ZCorum™

Penetration Testing

Identifying Your Common Vulnerabilities

Introduction

A penetration test (pen test) is a controlled cyber attack simulation designed to assess the security of a system, application, or network.

Unlike automated vulnerability scans, pentesting provides a comprehensive, hands-on evaluation, identifying real-world exploitable vulnerabilities that attackers could leverage. By mimicking adversarial tactics, it helps organizations understand their security weaknesses, validate defenses, and strengthen overall resilience against Cyber threats.

Reasons and Frequency for Conducting a Penetration Test

- **Compliance Requirements:** Many industries impose strict regulatory requirements mandating regular penetration testing. Compliance with standards such as PCI DSS, HIPAA, and GDPR not only enhances an organization's security posture, but also mitigates legal, financial, and reputational risks associated with data breaches. Regular testing ensures that security controls remain effective, helping businesses stay ahead of evolving threats and regulatory obligations.

- **Cyber Insurance:** Cyber insurance providers are increasingly mandating documented penetration tests as a prerequisite for coverage. These assessments serve as proof of due diligence, demonstrating an organization's commitment to proactive cybersecurity measures. A well-conducted pentest can directly impact policy eligibility, premium costs, coverage terms, and overall risk evaluation, helping businesses secure more favorable insurance conditions while strengthening their security posture.

- **Ethical Responsibility:** Organizations have a critical responsibility to safeguard sensitive information. Regular penetration testing reinforces data security, regulatory compliance, and risk management, ensuring that defenses remain resilient against evolving threats. Beyond protecting systems, it also fosters trust and credibility, demonstrating a strong commitment to maintaining high security and privacy.

- **When and How Often?** It is advisable to conduct penetration tests at least once a year or whenever significant IT changes occur. Regular testing enables organizations to proactively detect and mitigate new vulnerabilities arising from system updates, expansions, or infrastructure modifications, ensuring a robust security posture.

Characteristics of a Good Pentest

Ensuring Effective Security Testing

A well-structured penetration test goes beyond identifying vulnerabilities—it evaluates the effectiveness of security controls, detection capabilities, and response strategies.

Key Characteristics Include:

- ✓ **Comprehensive Assessment:** Covers network, applications, and human factors.
- ✓ **Real-World Attack Simulation:** Uses adversarial tactics to test resilience.
- ✓ **Actionable Insights:** Provides clear remediation steps, not just findings.
- ✓ **Positive and Negative Findings:** Highlights strengths along with weaknesses.
- ✓ **Retesting for Validation:** Confirms that security gaps are properly mitigated.

Understanding Control Functionality

- **Assessing Security Effectiveness:** Effective penetration testing evaluates how well an organization's security controls withstand real-world attack scenarios. By simulating adversarial tactics, it goes beyond automated scans to uncover hidden vulnerabilities, misconfigurations, and gaps in defenses.

- **Manipulating Human Interaction:** Social engineering tactics, such as phishing, vishing (voice phishing), and smishing (SMS phishing), can be integrated into penetration tests to assess human vulnerabilities within an organization.

- **Recognizing Security Strengths:** A well-executed penetration test should highlight not only vulnerabilities but also effective security controls. Recognizing successful defenses, best practices, and resilient configurations reinforces security awareness and encourages teams to maintain and expand on existing protections.

- **Penetration Testing and Vulnerability Scanning:** While penetration testing and vulnerability scanning serve different purposes, a pen test often includes a scanning phase. This integration enhances security assessments by identifying vulnerabilities through automated scans and validating their real-world exploitability through manual testing. By combining both approaches, organizations gain a more comprehensive evaluation of their security controls, ensuring weaknesses are not only detected but also effectively assessed for risk.

- **Retesting to Confirm Remediation** A robust penetration testing policy includes retesting to verify the successful remediation of identified vulnerabilities. This crucial step ensures that corrective actions have been effectively implemented and that security gaps are truly closed. By conducting follow-up assessments, organizations gain continuous assurance of their security improvements and reduce the risk of recurring threats.

Common Technique

Living Off the Land

Attackers today will exploit legitimate system tools that come preinstalled in the operating system (usually Windows) to perform reconnaissance on the network before they active their ransomware executables. This allows them to avoid detection. Pentesters are able to use those same LOLBins (Living Off the Land Binaries) to simulate real-world attacks, while also evading security controls.

LOLBins Allow the Pentester to:

- ✓ Bypass application whitelisting and restrictive security policies.
- ✓ Execute payloads stealthily without dropping custom malware.
- ✓ Mimic real-world adversaries to test detection and response capabilities.

Commonly Used LOLBins in Pentesting:

- ✓ cmd.exe & powershell.exe – Execute commands, download payloads, and escalate privileges
- ✓ rundll32.exe – Load and execute malicious DLLs
- ✓ mshta.exe – Execute malicious scripts via HTML applications
- ✓ certutil.exe – Download and decode payloads, often bypassing security filters

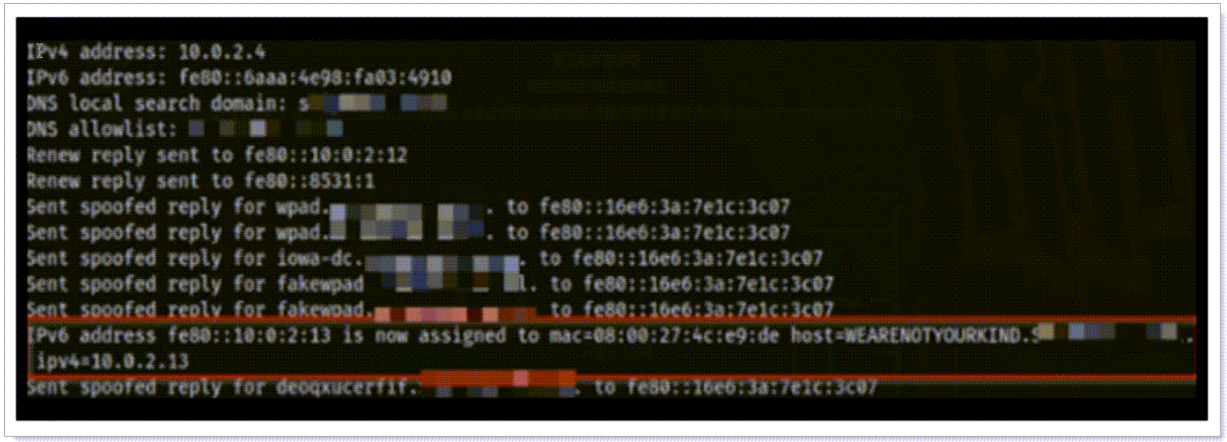
Attack Vectors

IPv6 - Man in the Middle (MiTM V6)

Many networks have IPv6 enabled by default, but lack proper security controls, making them prime targets for MITM attacks.

Pentesters can test for and exploit this by:

- ✓ Spoofing rogue DHCPv6 servers to redirect traffic.
- ✓ MITM6 + NTLM Relay to capture and relay authentication.
- ✓ Abusing WPAD via IPv6 for session hijacking.

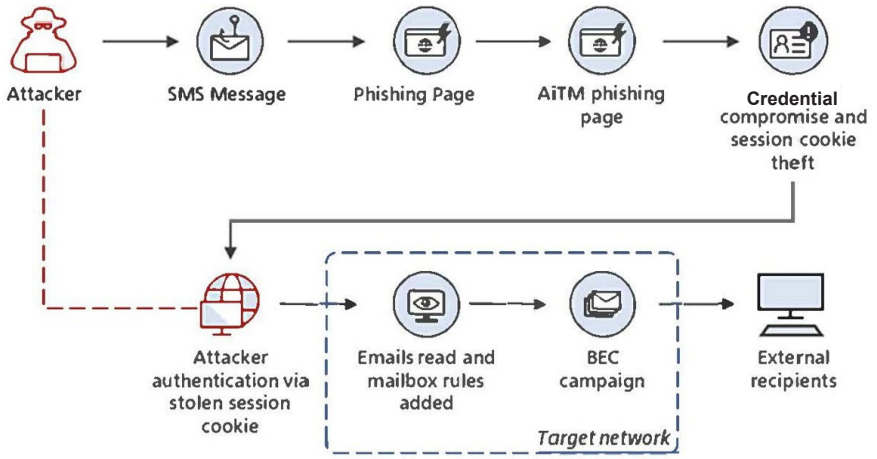


Attack Vectors

Smishing - Man in the Middle

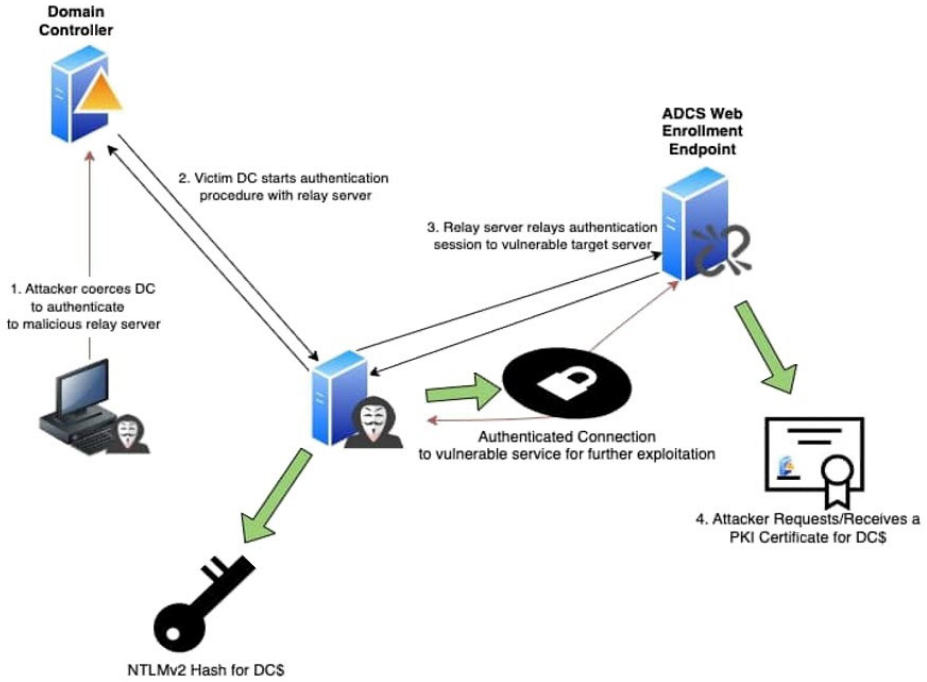
With Phishing via SMS (Smishing) an attacker sends deceptive SMS messages that trick victims into revealing sensitive information.

These messages may contain links to fake websites that mimic legitimate services. When the victim enters their credentials or 2FA codes on these fake websites, the attacker captures the information and can use it to access the victim's accounts.



ADCS Coercion

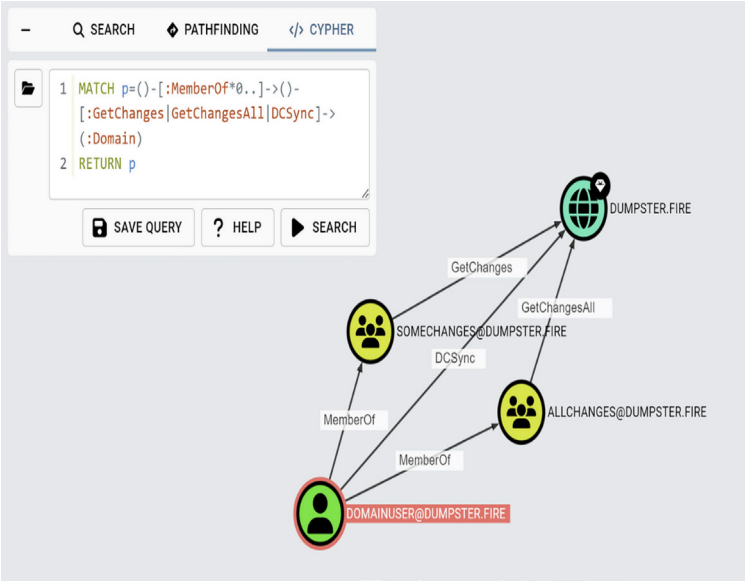
Active Directory Certificate Services (ADCS) can be misconfigured, allowing attackers to coerce authentication from privileged accounts and obtain certificates for NTLM relay attacks. This can lead to privilege escalation or even domain compromise by forging Kerberos tickets (Golden/Silver Ticket attacks).



Active Directory Exploits

Tools like BloodHound help Pentesters identify misconfigurations in Active Directory that enable privilege escalation and lateral movement. Common exploitable issues include:

- ✓ Excessive Privileges – Users with unnecessary DCSync or admin rights.
- ✓ Weak ACLs (Access Control Lists) – Attackers exploit WriteDACL or GenericAll to take over accounts.
- ✓ Kerberoasting & AS-REP Roasting – Identifying weakly encrypted service accounts for offline cracking.
- ✓ Shadow Admins – Users with indirect privilege escalation paths that can be abused.



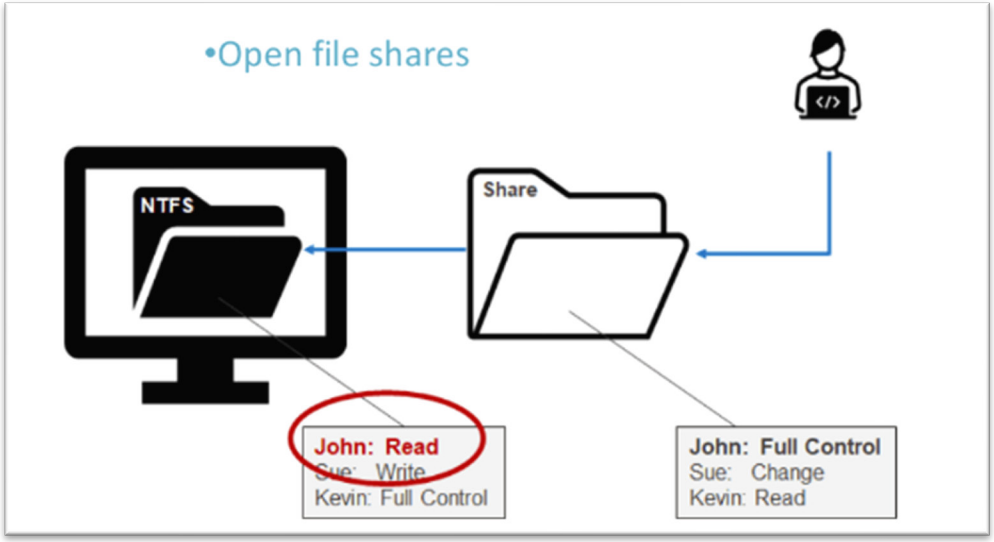
Default Passwords

Pentesters frequently encounter default credentials left unchanged, providing an easy foothold into systems. Many organizations overlook these weak entry points, allowing attackers to gain initial access, escalate privileges, or pivot within networks. Common exploitable issues include:

- ✓ Admin/Admin on network devices (routers, switches, firewalls).
- ✓ Default logins on web apps & databases (e.g., sa:password123).
- ✓ Hardcoded credentials in scripts & configuration files.

Attack Vectors: Open File Shares

Unrestricted file shares can be a goldmine for attackers, often exposing sensitive data, credentials, or scripts that aid in lateral movement and privilege escalation. A pentester can help you find what file shares are out there and what data they contain that can be exploited.



Basic Steps to Improve Network Security

- ✓ Get a Pentest
- ✓ Use strong passwords
- ✓ Implement MFA everywhere
- ✓ Store passwords in a vault
- ✓ Set your Active Directory Machine Account Quota to zero

Next Steps

ZCorum offers comprehensive pentesting for broadband providers. The assessments cover all layers of the network, from subscriber devices to DOCSIS and FIBER infrastructure, providing actionable insights for mitigation and risk reduction.

After testing is completed our reports turn the technical findings into practical recommendations that comply with regulatory and funding requirements. We also offer guidance to ensure that weak spots are corrected without introducing new vulnerabilities. By adding pentesting into an overall security strategy, you will gain a stronger defense and greater subscriber trust.

Take the Next Step in Securing Your Network

Don't wait for an attack to expose your vulnerabilities. Schedule a comprehensive penetration test today to identify weaknesses, validate your defenses, and strengthen your broadband network against evolving cyber threats. Contact our team to learn how a customized assessment can protect your systems, your subscribers, and your reputation. You can also learn more about our cybersecurity solutions on our website at ZCorum.com/cybersecurity.

ZCorum™

4501 North Point Parkway,
Suite 125
Alpharetta, GA 30022
Toll Free: 1-800-909-9441
info@ZCorum.com

ZCorum provides broadband Internet and communication solutions to telcos, cable companies, utilities, and municipalities, assisting in all facets of broadband implementation, integration, engineering and consulting, cybersecurity network monitoring and diagnostics. ZCorum also offers wholesale, private-labeled Internet services, including data and VoIP provisioning, email, Web hosting, and 24x7 support for end-users, enabling service providers to compete effectively in their local rural and suburban markets. ZCorum is headquartered in Alpharetta, GA.