Why the Pen Test Needs an Update

SPONSORED BY

A SANS First Look

Written by **Dave Shackleford** | March 2022

Introduction

Most mature security organizations perform some regular penetration testing by internal teams, consulting, or both. However, in today's realm of fast-moving technology changes and complex on-premises and cloud infrastructure, performing regular pen tests can be challenging for a variety of reasons. First, most teams rely on vulnerability scanning to locate assets and potential avenues of exploitation during pen tests—these can be disruptive and produce a lot of false positives. Vulnerability scanners are certainly important, but their usefulness in comprehensive pen testing can be somewhat limited. Secondly, manual pen tests are always somewhat of a "point in time" endeavor and may have limited value over a longer period of time.

Fortunately, new technologies are emerging to help provide automated attack modeling and more consistent, repeatable pen tests that mimic real-world attack techniques.

The First Look

SANS took a look at the Horizon3.ai NodeZero, a continuous, autonomous penetration testing platform offered in a SaaS format. For security teams, there are several well-defined use cases for a platform like NodeZero, including:

- A "sparring partner" for the SOC—Security teams use NodeZero to quickly verify they are logging the right data in their SIEM, any EDR is configured correctly, and that policies and procedures work effectively to quickly address attacks.
- "Self-service pen tests" for the Blue Team—IT admins, network engineers, and other defensive operators on the Blue Team can leverage NodeZero to execute self-service pen tests to proactively harden their systems and fix exploitable vulnerabilities.
- Efficiency for the Red Team—Internal pen testing teams use NodeZero as a force multiplier, where NodeZero conducts reconnaissance and post-exploitation at scale, enabling the team to focus and spend more time on specific and advanced attack tactics.

The platform offers several key benefits, including:

- Simple deployment—NodeZero is deployed as an unauthenticated Docker container that only requires a single Docker host for operation. The container coordinates and performs all attacks within any environment, requiring communication to the SaaS service only for coordination and updates.
- Agentless approach—Other pen test automation platforms require agents installed on systems to be tested, which is cumbersome and unwieldy. NodeZero is an agentless platform that requires minimal effort to run a pen test in minutes, compared to weeks spent configuring other solution's agents.
- Exploitation verification—To reduce false positives, NodeZero performs actual exploitation techniques with real-world tools and tactics, ensuring that any vulnerability exploited is fully verified. All evidence of commands and tools run, responses, and follow-up actions is fully captured to provide proof of exploitation to organizational stakeholders.

- Attack path visualization—It's critical for security organizations to accurately map how attacks occur from initial compromise and attacker access through lateral movement and data access/exfiltration. NodeZero provides detailed visualization of all steps in the attack chain, with the capability to drill into each step/phase and see what activities were performed.

Evaluating the Platform

Our high-level review found many useful and beneficial features that security operations teams can make use of to perform more consistent, well-documented, and automated penetration tests. First was the ease-of-use within the user interface. Security teams can kick off a pen test within minutes by following a few steps that include:

- Adding scope (IP addresses and ranges)
- Open source intelligence gathering online (useful for external tests in particular)
- Specific exclusions and/or types of testing (templates are available for quick execution too)

At the end of this process, a link is generated to download from a local Docker host to access NodeZero online, download the Docker container image, and get things rolling. This process simulates an endpoint system being compromised in some way and initiates the early attack stages seen in the wild consistently (see Figure 1).

Any security team could quickly plan and initiate a pen test in their environment with the simple-to-use interface. The platform then begins enumerating the environment, looking to harvest credentials, exploit vulnerabilities, and exploit default settings and misconfigurations where they exist. Horizon3.ai calls this process the "maneuver loop" and it represents a well-known attacker approach. Based on what is discovered and potentially exploited, NodeZero then builds a visual analytics map of the attack paths deemed possible. This "cyber terrain map"

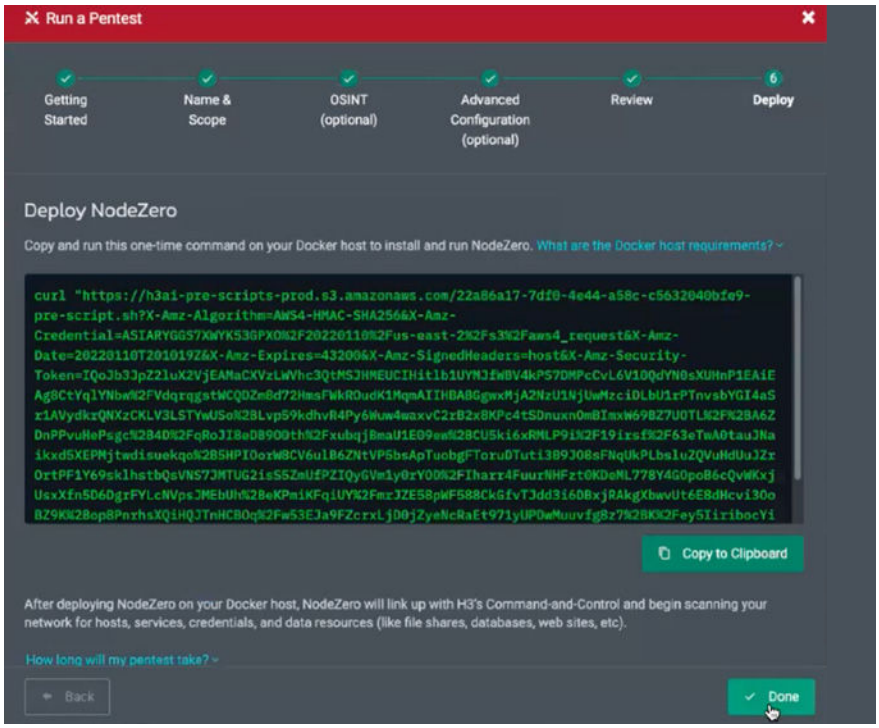

Figure 1. Initiating and Executing the Pen Test with NodeZero

helps clarify the range of vulnerablity scenarios to which the organization may be susceptible.

When these issues have been identified and potentially exploited, NodeZero can easily help identify a broad array of security issues that need attention or potential remediation. The security team can drill into these top issues (under categories including "weaknesses" or basic detected vulnerabilities, exposed credentials, exposed storage in the cloud or otherwise, and more) and then see a full attack path, as shown in Figure 2.

Figure 2. Attack Path for a Domain Admin Credential Compromise

Along the path, NodeZero provides several "proofs" that illustrate the tools and techniques used to exploit systems and applications. It highlights the results, as shown in Figure 3.

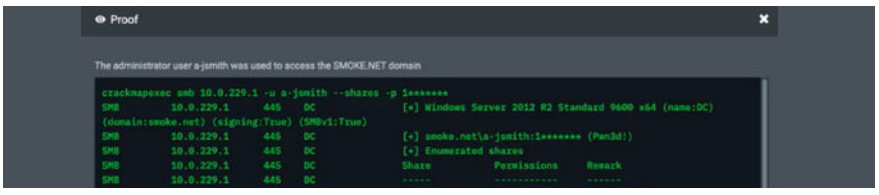

Figure 3. Proof of Exploitation from NodeZero

Overall, the reporting capabilities from Horizon3.ai are excellent and useful for security and infrastructure teams alike. Priorities, patches, and alternate approaches to remediation are clear for each issue detected. One feature worth mentioning is the contextual scoring for detected vulnerabilities, which helps organizations determine whether issues noted in the environment are more or less severe than noted at first glance. This can help to prioritize defensive remediation efforts (see Figure 4).

We really liked NodeZero's operational simplification that ensured that the time to test and verify detected issues was minimal. During tests, significant details are captured, including weaknesses detected, services noted, actions taken by the testing platform, and additional impacts—all of which can be easily accessed and observed in the reporting and follow-up, as shown in Figure 5.

With this type of automation and control, organizations should be able to emulate attacks much more safely, consistently, and accurately to improve defenses.

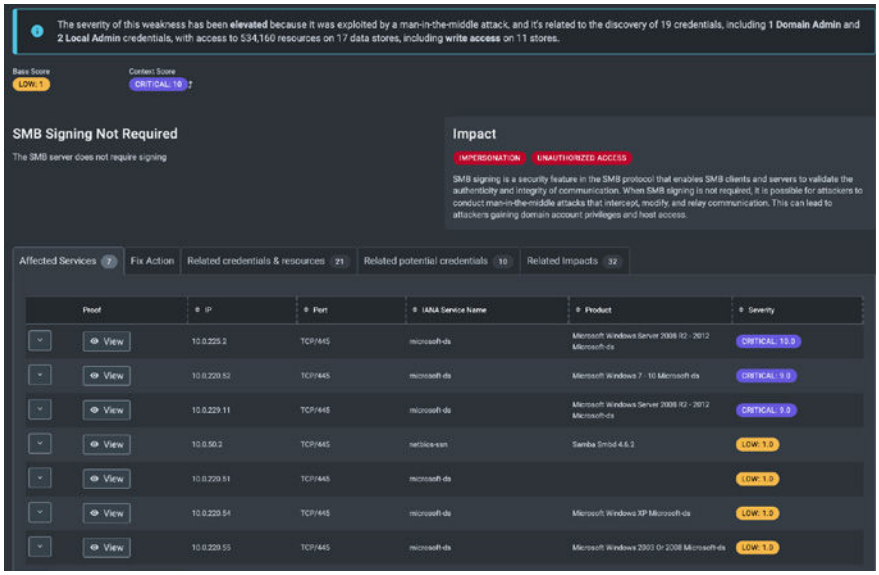

Figure 4. Contextual Scoring for a Vulnerability

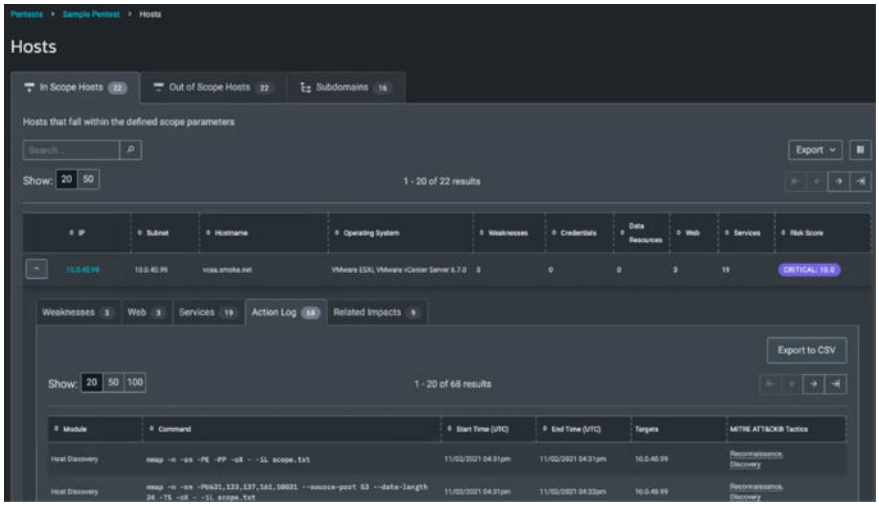

Figure 5. Operational Details of NodeZero Testing

Conclusion

We found that Horizon3.ai NodeZero offers a simple, easy-to-deploy pen testing platform that can help organizations perform tests more frequently, with more control and consistency.

SANS would like to thank this paper's sponsor:

HORIZON3.ai