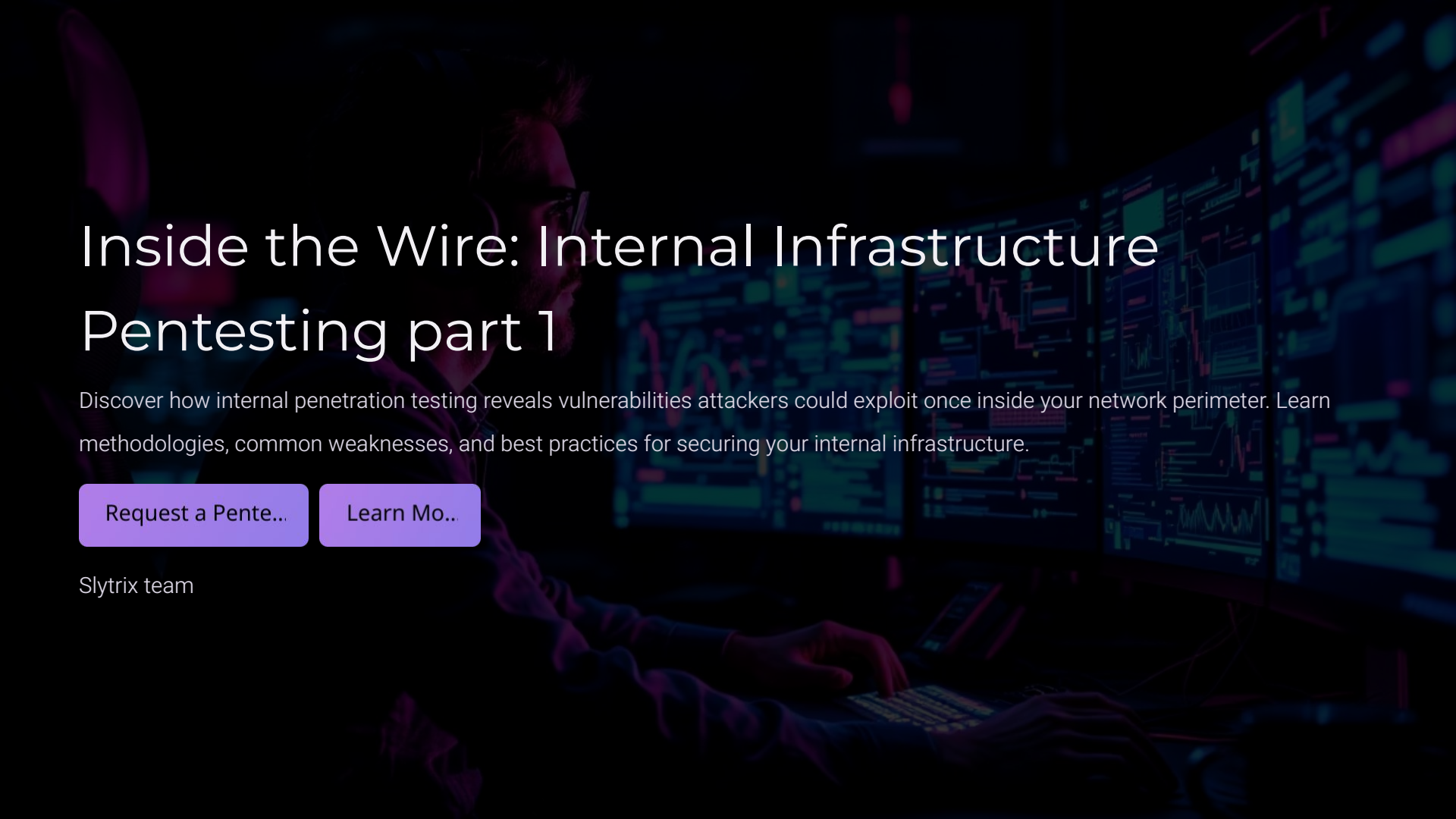


Inside the Wire: Internal Infrastructure Pentesting part 1

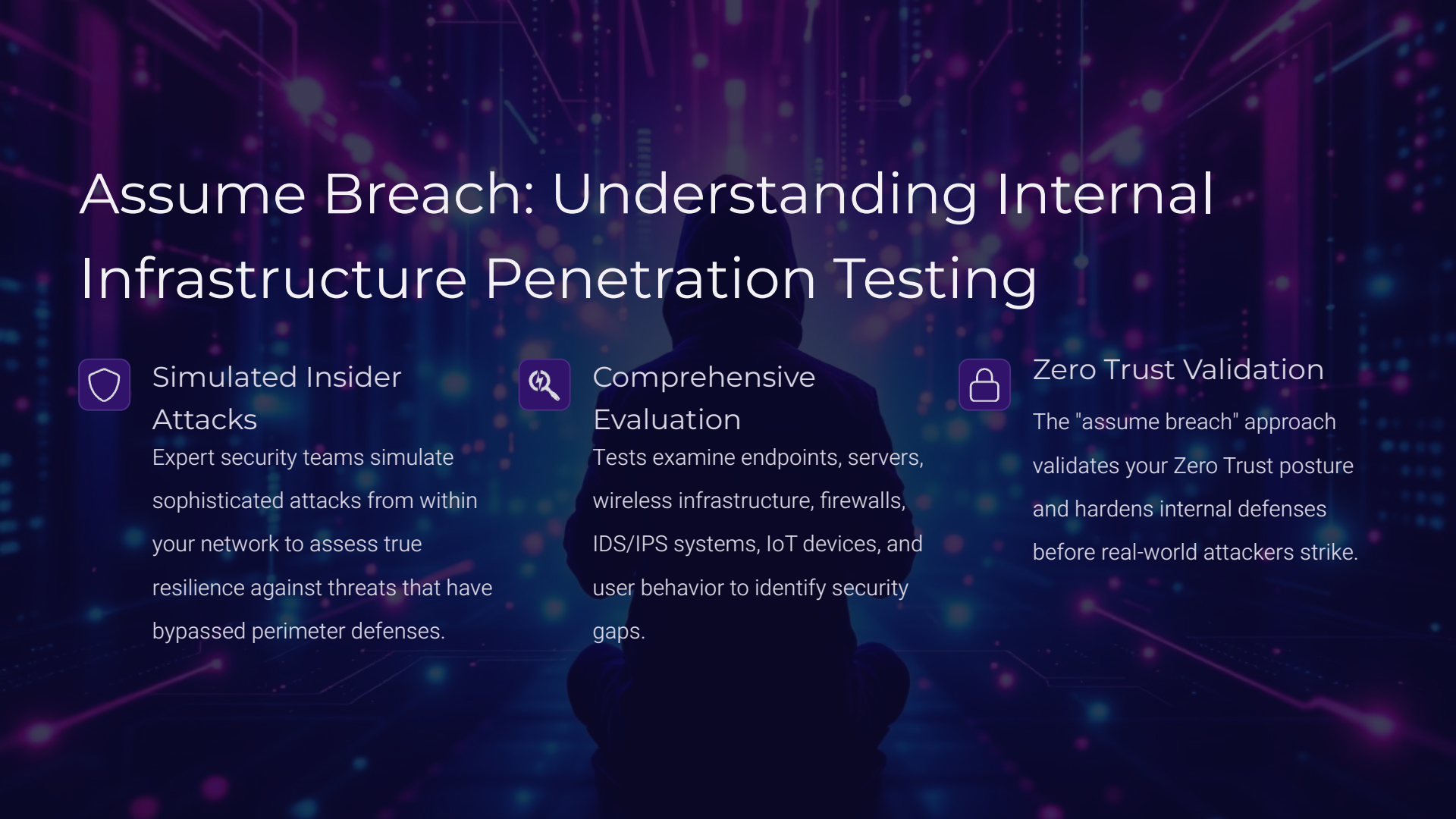
Discover how internal penetration testing reveals vulnerabilities attackers could exploit once inside your network perimeter. Learn methodologies, common weaknesses, and best practices for securing your internal infrastructure.

Request a Pente...

Learn Mo...

Slytrix team

Assume Breach: Understanding Internal Infrastructure Penetration Testing



Simulated Insider Attacks

Expert security teams simulate sophisticated attacks from within your network to assess true resilience against threats that have bypassed perimeter defenses.

Comprehensive Evaluation

Tests examine endpoints, servers, wireless infrastructure, firewalls, IDS/IPS systems, IoT devices, and user behavior to identify security gaps.

Zero Trust Validation

The "assume breach" approach validates your Zero Trust posture and hardens internal defenses before real-world attackers strike.

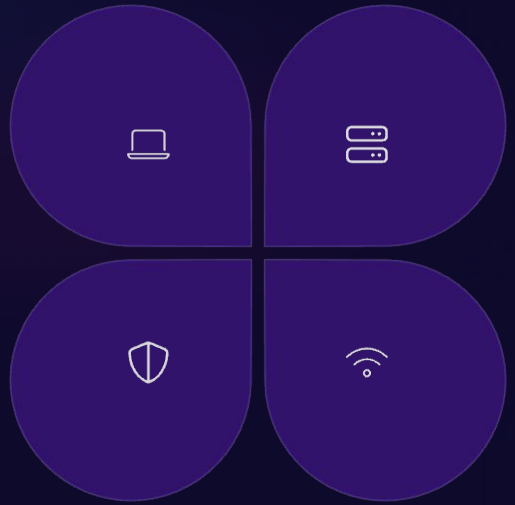
What We Evaluate During Internal Pentests

Endpoints & Devices

Desktop workstations, laptops, and mobile devices—identifying unpatched OS, insecure configurations, and weak endpoint protections.

Security Controls

Internal firewalls, ACLs, NAC solutions—verifying rule accuracy, segmentation effectiveness, and bypass opportunities.



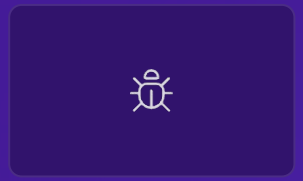
Servers & Network Hardware

Domain controllers, file servers, routers, and switches—scanning for misconfigurations, open ports, and outdated firmware.

Wireless Infrastructure

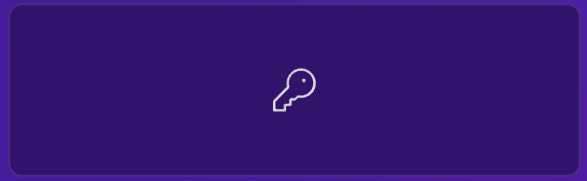
Wi-Fi networks and access points—detecting rogue APs, weak encryption (WPA2/WPA3), and SSID spoofing.

The Primary Objective of Internal Pentesting



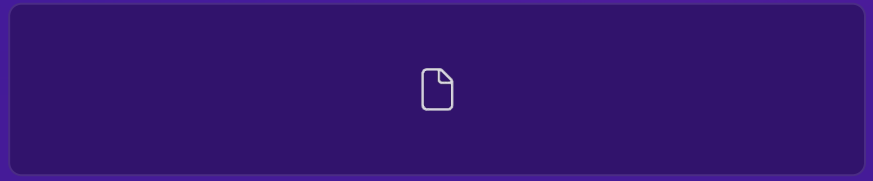
Identify Vulnerabilities

Discover critical security gaps before attackers do



Exploit Weaknesses

Test real-world attack scenarios and techniques



Document Findings

Provide actionable remediation guidance

Internal penetration testing identifies, exploits, and documents critical vulnerabilities such as inadequate access controls, lateral movement vectors, and privilege escalation paths that could enable unauthorized access, data exfiltration, and network compromise.

Identity and Access Management Weaknesses

Weak Passwords

Easily cracked credentials via brute-force or dictionary attacks provide initial access points for attackers.

Inadequate Access Controls

Permissions that allow unauthorized users to access sensitive resources create dangerous security gaps.

Over-Privileged Accounts

Service accounts with excessive administrative permissions enable privilege escalation across environments.

Default Credentials

Unchanged factory settings on routers, printers, or legacy applications offer easy network entry points.

These identity and access management flaws serve as the initial entry points for attackers and often facilitate privilege escalation and lateral movement across the environment.

Network Configuration Flaws

LLMNR/NetBIOS Spoofing

Allows credential interception in Windows environments

Disabled SMB Signing

Enables man-in-the-middle attacks on file sharing

Flat Networks

Little or no segmentation between critical assets and general endpoints

Weak Firewalls

Inadequate configurations and poorly implemented ACLs

Misconfigured networks are a goldmine for attackers during internal penetration tests. These flaws often allow lateral movement and privilege escalation once an initial foothold is established.

Unpatched Systems and Legacy Vulnerabilities

Missing OS-Level Patches

Outdated Windows/Linux systems vulnerable to privilege escalation exploits like PrintNightmare or Dirty Pipe

Outdated Applications

Internal tools running vulnerable versions of Tomcat, JBoss, or Apache

Legacy Systems

Unsupported Windows Server 2008 machines or end-of-life routers still in production

Insecure Configurations

Admin panels without authentication, verbose error messages, or services running with SYSTEM privileges

Why Legacy Vulnerabilities Matter

70%

Hidden From View

Legacy vulnerabilities are rarely scanned by external vulnerability management tools

90%

False Security

Often assumed to be protected behind "trusted" firewalls

65%

Patching Challenges

Operationally risky to update, so they remain vulnerable indefinitely

Once attackers gain an initial foothold (e.g., via phishing or credential reuse), these weaknesses can be used to escalate privileges, execute lateral movement, and potentially compromise the entire domain.