HORIZON3.ai

~~TRUST BUT~~ VERIFY

Autonomous Penetration Testing

with Horizon3

A professional penetration test brings value to organizations by identifying attack vectors and providing proof of exploitability. It can provide evidence that defensive controls are implemented effectively and focus remediation efforts on an organization's most critical weaknesses.

There are two primary goals when organizations conduct penetration tests: external penetration tests to ensure they have a strong perimeter; and internal penetration tests to discover weaknesses that could be exploited by an attacker who gains a foothold.

Harden Your Perimeter.

Test your security posture as would an external attacker. An external penetration test evaluates the externally facing assets to identify how an adversary can identify and exploit weaknesses to enter and persist in your network.

External penetration tests identify attack vectors that include:

- Open ports and misconfigurations that allow an attacker to enter the network.
- Unpatched vulnerabilities that can be exploited to all access to unauthenticated users.
- Shadow IT projects that expand the attack surface.

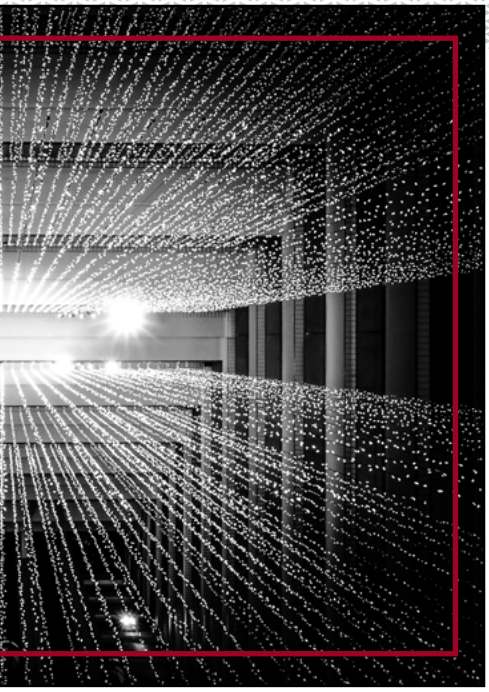
Presume Breach to Limit Damage.

In today's environment of constant social engineering attacks via email, availability of stolen credentials, and misconfigured systems, organizations must presume an initial breach has already occurred and attackers have a foothold in their internal systems.

An internal penetration test starts with the acceptance that an attacker can gain access to your internal network where your sensitive data resides. In addition to the attack vectors like those in external tests, internal penetration tests determine what a malicious actor can accomplish from that starting point:

- How can they access additional credentials and privileges?
- What weaknesses, misconfigurations, and vulnerabilities can they exploit to move laterally?
- What sensitive data can they access?
- Which exact issues must be remediated – and how – to prevent a successful attack?

Not a Vulnerability Scanner



Vulnerability scanners search your perimeter and internal systems for unpatched applications and run rules to look for specific known vulnerabilities as detailed by NIST's Common Vulnerabilities and Exposures (CVE). They will provide reports on those systems they 'think' are unpatched and those CVEs they can identify. The resulting noise of low criticality issues can distract teams for identifying and focusing effort on the most critical vulnerabilities while spending cycles fixing non-exploitable issues.

Importantly, vulnerability scanners do not identify systems that were incorrectly patched, or identify exploitable attack paths that may be available to adversaries who chain together weaknesses in their attacks.

Vulnerable ≠ Exploitable

In contrast, NodeZero identifies exploitable weaknesses in your perimeter and/or internal systems, even when vulnerability scanners and patch management systems show that security updates have been successful. It provides step-by-step path and proof of each successful exploitation so teams understand how an attacker can execute and attack along with remediation advice to prevent those attacks. This allows defensive teams to focus on the most critical issues affecting their security posture without wasting cycles on non-exploitable issues.

What is Autonomous Penetration Testing?

NodeZero is different from other pentesting solutions – combining the lower cost and high frequency testing capabilities of automated pentesting with the expertise, thoroughness, and precision of manual pentests performed by highly skilled security professionals. The result is an ability to run continuous purple teaming exercises at a low annual cost. Pentesting has evolved from manual, to crowdsourced, to automated, and now autonomous.

Manual pentesting requires a trained security resource using commercial and specialized tools to explore an application or system and identify weaknesses. The effectiveness (and cost) of a manual pentest is dependent on the time allotted to the test and the skill of the pentester, leading many organizations to save costs by providing credentials to pentesters. While the results are much cleaner than in an automated pentest, remediation advice is often limited. Further, the high cost of manual pentests prevent organizations from using them frequently, such as after a system is patched to ensure the update was completed correctly.

Automated pentesting is a simple "point and click" approach using commercial dynamic analysis tools. The tool is provided a URL or IP address and spiders the application to identify fields where a malicious user could input data. The tool then "fuzzes" data to the fields to attempt to prove the presence of input validation weaknesses that could be exploited by a skilled attacker or overwhelm the application in a denial of service attack. These tests normally run in a day or two and generate much "noise"; unproven results that defenders must research to determine if they require remediation.

Crowdsourced pentesting includes manual pentests, but rely on a network of independent security researchers who are paid "per vulnerability identified" (plus a platform fee to the vendor). Crowdsourced pentests have the advantage of being open ended, meaning – in theory – you can have people searching for issues every day for months. They can be quite expensive if there are large numbers of vulnerabilities, and findings often lack proof of exploitability (e.g., unpatched systems, open ports, etc.) leading development teams to spend time on non-critical issues.

Autonomous pentesting combines the benefits of automated pentesting; more frequent testing, lower costs, and no requirements for internal security expertise, with those of manual pentests; more complete coverage of the application and proven exploitability. Autonomous pentesting does not require credentials to start. It can chain together weaknesses like a skilled adversary and automatically generate attack trees to isolate the root cause of an exploit. This allows defenders to understand precisely what changes are needed to protect an application.

HORIZON3.ai
~~TRUST BUT~~ VERIFY

How NodeZero Works

Reconnaissance –Any successful attack requires intelligence on the target. NodeZero starts with unauthenticated access to the system, then creates a Knowledge Graph, identifying all hosts, misconfigurations, open ports, and searches for credentials.

Maneuver Loop – NodeZero orchestrates over 100 offensive tools to harvest credentials, exploit vulnerabilities, and exploit default settings and misconfigurations to execute attacks.

Verified Attack Plans – To simplify prioritization and remediation, results are provided as "Proofs" with graphical and textual representations of each step in a successful attack. This includes which tactics were used, which weaknesses were identified and exploited, how credentials were obtained, and the paths taken to gain privileges and access to systems.

Impact – NodeZero identifies and reports on data at risk across physical and virtual environments it was able to access with read/write privileges, including SMB shares, NFS shares, FTP shares, cloud storage, vCenter servers, and databases.

Contextual Scoring – NodeZero evaluates and prioritizes each weakness by its role in the successful attack – not by base CVSS score. Organizations can quickly identify those weaknesses that present the greatest threat and must be addressed immediately, and which can be safely deferred.

Actionable Remediation – NodeZero provides precise and actionable remediation guidance, allowing security and operations to resolve issues at the root cause quickly.

Ready to Learn More?

NodeZero is an Autonomous Penetration Testing as a Service (APTaaS) that helps organizations **find and fix attack vectors before attackers can exploit them**. It is safe to run in production and requires no persistent or credentialed agents.

- **Sign up for your free demo today.**
  https://pages.horizon3.ai/demo

HORIZON3.ai
TRUST BUT VERIFY