ZERO Networks

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

USE CASES

Pass a Pen Test With Flying Colors

TL;DR

Whether taken to comply with regulations or to uncover and resolve security issues within an organization, penetration tests (or 'pen tests') are notoriously hard to pass.

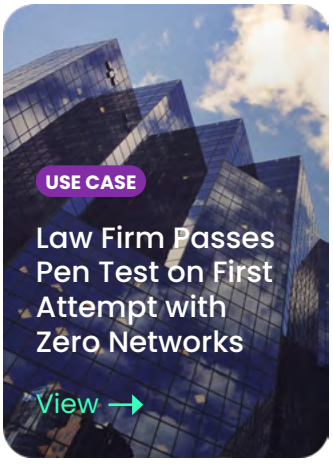
Instead of reactively dealing with each issue the pen test reveals, Zero Networks is proactive: Leveraging automated, agentless microsegmentation and multi-factor authentication (MFA) to solve the underlying root cause of why these issues happen in the first place.

The Pen Test Challenge

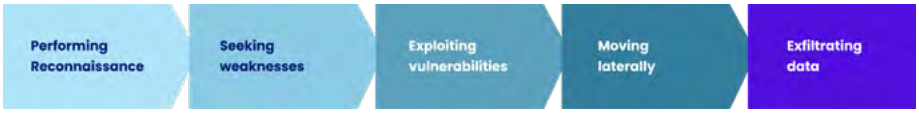
A penetration test (or 'pen test' for short), is a type of cybersecurity assessment that is designed to simulate how and to what extent an attacker can cause damage to the organizational network.

Successfully passing a mandated or even voluntary pen test proves the organization can safeguard itself against a variety of attacks. Plus, many cyber insurance companies and various regulations require a "green" pen test as part of their policy.

During a pen test, various tactics are used in the company's network to assess its resilience. Many of these tests are notoriously difficult to pass—even with the best security solutions. A tight timeline, a limited budget, a small IT team—these are some common organizational challenges that make passing a pen test even harder than it should be.



How pen-testers (and attackers) are operating:



Main reason for pen test failure: Excessive network permissions

The root cause of most failed pen tests – as well as real network breaches – is excessive network permissions. Networks were designed for connectivity, not security, and tend to be wide open from the inside, allowing machines more network access than they need or ever should have. This simplifies an attacker's ability to move laterally once they manage to compromise one machine.

Simulating an attack, pen tests start with one "compromised" machine, from which the pen testers can perform various types of reconnaissance, identify misconfigurations, use weak protocols to exploit vulnerabilities and move laterally to identify how an attacker may exfiltrate data or encrypt it with ransomware.

Glossary

What is a security breach? Learn how to identify and protect against them

View →

The Zero Networks Way: Putting microsegmentation "to the pen test" with just in time MFA

Instead of reactively dealing with each issue the pen test reveals, Zero Networks Segment takes a proactive approach to tackle the root cause of why breaches happen. Zero Networks leverages automated, agentless microsegmentation (segmenting every asset with a firewall) to consolidate network permissions, leaving only what's actually required, and applying just-in- time MFA for sensitive, privileged connections that attackers usually use. Zero Networks Segment is a simple, turnkey solution designed for a set and forget approach. It learns all network traffic for up to 30 days, then creates highly accurate rules and policies, and centrally applies them on the host firewalls of every asset in the network – every client or server, on prem or in the cloud. All privileged ports used for remote admin protocols such as RDP, SSH or WinRM are closed by default, and only open for a limited time for privileged users after authenticating with MFA. With Zero Networks, all ports remain invisible to attackers to block lateral movement. MFA-enabled microsegmentation ensures that organizations pass a pen test on the first attempt: Reconnaissance can't gather information about the network behind ports that are now closed, vulnerabilities cannot be identified and exploited behind closed ports, and lateral movement is impossible because of (you guessed it) closed ports. Ultimately, if attackers cannot see anything in the organizational network, they cannot exfiltrate or encrypt its data.

ABOUT SRC CYBER SOLUTIONS LLP

SRC Cyber Solutions LLP is a renowned name in India for Cybersecurity. We are known for our exclusive distribution of cutting-edge solutions in India, GCC, Africa and APAC. We take pride in offering a comprehensive suite of Cybersecurity solutions which includes Platforms and Technologies for AI-powered Comprehensive Email Security, Automated Patch and Endpoint Management,Asset Visibility and Risk Management, securing the Cloud environments with Hybrid Cloud Workload Protection, enhancing Network Security with Agentless Micro- Segmentation, ensuring Third-Party Data Flow Management and API Management, and Agentless Compliance Management, thereby strengthening our commitment to protecting organizations against evolving known and unknown Cyber Threats. With a focus on embracing innovation, we continuously evolve to meet the dynamic threat landscape, offering a comprehensive range of Nex-Gen technologies with a high degree of automation, reducing the dependency on IT Resources and ensuring a strong value proposition.