Active Directory Pentesting

Index

Introduction to Active Directory

Active Directory (AD) is a directory service developed by Microsoft for Windows domain networks. It is a centralized and standardized system that automates network management of user data, security, and distributed resources. AD allows administrators to manage permissions and access to network resources efficiently.

Practical Scenario: A company uses Active Directory to manage user accounts, computers, and resources within its network. This setup allows IT administrators to control access permissions, implement security policies, and manage software deployment across the organization.

Active Directory Architecture

1. Domain Controllers (DCs): Servers that respond to authentication requests and verify users in computer networks. They host the Active Directory database, which contains information about the domain, users, and computers.

2. Forests, Trees, and Domains:

- **Forest:** The top-level container that houses multiple domains and trees, representing the security boundary within an organization.
- **Tree:** A collection of one or more domains that share a common namespace.
- **Domain:** A logical grouping of objects (users, computers, etc.) that share the same Active Directory database.

3. Organizational Units (OUs): Containers within a domain that can hold users, groups, computers, and other OUs. They help organize and manage objects efficiently.

4. Global Catalog: A distributed data repository that contains a searchable, partial representation of every object in every domain within a forest.

Practical Scenario: In a multinational corporation, the AD structure might include separate domains for different regions (e.g., Europe, Asia, Americas), each with its own OUs for departments like HR, IT, and Sales. The Global Catalog allows users to search for resources across the entire organization.

Active Directory Installation and Configuration

1. Pre-Installation Requirements:

- Windows Server operating system.
- Static IP address for the server.
- Proper network and DNS configuration.

2. Installation Steps:

- Install the Active Directory Domain Services (AD DS) role.
- Promote the server to a Domain Controller.
- Configure DNS, select a domain name, and create the necessary objects.

3. Post-Installation Configuration:

- Set up Organizational Units (OUs).
- Create and manage user accounts and groups.
- Implement Group Policy Objects (GPOs) for security and management.

Practical Scenario: A company setting up a new branch office installs Active Directory on a server to manage local resources and integrate with the central AD infrastructure. This includes creating user accounts for employees and configuring GPOs to enforce security settings, such as password policies and software restrictions.

Active Directory Penetration Testing Overview

Penetration Testing (Pen Testing) involves evaluating the security of a system by simulating attacks from malicious outsiders and insiders. In the context of AD, pen testing focuses on identifying vulnerabilities in the directory services and exploiting them to assess the organization's security posture.

Goals of AD Pen Testing:

- Identify misconfigurations and weaknesses.
- Test the effectiveness of security controls.
- Simulate real-world attack scenarios to evaluate the organization's detection and response capabilities.

Practical Scenario: An organization contracts a security firm to conduct an AD penetration test. The testers aim to identify vulnerabilities, such as weak passwords, unpatched systems, and inadequate access controls, to improve the company's security posture.

Reconnaissance and Information Gathering

1. Passive Reconnaissance:

- Gathering publicly available information without direct interaction with the target system.
- Techniques include searching online forums, job postings, and social media for information about the organization's AD structure and technology stack.

2. Active Reconnaissance:

- Directly interacting with the target system to gather information.
- Techniques include network scanning, querying DNS records, and using tools like nslookup, Nmap, and Netcat to identify domain controllers, services, and potential entry points.

Practical Scenario: During the reconnaissance phase, a penetration tester discovers an open LDAP port on a domain controller. Further investigation reveals that the server is configured to allow anonymous queries, exposing sensitive information such as usernames and group memberships.

Exploiting AD Vulnerabilities

1. Credential Harvesting:

- Techniques like phishing, brute force attacks, or leveraging misconfigured services (e.g., SMB, LDAP) to obtain valid credentials.

2. Privilege Escalation:

- Exploiting weak permissions, vulnerable software, or misconfigurations to escalate privileges, gaining administrative access.

3. Kerberos Attacks:

- **Pass-the-Ticket (PtT):** Using stolen Kerberos tickets to authenticate as a user without knowing the password.
- **Kerberoasting:** Extracting service account credentials from Kerberos tickets for offline brute force attacks.

Practical Scenario: A tester exploits a weak password policy by using a brute-force attack to obtain credentials for a user account with elevated privileges. With this access, they perform a "pass-the-ticket" attack to impersonate a domain admin and gain full control over the domain.

Post-Exploitation Techniques

1. Persistence:

- Establishing a long-term presence in the network by creating new user accounts, backdoors, or modifying legitimate services.

2. Lateral Movement:

- Moving within the network to access additional systems and data, using tools like PsExec or WMI for remote command execution.

3. Data Exfiltration:

- Extracting sensitive data from the network without detection. Techniques include using encrypted channels, steganography, or splitting data into smaller parts.

Practical Scenario: After gaining domain admin privileges, a tester creates a new user account with administrative rights, ensuring persistent access. They then use the account to explore other systems within the network, gathering confidential data like financial records and employee information.

Defensive Measures and Mitigations

1. Strengthen Password Policies:

- Enforce complex passwords, regular changes, and prevent reuse of old passwords.

2. Patch Management:

- Regularly update systems to fix vulnerabilities in operating systems and applications.

3. Secure AD Configuration:

- Limit administrative privileges, use multi-factor authentication (MFA), and secure Kerberos by enforcing strong encryption.

4. Monitoring and Detection:

- Implement logging and monitoring solutions to detect unusual activity. Use tools like SIEMs (Security Information and Event Management) for real-time analysis.

5. Incident Response Plan:

- Develop and regularly update an incident response plan. Train staff on how to respond to security incidents, including containment, eradication, and recovery.

Practical Scenario: Following a penetration test, an organization implements stricter password policies and deploys MFA for all users. They also update their AD configurations to limit administrative privileges and regularly review security logs to detect and respond to potential threats.

Lab Guide for Active Directory Penetration Testing

Lab Setup:

1. **Environment:** A virtual lab environment with a Windows Server configured as a Domain Controller and several client machines.
2. **Tools Required:**
   - Network scanning tools (e.g., Nmap, Netcat)
   - Exploitation tools (e.g., Metasploit, Mimikatz)
   - Post-exploitation frameworks (e.g., Cobalt Strike)
   - Logging and monitoring tools (e.g., Splunk, ELK Stack)

Lab Activities:

1. **Reconnaissance:**
   - Perform network scans to identify AD domain controllers.
   - Query DNS records and LDAP services to gather information about the domain structure.
2. **Exploitation:**
   - Attempt password attacks on user accounts identified during reconnaissance.
   - Use Kerberoasting techniques to extract service account credentials.
   - Exploit misconfigurations or unpatched vulnerabilities to gain administrative access.
3. **Post-Exploitation:**
   - Establish persistence by creating new admin accounts.
   - Use lateral movement techniques to explore other systems within the domain.
   - Extract sensitive data and document the methods used.
4. **Mitigation and Defense:**
   - Apply security patches and updates.
   - Implement robust password policies and MFA.
   - Configure auditing and monitoring for suspicious activities.

- Review and update the incident response plan based on findings.