03

Schedule a Demo

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

VONAHI
SECURITY

ABOUT US

Vonahi Security is a cybersecurity company that developed vPenTest, a SaaS platform that automates network penetration testing, a valuable service that mimics the way a hacker would target an organization to obtain confidential information. Through automation, our platform delivers monthly pentesting at a fraction of the cost of an outsourced consultant. We eliminate inefficiencies, increase the scope, free up budget for other cybersecurity initiatives, and ultimately make the organization more secure.

www.vonahi.io

HELLO WORLD.
MEET AUTOMATED NETWORK PENTESTING.

VONAHI
SECURITY
A **Kaseya** COMPANY

🌐 **www.vonahi.io**

✉️ **info@vonahi.io**

𝕏 in f @vonahisec