THRIVE℠

Know Your Business Risk

A Definitive Guide to Autonomous Penetration Testing

Introduction

In the fast-growing digital space, there is a constant wave of new technologies and cyber advancements that can allow businesses to prosper. However, traditional methods of securing IT infrastructure are no longer sufficient to counter new, sophisticated cyber attacks. As cyber adversaries become more advanced, the need for proactive and continuous security measures is crucial for organizations. Autonomous penetration testing has emerged as a cutting-edge solution to this pressing challenge, providing businesses with a robust and efficient means to identify vulnerabilities and system weaknesses before they can be exploited.

This definitive guide to autonomous penetration testing will dive into the importance of why businesses need to adopt autonomous penetration testing as part of their cybersecurity plan, the differences between penetration testing and vulnerability testing, implementing a penetration testing plan for your business, what to do with your testing results, and potential cybersecurity planning challenges. As businesses strive to stay ahead of cyber threats, embracing autonomous penetration testing becomes a critical component of a comprehensive security framework. Additionally, this guide aims to provide IT professionals, security practitioners, and business leaders with the knowledge and insights needed to harness the full potential of autonomous penetration testing, safeguarding their digital assets in an increasingly hostile cyber environment.

Autonomous penetration testing has emerged as a cutting-edge solution to this pressing challenge, providing businesses with a robust and efficient means to identify vulnerabilities and system weaknesses before they can be exploited.

The Importance of Conducting Penetration Testing in Today's Cybersecurity Landscape

What is Autonomous Penetration Testing

Penetration testing (or pen testing) is a cybersecurity practice that mimics an attacker by pivoting through your environment, chaining together techniques and exploits based on what it finds. Autonomous pen testing leverages advanced technologies such as artificial intelligence (AI), machine learning (ML), and automation to simulate real-world cyber attacks on an organization's IT systems. Unlike traditional penetration testing methods, which are often manual and time-consuming, autonomous pen testing automates the process, enabling rapid and comprehensive analysis, covering the entire attack surface without human intervention.

Why Organizations Should Implement Autonomous Penetration Testing

Autonomous penetration testing offers organizations a proactive and repetitive approach to identifying and mitigating security risks in their IT infrastructure. This constant testing and vigilance ensures that newly discovered weaknesses, such as system vulnerabilities, misconfigurations, unencrypted network traffic, legacy protocols/technologies, credentials from the dark web, and default configurations are promptly identified and addressed, significantly reducing the window of opportunity for cyber attackers.

The core advantage of autonomous pen testing lies in its ability to rapidly and accurately identify security risks across diverse IT environments. By mimicking the tactics, techniques, and procedures (TTPs) used by cybercriminals, these systems can uncover hidden weaknesses that traditional methods might overlook. Furthermore, the integration of AI and ML enables pen testing tools to learn and adapt to emerging threats, enhancing their effectiveness over time. By integrating pen testing into their security strategy, organizations can enhance their security posture, improve compliance with industry regulations, and ultimately protect their sensitive data and critical systems from breaches and disruptions.

Industries that handle sensitive data and operate within highly regulated environments, such as finance, healthcare, retail, manufacturing, and critical infrastructure, greatly benefit from regular penetration testing. Financial institutions, for example, are prime targets for cybercriminals due to the valuable data they manage, and regular penetration testing helps identify and mitigate risks before they can be exploited. In healthcare, where patient data privacy is paramount, penetration testing ensures compliance with regulations such as HIPAA by regularly assessing security measures. Retail and manufacturing businesses, dealing with large volumes of payment card transactions, must comply with PCI-DSS requirements, which mandate regular testing of security controls to protect cardholder data. Additionally, critical infrastructure sectors, including energy and utilities, must adhere to stringent regulations like NERC CIP, necessitating continuous security evaluations to safeguard national security interests. By implementing autonomous pen testing, these industries can not only enhance their security posture with regular, unbiased testing, but also meet their stringent regulatory compliance requirements, avoiding potential business-halting penalties and maintaining the trust of their customers and stakeholders.

Furthermore, for compliance-driven reasons for penetration testing, implementing a quarterly autonomous pen test can help you meet government-sanctioned cybersecurity requirements, such as in the United Kingdom's General Data Protection Regulations (GDPR) or the Canadian Common Criteria Program.

75%

of information security companies perform penetration tests to measure their security posture or for compliance reasons. Only 57% of them perform penetration tests to support a vulnerability management program.[1]

[1] https://www.statista.com/statistics/1363099/average-days-to-patch-vulnerability-by-severity/#:~:text=According%20to%20a%202023%20study,high%20severity%20within%2082%20days.

Pen Testing vs. Vulnerability Testing

While they may seem like one and the same, there is a difference between pen testing and vulnerability testing for organizations. The primary difference between pen testing and vulnerability testing lies in their scope and depth. Penetration testing goes beyond identifying vulnerabilities; it simulates real-world attacks to understand the potential consequences of those vulnerabilities being exploited, so organizations can have a better understanding of their organizational risk and consequences of a threat actor conducting malicious activity within their environment. This approach provides deeper insights into the effectiveness of an organization's defenses and helps in developing targeted mitigation strategies. On the other hand, vulnerability testing provides a broader overview of potential security weaknesses without delving into exploitation. It is more about identifying and prioritizing vulnerabilities to guide remediation efforts, such as implementing patching and mitigating zero day vulnerabilities.

Another significant difference is the frequency of the tests and departmental resource requirements. Traditional penetration testing is typically conducted periodically, often annually or bi-annually, due to its resource-intensive nature and high cost. It requires significant expertise and time to execute effectively. However, autonomous pen testing is a much more cost-effective, unbiased, and faster way to check for these potential attack paths. In contrast, vulnerability testing is more frequent, sometimes conducted weekly or monthly, due to its automated nature and lower resource requirements. This frequent scanning helps organizations stay updated on new vulnerabilities and ensures continuous monitoring of their security landscape. The autonomous approach also allows for remediation testing that duplicates the original test scenario and is free from the possibility of human error.

1 in 5

organizations do not test their software for security vulnerabilities[2]

[2] https://www.hcl-software.com/appscan/ponemon-report

Implementing an Autonomous Penetration Testing Plan

For organizations with little to no existing cybersecurity solutions in place, the introduction of autonomous pen testing is a crucial first step towards establishing a robust security framework and getting stakeholder buy-in to build out a larger cybersecurity budget. Without a robust cybersecurity posture, businesses are highly vulnerable to cyber threats, and any breach can result in significant financial losses, reputational damage, and regulatory penalties. Autonomous pen testing provides a rapid and comprehensive assessment of the organization's vulnerabilities, offering actionable insights into the most critical areas that need to be addressed. This proactive approach enables businesses to build a strong foundation for their cybersecurity efforts, ensuring that they are better protected against potential attacks.

For businesses with a weak cybersecurity posture, autonomous pen testing serves as a cost-effective enhancement to their existing security measures. A poorly built out IT stack, a misconfigured EDR product that isn't working to stop threat actors, or an understaffed team can often mean that there are numerous unaddressed vulnerabilities and that current security protocols may not be effective against advanced cybersecurity threats. Autonomous pen testing thoroughly monitors and evaluates the security environment, identifying weaknesses that might not be apparent through traditional testing methods. This automated approach ensures that vulnerabilities are promptly identified, prioritized, and able to be remediated, significantly strengthening the overall security posture and providing unbiased results with actionable resolutions. Additionally, the results of an pen test can be used to better plan and prioritize business's cybersecurity budgets and determine which areas may need more coverage to ensure seamless business continuity. Regular testing can help businesses with weaker cybersecurity postures figure out what's working and what areas may need more priority as they continue to build out their IT infrastructure.

Businesses currently working with a Managed Services Provider (MSP) can also greatly benefit from implementing autonomous pen testing in their cybersecurity plan. While MSPs typically offer a range of security services, including monitoring and incident response, there may be gaps in their assessment and testing processes, leaving your business processes vulnerable to attacks. Autonomous pen testing provides an unbiased evaluation of the organization's security measures, offering a layer of validation to ensure that the MSP's implementation is effective. This additional oversight helps businesses verify that the services provided by the MSP are comprehensive and align with the organization's security objectives. Furthermore, the repetitive nature of autonomous pen testing ensures that the effectiveness of the MSP's solutions is regularly assessed on a quarterly basis, allowing for timely adjustments and improvements.

Organizations saved an average of

$2.22M

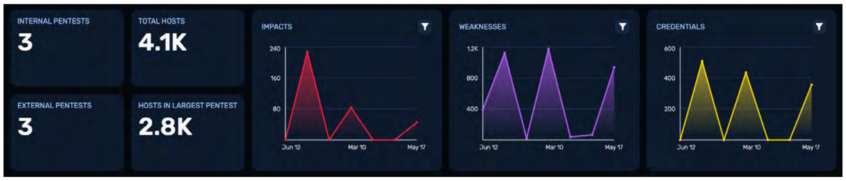
by using security AI and automation extensively in prevention vs. those that didn't, according to IBM's Cost of a Data Breach Report 2024[3]

[3] https://www.ibm.com/reports/data-breach

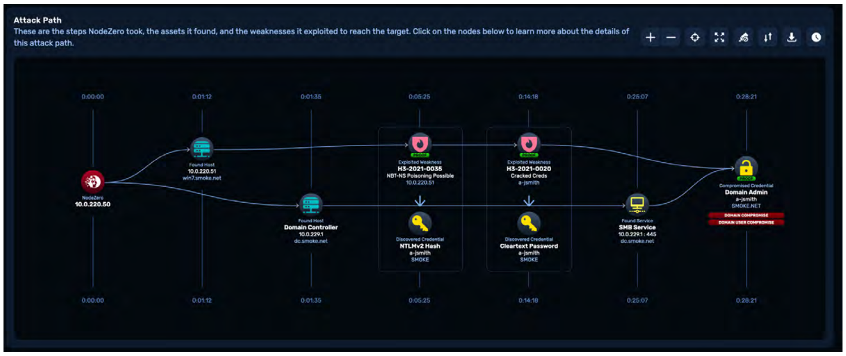
Risk Follow Up: What To Do With Your Pen Testing Results

When working with a managed service provider (MSP), like Thrive, to conduct a pen test, you will be given a set of actionable results at the conclusion of the pen test. Once the results of the pen test are available, an expert from the MSP, like Thrive, will step through with you how to implement the actionable steps provided to mitigate future risks. The results will be presented in an easy to understand dashboard that shows:

- How many tests were conducted *(see figure 1)*
- Attack Path of each test *(see figure 2)*
- Fix Actions *(see figure 3)*
- Systemic issues *(see figure 4)*



(Figure 1)



Attack Path

These are the steps NodeZero took, the assets it found, and the weaknesses it exploited to reach the target. Click on the nodes below to learn more about the details of this attack path.

(Figure 2)

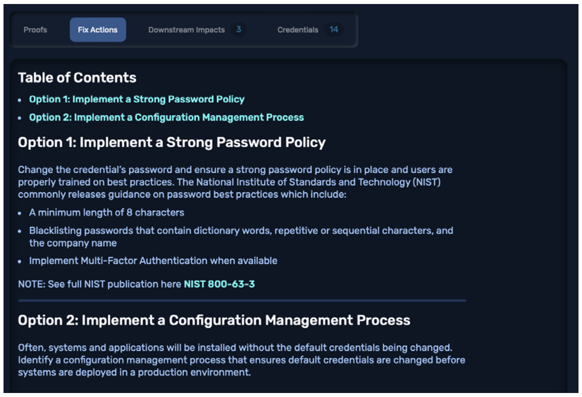


Table of Contents

- Option 1: Implement a Strong Password Policy
- Option 2: Implement a Configuration Management Process

Option 1: Implement a Strong Password Policy

Change the credential's password and ensure a strong password policy is in place and users are properly trained on best practices. The National Institute of Standards and Technology (NIST) commonly releases guidance on password best practices which include:

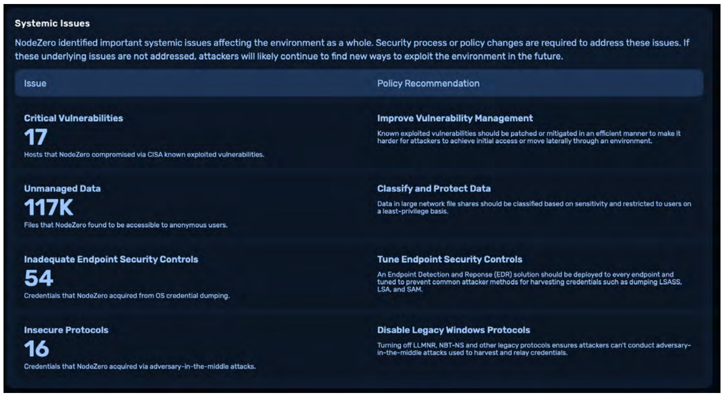
- A minimum length of 8 characters
- Blacklisting passwords that contain dictionary words, repetitive or sequential characters, and the company name
- Implement Multi-Factor Authentication when available

NOTE: See full NIST publication here **NIST 800-63-3**

Option 2: Implement a Configuration Management Process

Often, systems and applications will be installed without the default credentials being changed. Identify a configuration management process that ensures default credentials are changed before systems are deployed in a production environment.

(Figure 3)



Systemic Issues

NodeZero identified important systemic issues affecting the environment as a whole. Security process or policy changes are required to address these issues. If these underlying issues are not addressed, attackers will likely continue to find new ways to exploit the environment in the future.

Issue	Policy Recommendation
Critical Vulnerabilities 17 Hosts that NodeZero compromised via CISA known exploited vulnerabilities.	**Improve Vulnerability Management** Known exploited vulnerabilities should be patched or mitigated in an efficient manner to make it harder for attackers to achieve initial access or move laterally through an environment.
Unmanaged Data 117K Files that NodeZero found to be accessible to anonymous users.	**Classify and Protect Data** Data in large network file shares should be classified based on sensitivity and restricted to users on a least-privilege basis.
Inadequate Endpoint Security Controls 54 Credentials that NodeZero acquired from OS credential dumping.	**Tune Endpoint Security Controls** An Endpoint Detection and Reponse (EDR) solution should be deployed to every endpoint and tuned to prevent common attacker methods for harvesting credentials such as dumping LSASS, LSA, and SAM.
Insecure Protocols 16 Credentials that NodeZero acquired via adversary-in-the-middle attacks.	**Disable Legacy Windows Protocols** Turning off LLMNR, NBT-NS and other legacy protocols ensures attackers can't conduct adversary-in-the-middle attacks used to harvest and relay credentials.

(Figure 4)

These actionable results empower organizations to proactively fix their server weaknesses and help them understand the full picture of their risk and the potential business-halting consequences of the current state of their systems. Organizations can then implement the actionable changes, such as requiring multi-factor authentication (MFA) across their org, or work with an MSP to deploy the changes, such as regular patching management services.

Sitting on Risk: A Story of How a Vulnerable IT Stack Compromised Another Company's IT Stack

Thrive was hired to run an autonomous penetration test on a company's network to see what would happen if a malicious attacker got in. Thrive partners with Horizon3.ai and used their NodeZero tool to perform this attack. The below is a story of what happened.

Thrive performed a black box test with no credentials. Within 40 minutes of the test starting, the first account was compromised using a password spray attack. The password for the account matched the user name. Then a server susceptible to PrintNightmare was identified and a RAT was installed on the server running as SYSTEM. The LSA database was dumped on the device. One of the accounts identified within the LSA turned out to be a domain admin and credentials were verified against a domain controller. The domain was now fully compromised.

Now usually at this point, the test results would see the domain being fully compromised as a win. But of course, the device keeps going and we (Thrive) wanted to see how far we can push this. RAT tools were installed on multiple devices and the LSA on each of these were dumped. Local admin credentials were identified from these dumps. During testing of these credentials, it was discovered that the local admin credentials were reused on multiple machines, both on and off the domain.

Eventually, a non-domain server was identified that utilized the same local administrator credentials as previously discovered. On that server, a file containing API credentials to a cloud storage site was identified.

Just 36 seconds after identifying this file, the NodeZero device verified these credentials and accessed the cloud. Within a few minutes, the device identified all files within the cloud, including sensitive data.

Following the completion of this pen test and discussing the results with the client, it was discovered that the client did not have any cloud storage. It was then disclosed to the client's critical business partners and their MSP. None of these companies were able to identify this cloud storage. Further discovery led us to learn that none of the stakeholders were aware of what this server was actually doing in their environment.

Manual investigation then occurred to identify what was going on. Thrive was eventually able to identify the company to whom these credentials belonged, along with some more credentials. Of course, an ethical disclosure to the company immediately occurred to ensure that these credentials and keys were disabled.

Conducting a pen test uncovered vulnerabilities that extended beyond the company being tested. Instances like this show how crucial it is for companies to invest in cybersecurity planning and proactively understand what and who has access to your private servers. The trickle down effect of a hack like this could have been astronomical, leaving many users with compromised PII or worse. Taking the precautionary step of employing a penetration test can save your company and your 3rd party vendors from havoc.

Conducting an autonomous penetration test uncovered vulnerabilities that extended beyond the company being tested. Instances like this show how crucial it is for companies to invest in cybersecurity planning and proactively understand what and who has access to your private servers.

Cybersecurity Planning Challenges

Businesses face numerous challenges when developing and implementing effective cybersecurity plans. One of the most significant hurdles is budgetary constraints. Cybersecurity investments can be substantial, encompassing not only the cost of advanced security tools and technologies but also the ongoing expenses associated with training, monitoring, and incident response. For many organizations, especially small to medium-sized businesses (SMBs), allocating a sufficient budget to cover these costs can be difficult. Budget limitations often result in gaps in security coverage, leaving them vulnerable to cyber threats.

Another major challenge is balancing different cybersecurity priorities. Organizations must protect a diverse range of assets, from customer data and intellectual property to operational systems and employee's personally identifiable information (PII). Prioritizing these different elements requires a thorough understanding of potential threats and their potential impact on day-to-day business operations. Limited resources and IT expertise can make it challenging to develop a comprehensive strategy that addresses all critical areas for a business.

The decision between outsourcing cybersecurity functions and maintaining them in-house also poses a significant challenge for businesses, both budgetarily and strategically. Outsourcing can provide access to specialized teams of experts and advanced technologies that may be cost-prohibitive for businesses to develop internally. On the other hand, it may raise concerns about vendor reliability, data privacy, and control over security processes. While managing cybersecurity in-house allows for greater control and customization of security measures, it requires a substantial investment in skilled personnel and technology infrastructure, which small to medium-sized businesses may lack the resources for. Striking the right balance between these options is critical to ensuring robust cybersecurity while optimizing costs and resources.

Autonomous pen testing offers a powerful solution to these cybersecurity planning challenges. By automating the penetration testing process, businesses can significantly reduce costs associated with manual testing and human resources. Furthermore, autonomous pen testing helps businesses manage their cybersecurity priorities more effectively. These tools can be configured to focus on different areas of the IT infrastructure, ensuring that all critical assets are regularly tested for vulnerabilities and that potential threats are mitigated in a timely fashion. This allows organizations to adapt their security strategies in real time, staying on top of threats and protecting their assets.

Autonomous penetration testing is a black-box penetration test, meaning that no one user can influence the test or its results. With or without insider information, the test results will always be fair and consistent, giving businesses a real view of their security weaknesses. When it comes to outsourcing vs. in-house, the results of the test and the needed actions to fix any risks can help your team determine if expanding your IT team internally or hiring an MSP is the best option forward.

How Often Should I Pen Test?

Pen testing is only good on the day it is performed. While many simulations can be run at the same time, the introduction of new vulnerabilities or any other changes to the environment will invalidate the results and may not give your organization the full picture of what's going on with your system. Recurring testing allows for validation of any remediation that has taken place, while also conducting the entire test from start to finish. Quarterly autonomous pen testing reduces the cycle of a traditional annual pen test and provides better insight as well as the ability to perform corrective actions.

Conclusion

Understanding and implementing autonomous pen testing is the right choice for many organizations seeking to identify their vulnerabilities and secure their IT infrastructure, data, and applications without expending unnecessary resources and time. As cybercriminals continue to increase their sophistication and effectiveness, companies find themselves in a constant state of defense, often hindered by vulnerable legacy security systems that are labor-intensive to update and require extensive training and upkeep.

As a leader in managed IT security services for enterprises of all sizes, Thrive provides value that extends beyond individual solutions. Thrive's NextGen Managed Services Platform leverages 20 years of industry, business, and technology knowledge for the implementation and delivery of cloud, security, disaster recovery, networking, compliance, and workflow automation services.

Once an organization implements a regular autonomous pen testing plan with Thrive, they benefit from Thrive's service-driven experts who will provide a report on all vulnerabilities and security risks and will step through with you how to implement the actionable steps provided to mitigate future risks. Thrive creates a seamless experience that operates round the clock, 24x7x365, delivering lasting solutions that proactively safeguard your business. Reach out to the Thrive team today to learn more about integrating autonomous pen testing into your security strategy for comprehensive, managed security.

Reach out to the Thrive team today to learn more about partnering for better, managed security.

Contact the Thrive Team

To Learn More, Contact Us Today, or Give Us a Call At:

thrivenextgen.com | info@thrivenetworks.com | 1-866-205-2810

About Thrive

Thrive is a leading provider of NextGen managed Cybersecurity & Cloud-based services designed to drive business outcomes through application enablement and optimization. The company’s Thrive5 Methodology utilizes a unique combination of its Application Performance Automation Platform and strategic services to ensure each business application achieves peak performance, scale, uptime, and the highest level of security.