Inside the Wire: Internal Infrastructure Pentesting part 2

Discover advanced tools and methodologies used by red teams to simulate real-world attacks within corporate networks, along with practical recommendations for hardening your internal infrastructure against lateral movement and privilege escalation.

Request a Pente...

Learn Mo...

Essential Red Team Arsenal

Red teams utilize a sophisticated toolkit to simulate real-world attack scenarios within corporate networks. These tools help identify vulnerabilities and demonstrate potential privilege escalation paths that malicious actors might exploit.

Metasploit

Open-source framework for discovering and exploiting security vulnerabilities

Cobalt Strike

Professional-grade post-exploitation tool for Red Team operations and adversary simulations

BloodHound

Maps and analyzes Active Directory environments to reveal privilege escalation paths

Mimikatz

Extracts plaintext passwords and credentials from Windows systems

Advanced Penetration Testing Tools

Beyond the core toolkit, penetration testers rely on specialized tools for network reconnaissance, traffic analysis, and credential harvesting to gain a comprehensive view of potential attack vectors.

PowerShell Empire

Post-exploitation framework leveraging PowerShell to maintain persistence on compromised machines

Responder

Credential harvesting tool that intercepts authentication requests on internal networks

Nmap

Network scanner used to identify open ports and services across target systems

Wireshark

Packet analyzer for capturing and inspecting network traffic in real-time

Structured Penetration Testing Methodology

Internal penetration testing follows a systematic approach to ensure comprehensive coverage and actionable results. The "Assume Breach" methodology is particularly effective, as it evaluates security posture under the assumption that perimeter defenses have already been compromised.

Planning

Define test scope, engagement objectives, and rules of engagement

Discovery

Conduct reconnaissance to gather data about the internal environment

Attack

Exploit discovered vulnerabilities to gain access or escalate privileges

Reporting

Compile comprehensive findings with actionable remediation steps

Network Segmentation & Access Controls

Effective network segmentation is the foundation of a secure internal infrastructure. By creating logical boundaries between different parts of your network, you can contain breaches and prevent lateral movement.

Strong Segmentation

Enforce boundaries with router ACLs, stateful packet inspection, and advanced firewalls to restrict unauthorized traffic flow between network segments.

Demilitarized Zones

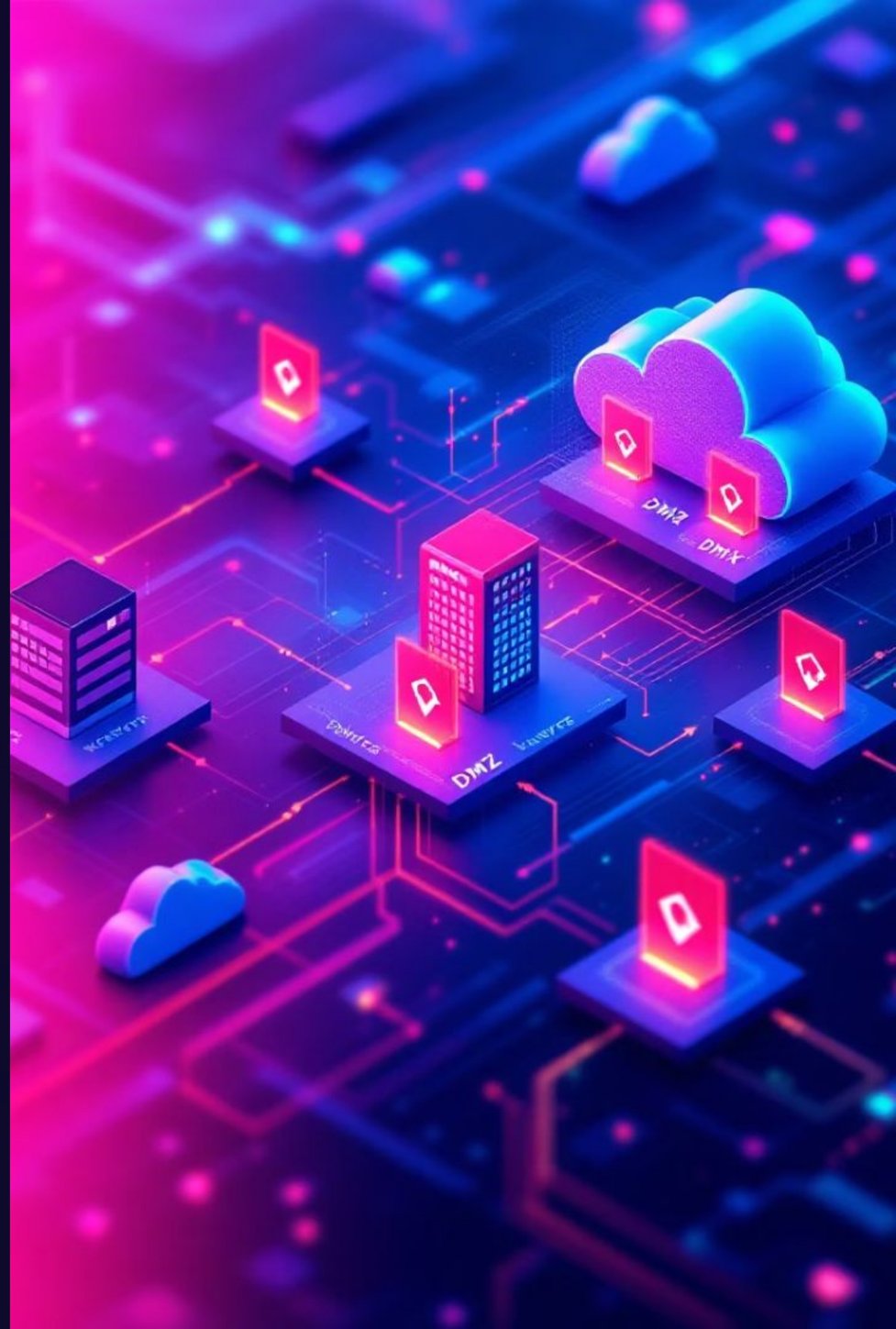
Establish DMZs for externally facing services such as DNS, web, and mail servers to isolate them from internal resources.

VLAN Implementation

Utilize VLANs and PVLANs for additional logical separation, grouping similar devices for streamlined management and enhanced security.

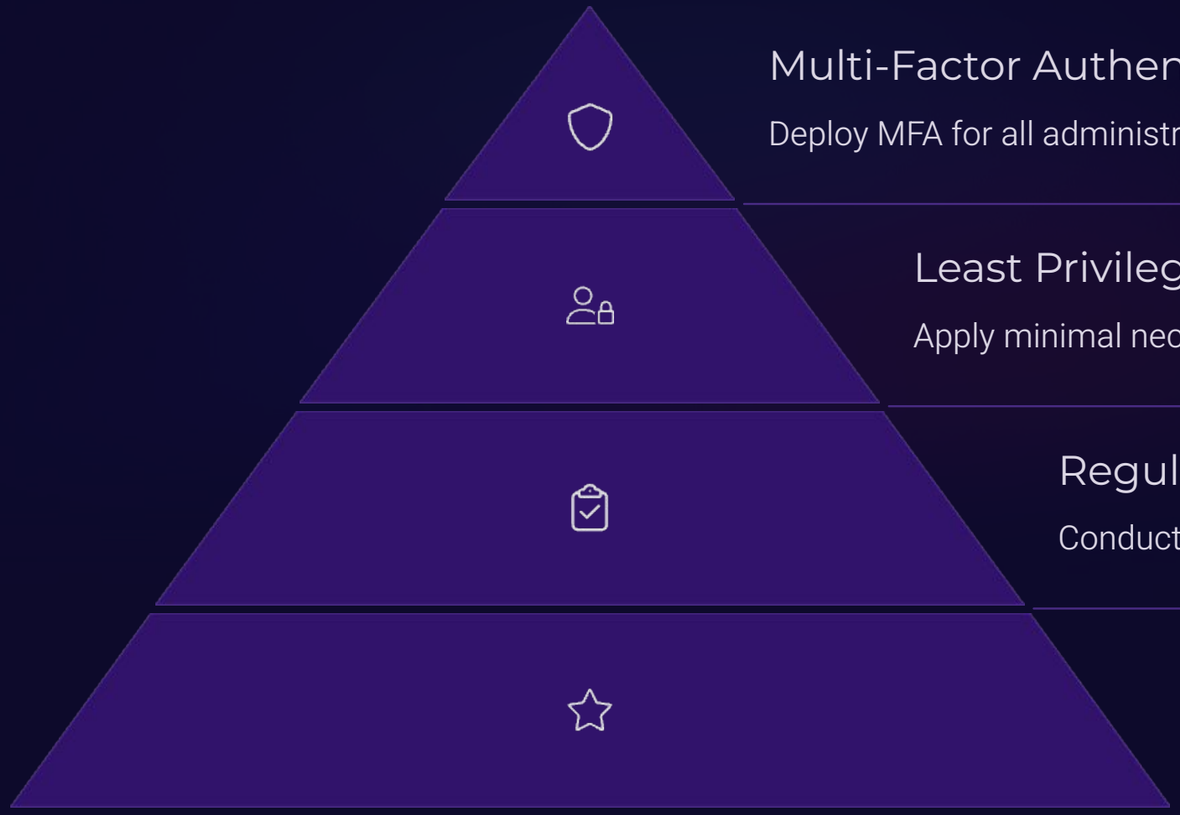
VTY Access Restriction

Restrict VTY access via ACLs to block unauthorized lateral connections between network devices.



Authentication & Access Management

Strong authentication mechanisms and proper access management are critical for preventing unauthorized access to sensitive systems and data within your internal network.



Multi-Factor Authentication

Deploy MFA for all administrative accounts

Least Privilege Principle

Apply minimal necessary permissions to user and service accounts

Regular Permission Audits

Conduct audits and promptly remove excessive rights

Strong Password Policy

Enforce complexity requirements and scheduled rotations

Implementing these authentication controls creates multiple layers of defense against credential theft and abuse, which are common tactics used in lateral movement attacks.

Secure Configuration Management

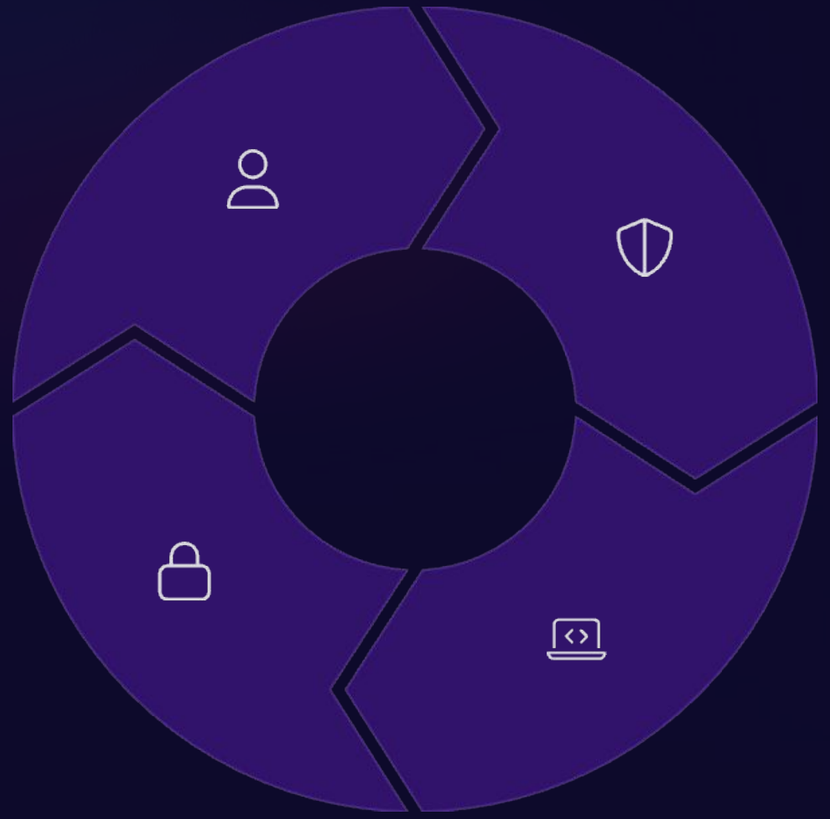
Maintaining secure configurations across all network devices is essential for reducing your attack surface and preventing exploitation of known vulnerabilities.

Centralized Storage

Maintain centralized storage and continuous auditing of all device configurations

End-to-End Encryption

Ensure all sensitive network traffic is encrypted from source to destination



Disable Risky Features

Remove deprecated features and cryptographic algorithms that pose security risks

Restricted Management

Limit device management to trusted endpoints in isolated management zones

Monitoring & Detection Strategies

Comprehensive monitoring and detection capabilities are your last line of defense, enabling you to identify and respond to potential breaches before significant damage occurs.

Centralized Logging

Implement centralized logging for Authentication, Authorization, and Accounting activities and forward logs securely to a dedicated logging server for analysis and retention.

Configuration Change Monitoring

Monitor security configuration changes in real-time to detect unauthorized modifications that could indicate compromise.

IDS/IPS Deployment

Deploy network-based and host-based intrusion detection and prevention solutions to identify and block suspicious activities.

Behavioral Baseline Establishment

Establish a baseline of normal network behavior to detect anomalies and potential attacks through deviation analysis.