

vPENTEST

for Managed Service Provider (MSPs)



Table of Contents

03 EXECUTIVE SUMMARY

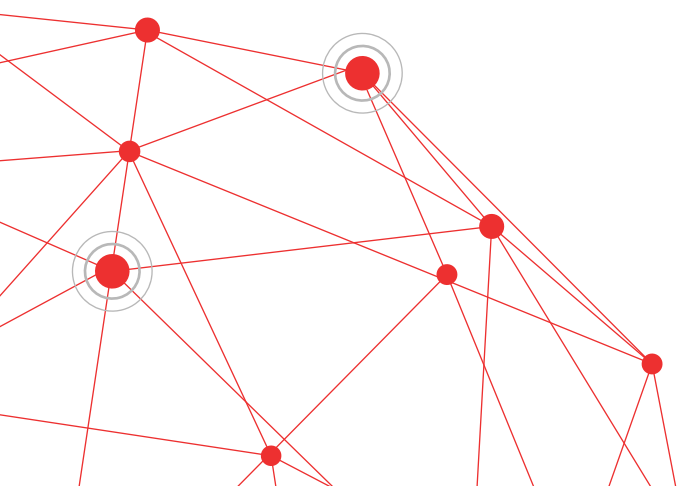
04 WHAT IS vPENTEST

05 ADVANTAGES OF vPENTEST TO TRADITIONAL PENETRATION TESTING

06 HOW MSPs CAN BENEFIT FROM vPENTEST

07 SCHEDULING FLEXIBILITY

08 FREQUENTLY ASKED QUESTIONS





EXECUTIVE SUMMARY

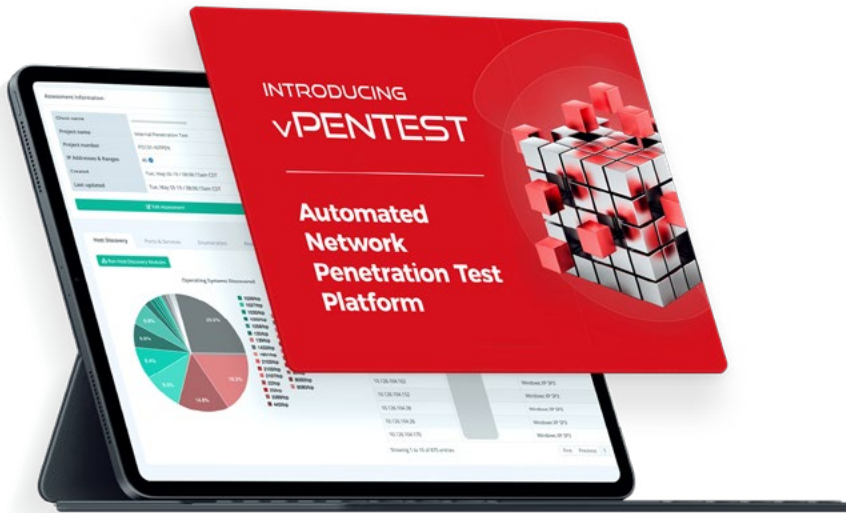
A Managed Service Provider (MSP) is the lifeline of many organizations around the globe, ranging from small and medium-sized businesses (SMBs) to even some larger organizations. For many decades, organizations have relied on MSPs to enable their businesses to operate and conduct business. This includes installation of physical network hardware and software needed to operate, as well as the on-going support and maintenance.

The demand for IT services have significantly increased over the last decade, thus many MSPs have entered the market. However, one of the challenges that are faced by MSPs is fulfilling the need of customers who need comprehensive cybersecurity services. Currently, MSPs have the ability to provide automated vulnerability scanning, but this is the limitation; additional services require outsourcing.

Although cyber security services are critical for SMBs due to the high risk of a data breach and going out of business, the cost of cyber security services make providing

these services unfeasible. This is due to the level of manual effort required to fulfill these services, which typically take several days, hacking skills, and require a lot of interaction with the customer. Many larger organizations have the budget and capabilities to have these services fulfill; however, SMBs typically have to figure it out themselves until they are large enough to afford such assistance.

Vonahi Security intends to partner with MSPs to solve this long-lasting and continually growing challenge with the introduction of an automated solution that is efficient, competitive, affordable, and scalable without limitations. By providing an automated solution to solve this challenge, MSPs can provide this service to their customers to compliment IT services. By partnering with Vonahi Security, MSPs will have the ability to offer more value than traditional cybersecurity consulting companies, and on a much larger scale.



WHAT IS vPENTEST?

vPenTest is an automated network penetration testing platform that replicates the exact same steps and processes performed by a security consultant. This includes technical tasks such as host discovery, service enumeration, vulnerability analysis, exploitation, post-exploitation, privilege escalation and lateral movement, as well as documentation and reporting.



vPenTest combines the knowledge of multiple highly skilled penetration testers along with numerous tools and techniques used in the industry by penetration testers with over a decade of experience and certifications.



ADVANTAGES OF vPENTEST TO TRADITIONAL PENETRATION TESTING

Traditional penetration testing has come a long way in the world of offensive cyber security services; however, there are limitations that even many cyber security consulting firms face. This includes some of the following issues:

01.

FINDING AND EXPANDING TALENT

02.

TRAINING AND ON-BOARDING NEW CONSULTANTS

03.

FULFILLING A HIGH DEMAND OF SERVICES

04.

HIGH INDUSTRY TURNOVER AND SKILL GAP

05.

PROCESS AND METHODOLOGY STANDARDIZING

06.

COSTLY AND TIME-CONSUMING ENGAGEMENTS

07.

UNAVAILABILITY WHEN NEEDING SECURITY CONSULTING SERVICES WITHIN A SHORT TIME-FRAME

vPENTEST SOLVES EACH ONE OF THESE CHALLENGES, AND VERY EFFICIENTLY.

For example, the average manual penetration test report takes approximately 5 hours. This includes reporting, QA, revisions, etc. vPenTest accomplishes reporting in less than 10 seconds, providing almost twice as much valuable information than traditional penetration test reports. Another great example is that, because vPenTest is automated, it is able to scale across numerous customers without any limitations.



HOW MSPs CAN BENEFIT FROM vPENTEST

01.

Provide flexibility to your customers, allowing for penetration tests to be performed at any time.

04.

More extensive and goes way beyond an automated vulnerability scan.

02.

Provide more value in penetration test reports, including activity logs for customers to increase visibility on their networks.

05.

Significantly more affordable with better results than a traditional network penetration test.

03.

Ability to provide on-going penetration tests to customers with real-time activity tracking in the vPenTest dashboard.

06.

Ability to assign modules to customers based on IPs and schedule flexibility.



vPENTEST allows managed service providers to compete with traditional cyber security firms due to its **competitive pricing** structure, **value** within the deliverable documentation that it provides, along with its **speed** and **efficiency** performing a penetration test.

Additionally, since vPenTest provides activity logs to help customers identify where detection and response gaps may exist, this allows MSPs to sell additional services to their customers, such as network firewalls, intrusion detection and response systems (IDS/IPs), and more.



SCHEDULING FLEXIBILITY

Add assessment

1 PROJECT DETAILS 2 FREQUENCY 3 SCAN TIMES 4 IP RANGE 5 NOTIFICATIONS 6 SUMMARY

Contract Details

Company: Demo Company OR + Add New

Contract: Demo Contract Name OR + Add New

Project Assessment

Choose assessment to be performed in this schedule.

- External Vulnerability Assessment
- External Network Penetration Test
- External Network Security Assessment
- Internal Network Penetration Test
- Internal Vulnerability Assessment
- Internal Network Security Assessment

Previous Next

Save Close

From the vPenTest dashboard, your organization can easily set-up a customer and schedule a full blown penetration test in 6 easy steps.

New Contract

Company: Demo Company 1

Contract Code: DEMO1

Contract Period: 12/09/2019 - 12/09/2020

IPs available

430 IPs available from 465 IPs.

Contract Modules

- Internet presence check
- External network penetration test
- External vulnerability assessment
- Internal network penetration test
- Internal vulnerability assessment
- Segmentation testing

Total IP allowed in this module	Select Frequency
Total IP allowed in this module	Select Frequency
Total IP allowed in this module	Select Frequency
35	Quarterly
Total IP allowed in this module	Select Frequency
Total IP allowed in this module	Select Frequency

Save Cancel

vPenTest gives you the ability to assign modules to customers based on IPs and schedule flexibility.



FREQUENTLY ASKED QUESTIONS

01. How does vPenTest differ from a vulnerability assessment?

A vulnerability assessment simply informs an organization about the vulnerabilities that are present within their environment. However, a vulnerability assessment **does not** attempt to exploit those vulnerabilities to determine the potential impact of successfully exploiting those vulnerabilities. This is not a flaw with vulnerability scanners; they just simply aren't designed to do this.

vPenTest differs in that it is able to perform exploitation and post-exploitation techniques to demonstrate to customers how successfully exploiting a vulnerability could potentially lead to further access to systems and/or confidential data within their environment.

02. What is the biggest difference with vPenTest compared to a traditional penetration test?

Traditional penetration tests are extremely time consuming, whereas vPenTest can run numerous tools simultaneously, wait for them to complete, automatically analyze the results, and determine its next move. This saves a significant amount of time from simply running one command at a time. Furthermore, vPenTest reduces the time spent reporting from 6 hours (average between reporting, QA, etc.) to less than a minute. **That's a 29,900% speed increase per assessment that it saves.**

[See the Infographic](#) for additional benefits provided by vPenTest compared to traditional penetration testing.

03. What are some types of exploitation and post-exploitation techniques that it tries?

vPenTest attempts to perform SMB relay attacks, man-in-the-middle attacks, cautiously executed DNS poisoning attacks, hash cracking, password dumping and retrieval, and more. These are the exact same techniques executed during a manual penetration test, except much faster.



FREQUENTLY ASKED QUESTIONS

04. How does support work?

Vonahi Security will provide on-going support included in the contract prices (at no additional charge) so long as the support involves assistance with issues in the portal or enhancement ideas. Furthermore, Vonahi Security has included a ticketing feature within vPenTest so that both MSPs as well as customers can open a support ticket.

Customers that log into vPenTest can submit a support ticket, which will be generated and sent to primary points of contacts at the MSP. If the issue cannot be resolved by the MSP, the MSP has the ability within vPenTest to escalate the ticket to Vonahi Security. At this point, Vonahi Security will work with the MSP or the customers on the requested support.

05. Is vPenTest geared more towards web app pen tests or network system pentest?

vPenTest is focused strictly on network security pentests, including the following activities:

- **Host Discovery/Info Gathering:** Discovering systems on the network environment based on the IP addresses provided to vPenTest.
- **Authentication-based attacks:** It will attempt to login to network services to authenticate, such as POP3, Telnet, SMB (and active directory), FTP, etc. to gain access to data and systems. It will also try to determine where any newly captured credentials work as well. It'll also use OSINT information to construct usernames for these password attacks.
- **Man-in-the-middle attacks:** This includes SMB relay attacks, DNS poisoning, ARP poisoning, with the intent of capturing credentials (hashed and/or cleartext)
- **Exploitation & Post Exploitation:** Including uploading files that would provide access via a shell, enumerating AD group memberships to look for elevated access, enumerating shares, etc.



FREQUENTLY ASKED QUESTIONS

06. Does vPenTest cover MITRE ATT&CK types?

The platform does indeed actually replicate some of the attacks documented in the MITRE ATT&CK framework, although the reporting structure does not currently include references to the framework at the moment.

07. Do you have any mapping to common compliance frameworks like PCI, HIPAA, or NIST?

vPenTest does not currently map to any compliance frameworks. We've started developing some PCI-oriented configurations around the platform (e.g. performing segmentation testing and validation), but these changes are going to be pushed out in a future release.

08. Do you have a sample report I can send to a client?

Yes, please send an email to support@vonahi.io or your point of contact (channel partner maybe?) requesting a copy and we'd be happy to share a sample report.

09. When the report is completed, do the results stay in the portal? Where is the data stored?

Upon completion of the projects, the data within the portal is destroyed within one month unless specifically requested not to.

The data is temporarily stored in a database protected in a PKI infrastructure requiring an IP address whitelist, multi-factor authentication, certificate-based authentication, and explicit user permissions. This server is stored within a digital ocean droplet, located within the US, that is also protected by 64+ character authentication credentials and multi-factor authentication.



FREQUENTLY ASKED QUESTIONS

10. If a hacker gets in, can they see all your clients from one single login?

Only a small number of Vonahi Security employees (less than 3) have access to the portal and all of the client information. These accounts are protected with extremely long credentials and multi-factor authentication. The application also consists of several honeypots to lure malicious attackers and has a zero tolerance hack attempt - any malicious attempt between vPenTest agents or even the vPenTest portal results in an immediate and permanent IP ban.

11. Is there a zero trust model implemented?

As ethical hackers ourselves, we deeply understand the extreme importance behind protecting our clients' data. We know we will be targeted numerous times and have taken several precautions to limit our attack surface, including temporarily storing data until unnecessary, incorporating the principles of least privilege, IP address whitelisting, and multi-factor authentication.

12. If I scan an entire subnet range, will the whole range count against my IP address limit?

No. If you provide a /24, for example, and there are only 5 live systems within that network, then your IP address count will only be reduced by 5.

vPenTest does not consider the range, or location(s) included in the assessment when it comes to the IP address count. The only thing that matters is the number of systems that are actually active within the environment.

13. What is considered an IP address when creating a scheduled assessment?

Anything that has an IP address on the network. This includes phones, network devices, printers, IP cameras, etc.

While many individuals may believe that excluding devices such as printers may be necessary to preserve IP addresses, it should be noted that any device on a network could present a risk to the environment.



FREQUENTLY ASKED QUESTIONS

14. How long does it take for an assessment to run?

It typically depends on the number of systems that are being targeted, along with the number of opened ports and services running on those systems. It's safe to estimate approximately 45 seconds to 3-4 minutes per IP address depending on the number of services running.

15. Can the VM scan over a VPN?

It is usually not recommended to perform a penetration test **and** vulnerability assessment over a local VPN interface if possible. Although the penetration test should run just fine, vulnerability scanners may sometimes have issues when it comes to performing over VPN interfaces.

16. Can we exclude IP addresses from the scans?

Yes. Whenever you create a scheduled assessment, step 4 allows you to provide IP addresses that you wish to test, along with those you wish not to test. Even if the IP address that you provide in the exclusion list exists in the inclusion list, they will not be scanned.

17. Do you recommend excluding certain devices?

No. Every device that has an IP address could potentially present a risk to the environment at some point in time, depending on their functionality. Even some of the devices that appear to pose the smallest risk to the environment could potentially be used by an attacker.

18. What platforms does the virtual machine support?

The virtual machine (VM) is downloaded in the .ova format. You can import this directly into VMware's hypervisor. For any other hypervisor, such as Hyper-V, you may need to download a standalone converter to convert the .ova file into an acceptable format.

PENETRATION TESTING COMPARISON

Traditional Penetration Testing

VS

vPenTest - Automated PenTesting

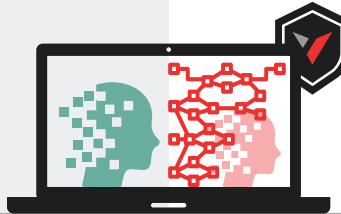


Executed manually by humans, possibly missing checks and low-hanging fruit

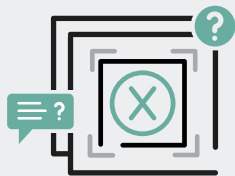
Consistently performs discovery, enumeration, exploitation, and post-exploitation



Methodology executed based on memory and experience

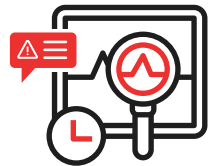


Tasks based on MITRE ATT&CK framework, experience, and Vonahi Security's Penetration Test framework

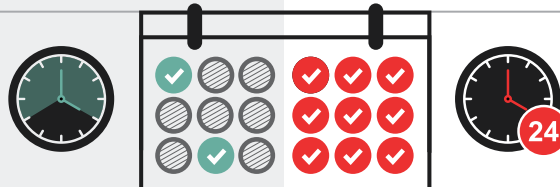


May lack consistent communication about assessment status and identified risks

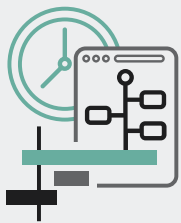
Real-time status updates and notifications for activities and identified threats



Scheduling assessments may be difficult, depending on available resources



Execute penetration tests at any time, any day



Risks are evaluated and demonstrated at a point-in-time with longer turnaround time on deliverables (approx. 2 weeks average)

On-going penetration tests, allowing for up-to-the-minute identifications of risks



Consultant(s) may lack expertise depending on experience



Backed by OSCP, OSCE certified consultants with contributions to Kali Linux, Metasploit, and other frameworks

Consultants sometime juggle multiple projects, resulting in less value to your organization and higher costs due to manual labor required.

Combination of red team penetration testers and developers to offer your organization more value, efficiency, consistency, and convenience.



ABOUT US

Vonahi Security is building the future of offensive cyber security consulting services through automation. We provide the world's first and only automated network penetration test that replicates full attack simulations with zero configuration. With over 30 years of combined industry experience in both offensive and defensive security operations, our team of certified consultants have experience working with a significant number of organizations, industries, networks, and technologies. Vonahi Security is headquartered in Atlanta, GA.

www.vonahi.io



HERE TO HELP!

Questions, concerns, or feedback? Our team is ready to assist.

partners@vonahi.io

HELLO WORLD. MEET MODERN SECURITY.



 www.vonahi.io

 info@vonahi.io

 1.844.VONASEC (866-2732)

 [in](#) [f](#) [@vonahisec](#)

