Active Directory (AD) penetration testing is a crucial aspect of securing an organization's infrastructure. This roadmap outlines a structured approach to performing Active Directory penetration testing. Keep in mind that penetration testing should only be conducted in environments where you have explicit permission.

Phase 1: Pre-engagement

Define Scope:

Clearly define the scope of the penetration test, including the target AD infrastructure, systems, and applications.

Gather Information:

Collect information about the target organization, such as network architecture, domain names, IP ranges, organizational structure, and publicly available information.

Legal and Compliance:

Ensure that all legal and compliance requirements are met, including obtaining written permission from the organization.

Phase 2: Reconnaissance

Network Discovery:

Identify domain controllers, servers, and other network devices.

Enumerate subnets, IP addresses, and network services.

OS and Application Fingerprinting:

Identify operating systems and versions.

Discover running services and their versions.

Active Directory Enumeration:

Enumerate AD information using tools like LDAP queries, DNS zone transfers, and SMB queries.

Phase 3: Vulnerability Analysis

Identify Vulnerabilities:

Conduct vulnerability scanning on systems and applications.

Analyze the results to identify potential weaknesses.

AD-specific Vulnerabilities:

Focus on vulnerabilities specific to Active Directory, such as insecure group policies, misconfigured permissions, and weak trust relationships.

Phase 4: Exploitation

Credential Attacks:

Attempt to obtain credentials through techniques like password spraying, credential stuffing, or phishing attacks.

Lateral Movement:

Exploit vulnerabilities to move laterally within the network.

Enumerate shares, sessions, and user privileges.

Privilege Escalation:

Identify and exploit opportunities to elevate privileges within the AD environment.

Exploit misconfigurations, weak permissions, or known vulnerabilities.

Phase 5: Post-exploitation

Maintain Persistence:

Establish and maintain persistent access to the network.

Identify and use techniques to avoid detection.

Data Exfiltration:

Attempt to exfiltrate sensitive data to simulate a real-world threat.

Phase 6: Reporting

Document Findings:

Compile a comprehensive report detailing vulnerabilities, exploited weaknesses, and potential impact.

Risk Prioritization:

Prioritize findings based on risk, providing recommendations for remediation.

Mitigation Strategies:

Offer clear and actionable mitigation strategies to address identified vulnerabilities.

Phase 7: Debriefing

Client Debrief:

Present findings and recommendations to the client.

Discuss any additional insights gained during the testing.

Lessons Learned:

Conduct an internal review to identify lessons learned and improve future testing processes.

Additional Tips:

Continuous Learning:

Stay updated on the latest Active Directory attack techniques, tools, and mitigation strategies.

Engage Red Teamers:

Collaborate with red teamers to simulate advanced persistent threats and enhance the depth of testing.

Adherence to Ethical Standards:

Ensure that testing is conducted ethically and in accordance with industry standards.

The goal is not only to identify vulnerabilities but also to help the organization improve its security posture. Regularly update the roadmap based on emerging threats and new security measures.