Active Directory Simulation Team

Penetration Testing Report: Active Directory Attack Simulation

Version 1.0

04/14/2019

Submitted to:

Active Directory Simulation Team

Content

I. Introduction

This report provides a comprehensive overview of the penetration testing conducted on the Active Directory (AD) environment. The goal of the assessment was to identify potential vulnerabilities, misconfigurations, and weaknesses that could be exploited by attackers to compromise the AD infrastructure.

II. Summary of Findings

The following critical vulnerabilities and misconfigurations were identified during the assessment:

1. **Enumeration of Active Directory:**
    - Successful enumeration using tools such as BloodHound and CrackMapExec revealed sensitive information about the AD environment, including users, groups, and permissions.
2. **AS-REP Roasting:**
    - Identified users with “Do not require Kerberos pre-authentication” enabled, making them vulnerable to AS-REP roasting attacks.
3. **SMB Signing Disabled:**
    - Lack of SMB signing allowed for NTLM relay attacks using tools like ntlmrelayx.py.
4. **Password Spraying:**
    - Weak password policies were exploited using CrackMapExec and other tools to successfully compromise accounts.

5. **Lateral Movement:**
    - Techniques like Pass-the-Hash, SMB relaying, and abusing ACLs/ACEs enabled lateral movement across the network.
6. **Privilege Escalation via DNSAdmins Misconfiguration:**
    - Exploitation of the DNSAdmins group allowed for injection of a malicious DLL, achieving SYSTEM-level privileges.
7. **DCSync Attack:**
    - Abuse of DCSync privileges allowed extraction of domain credentials, including the KRBTGT hash.
8. **Data Exfiltration:**
    - Critical data, such as user hashes and password dumps, was successfully extracted using tools like Mimikatz and secretsdump.py.

Severity Scoring Table

The identified vulnerabilities have been scored based on their severity to prioritize mitigation efforts. The scoring is based on the Common Vulnerability Scoring System (CVSS).

Vulnerability	Severity	CVSS Score
Enumeration of Active directory	High	7.5
AS-REP Roasting	High	8.0
SMB signing disabled	critical	9.0
Password spraying	High	7.5
Lateral movement	critical	9.0
Privilege Escalation via DNSAdmins Misconfiguration	critical	9.5
DCSync Attack	critical	10.0
Data Exfiltration	critical	9.5

III. Detailed Findings and Exploits

1. Enumeration of Active Directory

- **Tools Used:**
  - BloodHound-python
  - CrackMapExec
  - Nmap
  - Nbtscan
- **Key Findings:**
  - BloodHound identified potential attack paths to domain admins.
  - CrackMapExec provided an overview of accessible SMB shares and users.
  - Nmap scans revealed multiple open ports, including SMB (445) and RPC (139).

2. AS-REP Roasting

- **Attack:**
  - Using Impacket's GetNPUsers, hashes for accounts with the "DONT_REQ_PREAUTH" attribute were successfully extracted.
- **Impact:**
  - The extracted hashes can be cracked offline to reveal plaintext passwords.

3. SMB Signing Disabled

- **Attack:**
  - NTLM relay attacks using ntlmrelayx.py enabled unauthorized access to systems.
- **Impact:**
  - Unauthorized access to shared resources and lateral movement across the network.

4. Password Spraying

- **Attack:**
  - Conducted password spraying attacks against SMB and WinRM services using CrackMapExec.
- **Impact:**
  - Successfully compromised accounts with weak credentials (e.g., "P@ssw0rd1").

5. Lateral Movement

- **Techniques Used:**
  - Pass-the-Hash (using CrackMapExec and Impacket).
  - Exploitation of SMB shares and WinRM services.
- **Impact:**
  - Movement across the network, compromising additional systems and escalating privileges.

6. Privilege Escalation via DNSAdmins Misconfiguration

- **Attack:**
  - Injected a malicious DLL using the DNSAdmins group and restarted the DNS service to execute the payload.
- **Impact:**
  - Achieved SYSTEM-level privileges on the DNS server.

7. DCSync Attack

- **Attack:**
  - Extracted sensitive data, including domain administrator credentials, using Mimikatz and secretsdump.py.
- **Impact:**
  - Full compromise of the AD environment.

8. Data Exfiltration

- **Techniques Used:**
  - Dumped SAM hashes and AD credentials using Responder, ntlmrelayx, and Mimikatz.
- **Impact:**
  - Potential for significant data breach and further exploitation of compromised accounts.

IV. Recommendations to mitigate

To mitigate the identified risks, the following steps are recommended:

1. **Strengthen Account Security:**
    - Enforce strong password policies and require multi-factor authentication (MFA).
    - Regularly audit user accounts for misconfigurations (e.g., "DONT_REQ_PREAUTH").
2. **Enable SMB Signing:**
    - Configure SMB signing to prevent NTLM relay attacks.
3. **Implement Network Segmentation:**
    - Isolate critical infrastructure from general user networks to limit lateral movement opportunities.
4. **Audit Group Memberships and ACLs:**
    - Restrict sensitive groups (e.g., DNSAdmins) and audit permissions on critical objects.
5. **Patch and Update Systems:**
    - Regularly apply updates to address known vulnerabilities in SMB and other services.
6. **Monitor and Detect Anomalies:**
    - Implement logging and monitoring solutions to detect unauthorized access and privilege escalation attempts.
7. **Educate and Train Staff:**
    - Provide security awareness training to staff to recognize phishing and other social engineering techniques.

V. Conclusion

The penetration test revealed critical vulnerabilities in the Active Directory environment that could lead to significant security breaches if exploited. Addressing the recommendations outlined in this report will greatly enhance the security posture and resilience of the AD infrastructure.

Resources Used

- BloodHound: https://github.com/BloodHoundAD/BloodHound
- Impacket: https://github.com/SecureAuthCorp/impacket
- CrackMapExec: https://github.com/Porchetta-Industries/CrackMapExec
- Evil-WinRM: https://github.com/Hackplayers/evil-winrm