Progressive Penetration Testing

MNJ/Adlumin Progressive Penetration Testing Program offers progressive assessments to meet every customer's risk tolerance. Our tests can simulate internal and external vantage points. We can limit the scope to assess what can be exploited from inside a defined range or utilize an "outside-in" perspective to determine if critical data and assets can be accessed inside a specific scope.

Benefits of the MNJ/Adlumin Progressive Penetration Testing Program

CORE FUNCTIONALITY

- Requires no persistent or credentialed agents
- Scopes specific IP ranges to scan or IP ranges to avoid
- Intelligently identifies the scope for you
- Enables or disables specific attacks

USE CASES

Enables understanding of the security posture across several dimensions so cybersecurity teams can:

FIND

Proactively discover, leverage, and chain exploitable weaknesses to:

Prove out the potential critical business impacts with proof-of-exploit in hand.

Understand the attack vectors leading to critical impacts to know exactly what to fix to disrupt the kill chain.

FIX

Focus on efficiently mitigating or remediating weaknesses that can be exploited instead of chasing down unexploitable vulnerabilities and false positives.

VERIFY

Validate those mitigations or remediations were implemented and remain implemented.

ASSESS

Continuously assess the security posture and quickly compare results to see what new weaknesses have been added or fixed.

Industrialized criminals use sophisticated tactics, techniques, and procedures (TTP) that exploit vulnerabilities across accounts, remote access points, administrative tools, and core network infrastructure. With limited resources, most organizations struggle to identify these exposures, prioritize vulnerabilities, and align to business objectives that protect and meet the obligations of the management of protected assets.

Many organizations and regulatory frameworks require annual penetration tests to identify exposures. These tests no longer match the capabilities of cyber adversaries. Annual tests provide a snapshot of an organization's cybersecurity health. New systems and users, patches and application updates, and fluid configurations render the penetration test results irrelevant within days.

Traditional penetration tests use limited formulaic methodologies testing known criminal tactics, and not the evolving threat landscape facing organizations. The cybercrime ecosystem leverages a diverse set of skills and creativity with a significant amount of time and motivation to access an asset. Typical tests stress single points and controls rather than criminals' complex and multi-step exploitation.

Limited scope, high costs, and a short shelf life contribute to the need for a new method to test an organization's defenses.

MNJ/Adlumin Progressive Penetration Testing Program recognizes that criticality is a function of exploitability and impact and operates under the thesis that customers in a specific industry segment that continue to use traditional pen test methodologies may be elevating their risk-posture unnecessarily.

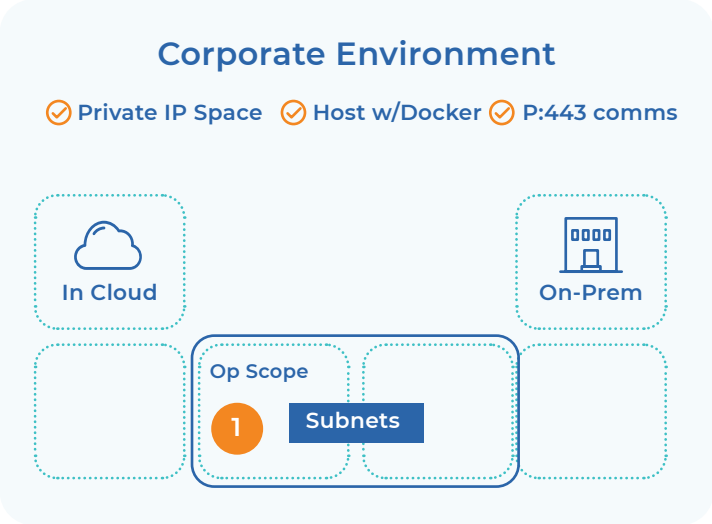
MNJ/Adlumin's Progressive Penetration Testing Program provides real-world penetration scenarios that cover industry-specific threat assessments and offers rapid results with actionable recommendations. An audit trail provides a reverse-engineered blueprint to demonstrate how testers could access the environment, move laterally, gain access to critical systems, and "capture the cyber flag" to prove the efficacy of the testing.

Deliverables:

The complete results of the penetration test are documented in four separate reports.

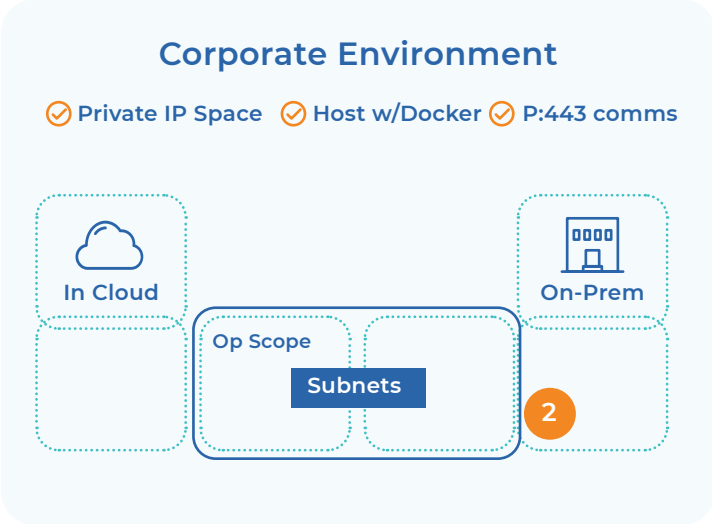
1. Executive Summary Report
2. Pen Test Technical Report
3. Segmentation Report
4. Fix Actions Report

The comprehensive results document and explain each vulnerability, impact, evidence, observed instances, and remediation recommendations. Vulnerabilities are visually documented to demonstrate impact and ensure a complete understanding of how they are to be exploited.



1 Inside Custom Scope

If you want to limit the scope and see what an attacker could exploit from inside that defined range, you will place the Node host within the scope you want to test.

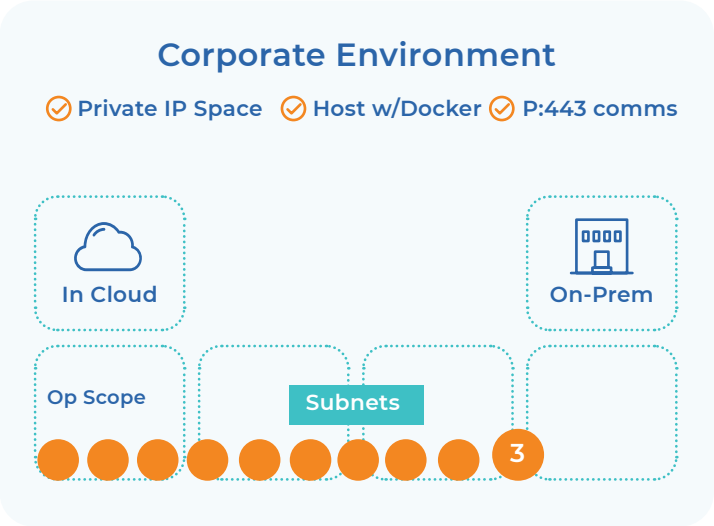


2 Outside Custom Scope

But if you want an "outside-in" perspective to see if an attacker could access critical data and assets inside a specific scope, you will place the Node host outside the scope you want to test.

When you set up the scope for your pen test, the Node host is NOT within the specified CIDR range(s) for the test.

NOTE: When Node is not in the same IP range as the scope, it will not execute man-in-the-middle and pass-the-hash attacks. This is your unrestricted assessment, providing true insight into what is accessible, valuable, and vulnerable from any starting point.



**NOTE: Endpoints Only Scope differs from the Outside Custom Scope approach in that when Node is not in the same IP range as the scope, it will not execute man-in-the-middle and pass-the-hash attacks. Further, with this restricted scope, Node will not chain weaknesses or paths as you have limited the scope to a specific endpoint for this assessment.*

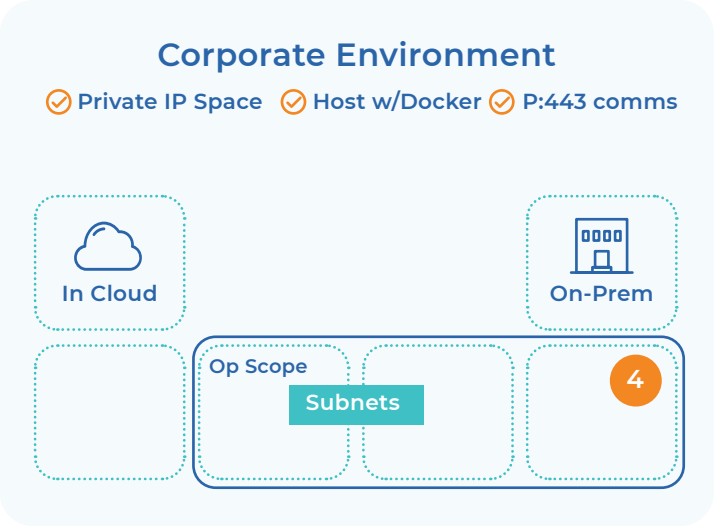
This is your restricted assessment; a quick turnaround op to verify your fix-action was implemented, and a vulnerability less severe to your attack surface.

3 Endpoints Only Scope

Once in a while, you may want to quickly verify if the vulnerability you just remediated had the desired effect. In this case, you can select a single host or range of hosts by /32s

When you set up the scope for your pen test, make sure the Node host has access to the specific host identified by the /32 CIDR range(s) for the test.

When you set up the scope for your pen test, just make sure the Node host is NOT within the specified CIDR range(s) for the test.

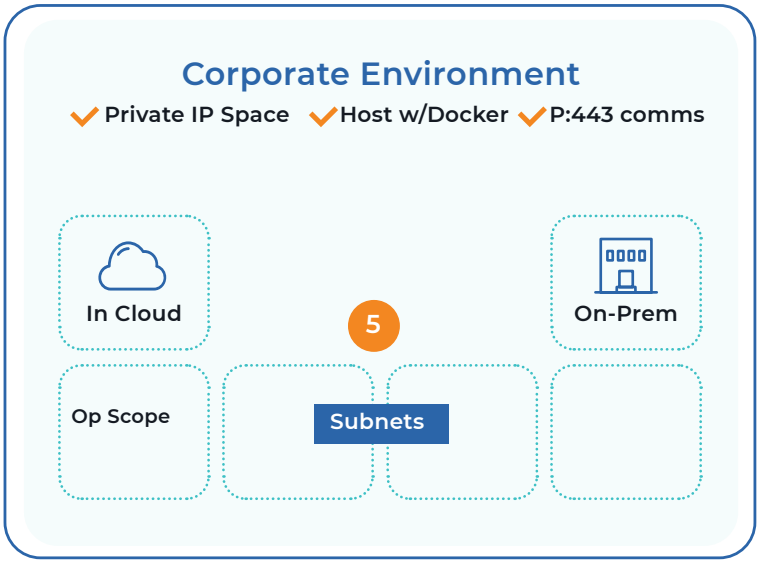


4 Intelligent Scope

Let's say you wanted to see what an uncredentialed attacker could enumerate and exploit from a specific starting point in your network – "black box" pen test – this calls for Intelligent Scope.

When you set up the scope for your pen test, leave the "Include" box blank. Node Zero's host subnet will provide the initial scope and expand organically during the pen test as more hosts and subnets are discovered, just like an attacker would.

This is your proactive assessment; providing accurate insight into what is accessible, valuable, and vulnerable from any starting point.



NOTE: This op may take a bit longer as Node enumerates any IPs and DNS names it can access…including edge routers; if yours are misconfigured for routing private IPs, Node may attempt to enumerate those external private IPs.

PRO TIP: if you want to see EVERYTHING, put Node in an unrestricted ACL so it can discover every nook and cranny online in your environment. This is your unrestricted and holistic enterprise assessment–and should be run regularly.

5

All Private IP Scope (i.e., RFC 1918)

And when you are really ready to roll, you'll love the ability to run an RFC 1918 full private scope pen test, enumerating everything accessible quickly and safely.

Deployment options - Your operation launch point matters

	Custom Scope			Intelligent Scope	RFC 1918	OSINT
	1	2	3	4	5	6
NodeZero placement	Inside the Scope	Outside the Scope	Outside @ endpoints (i.e. /32s)	Attack starting point	Full private scope	NOTE: CloudZero launches externally
Intent	I want to limit the scope and see what an attacker could exploit from that defined range	I want to limit the scope to see if an attacker can access host and data inside	I want to look at specific endpoints to check for host vulnerabilities	I want to see what an attacker can discover and access from a specific starting point	I want to search every nook and cranny of private IP space accessible in my environment	I want to see what publicly available data makes our business vulnerable to an attacker
Will enumerate and exploit	In-scope hosts, services domain, web, credentials, & data resources Pro-tip: ensure a DC is “in-scope”	In-scope hosts, services, web credentials (except MITM and PTH attacks) and cloud assets	Specified hosts, ports, services, web and certs, exploitable vulnerabilities	Discovered hosts, services, domain, web, credentials & data resources	Discovered hosts, services, domain, web, credentials & data resources	Publicly available user names, subdomains, (from TLDs), and web-facing attack surface
Won’t execute	On anything outside the prescribed scope	Man-in-the-middle attacks	On infrastructure nor chained vulnerabilities or misconfigurations that could lead to compromise	On inaccessible hosts, services, domain, web, credentials	On inaccessible hosts, services, domain, web, credentials	On internal assets *Note: When combined with an internal op w/access to a DC, will verify user/password access
Use cases	• Internal pen test • SOC SLAs • Verify policies • Verify EDM/ SIEM	• Internal pen test • Verify segmentation • Verify access to a sensitive VLAN • Third party security assessment	• Test EDR • Assess endpoint vulnerabilities	• Internal pen test • Verify segmentation • Verify policies • Verify EDM/ SIEM • Test blast radius • Test ZeroTrust	• Internal pen test • Environment & asset discovery • Assess hybrid environment • Verify policies • Verify EDR/ SIEM	• Public-facing reconnaissance • Company recon • User recon • Subdomain recon • Cred stuffing

The Portal and MNJ/Adlumin Integration:

MNJ/Adlumin operates under one application; one license concept delivering a command center for security operations to our customers. Customers can come to the MNJ/Adlumin portal and receive data and reporting on critical information about the service and the performance of the service itself. The standard is being able to convey accurate statistics about the performance and results of the service, for example:

1. Date of the last pen test
2. Monitoring the status of a pen test while it is running
3. Retrieving pen test reports after completion

Every customer can come to MNJ/Adlumin to produce an executive-level report that contains all these statistics as well as visually see results and service performance metrics in a dashboard.

About MNJ

MNJ is a leading Digital Transformation and IT Solutions Provider. We'll keep you ahead of the curve with our proven practice areas, focus on customer success, and extensive partner ecosystem.

Experience & Expertise

- 50+ Alliance Software Engineers
- 200+ Alliance Data Centers
- 21 years average experience for MNJ engineers

Consistent Execution

- 20 years in business
- 12 years average customer tenure
- 2,800 active satisfied customers

Company Culture

We're a women-owned family business and we treat our employees and customers like family. We're friendly, passionate, and committed to excellence.

Monitor and defend your network locally, in the cloud, and across the globe. Reach out to one of our specialists at **mnjats@mnjtech.com** to learn more about the premier command center for security operations.