Active Directory Security

Course Incharge: **Yahya Batla**

Course Instructor: **Umar Bilal**

Reference Book

Active Directory Security Guide

Introduction to Active Directory (AD)

- Active Directory (AD): Integral part of modern organizations
- Backbone of identity infrastructure for 90% of Fortune 1000 companies
- Simplifies access to resources and applications with single set of credentials
- Centralized management structure for users, computers, and resources
- Challenges in security breach recovery and importance of disaster recovery plans

Security Challenges in Active Directory

- Liability in security breaches due to widespread use and architectural limitations
- Priority target for adversaries seeking privileges elevation and launching devastating attacks
- Challenges in identifying breach source, determining extent of damage, and creating secure environment
- Statistics: 80% of breaches from external agents, potential for long-term undetected presence

Transition to Microsoft Azure Active Directory (AAD)

- Challenges in retiring outdated AD and adopting more secure alternatives like AAD
- AAD automates administrative tasks for improved efficiency
- Security risks persist; compromise of identity infrastructure can have devastating consequences
- Potential attack paths between separate identity management environments

Importance of Active Directory Security

- Disaster recovery plans and vigilant monitoring crucial for stopping attacks
- Choice between AD and AAD depends on organization's needs and resources
- Regardless of choice, risk of compromise remains
- Clear understanding of potential risks and commitment to security practices required

Active Directory Overview

- AD: Crucial directory service for managing network resources in Windows-based networks
- Centralizes management of user and computer accounts, resources, and security policies
- Hierarchical structure: Domains, users, computers, and groups
- Utilizes LDAP for communication between domains and domain controllers
- Employs Kerberos for secure authentication over a network

Active Directory Features

- Group Policy Objects (GPOs): Control and enforce security policies, software deployment, and administrative tasks
- Remote Procedure Calls (RPCs): Allow remote management of network resources
- Ensures efficient management from centralized location
- Not immune to attacks; successful attacks involve discovery, privilege escalation, and access to other computers

Attack Technique 1: Use of Alternate Authentication Methods (T1550)

- Adversarial attacks can bypass access controls using alternate authentication materials.
- Technique: T1550 in the MITRE ATT&CK framework enables lateral movement and unauthorized access.

Sub-Technique 1: Pass-the-Hash (T1550.002)

- Identity-based attack for gaining access and privileges within a network.

Adversaries:

- Gain initial access to network.
- Steal/dump hashed user credentials.
- Use hashed credentials to create new user session on compromised host.

Pass-the-Hash Attack Overview

- Pass-the-Hash leverages Windows NTLM authentication protocol.
- NTLM generates hash of user's password without salting, enhancing attacker's ability.
- Attackers do not need plaintext password, reducing time-consuming cracking operations.

Attack Execution with Mimikatz

Mimikatz:

- Steals password hashes from LSASS memory.
- Authenticates to remote systems using stolen hashes.
- Facilitates lateral movement within network.

Attack Execution with PowerShell

PowerShell usage:

- Invoke-WMIExec cmdlet.
- Execution of arbitrary commands on remote Windows machines using WMI.
- Covert operation without additional downloads or installations.

PowerShell Tool for Pass-the-Hash Attacks

Invoke-WMIExec:

- Built-in PowerShell cmdlet.
- Executes commands on remote Windows machines.
- Covert operation enhances attacker's stealth.

Attack Execution with evil-winrm

evil-winrm tool:

- Ruby gem for remote command execution on Windows machines using WinRM protocol.
- Requires installation before use.
- Facilitates remote connections and command execution.

Summary

- Pass-the-Hash (T1550.002) is a potent attack technique leveraging alternate authentication methods.
- Tools like Mimikatz, PowerShell, and evil-winrm enable attackers to execute PtH attacks.
- Understanding and defending against PtH attacks crucial for network security.

Detection Methods for Pass-the-Hash Attack

Event IDs:

- Event ID 1: Process Create
- Event ID 5: Process Terminated
- Event ID 10: Process Accessed
- Event ID 4624: Successful Account Logon
- Event ID 4663: Object Access Attempt
- Event ID 4672: Special Privileges Assigned
- Event ID 4688: New Process Created
- Key Description Fields for each event ID listed to aid in detection.

Mitigation Techniques for Pass-the-Hash Attack

Enable Windows Defender Credential Guard:

- Virtualization-based feature secures credential storage.

Revoke Administrator Privileges:

- Limits attacker's ability to execute malware and extract hashes.

Limit Administrative Privileges:

- Reduce endpoints with admin privileges, avoid admin privileges across security boundaries.

Implement Local Administrator Password Solution (LAPS):

- Randomizes and stores local admin passwords, reducing lateral movement risk.

Prevent Local Account Authentication Over Network:

- Use well-known SIDs in group policies to restrict local account authentication.

Pass-the-Ticket (T1550.003)

- Pass the Ticket (PtT) technique allows attackers to use previously acquired Kerberos Ticket Granting Ticket (TGT).
- TGT enables authentication to multiple systems without entering password each time.

Kerberos Ticket Granting Ticket (TGT)

- Issued by Domain Controller (DC) upon successful authentication.
- Contains user's session key, group membership, privileges.
- Encrypted with user's password hash using symmetric encryption algorithms (e.g., DES, AES).

Tools and Techniques

Tools:

- Mimikatz
- Kekeo
- Rubeus
- Creddump7

Mimikatz usage:

- Capturing Kerberos tickets.
- Reusing tickets.
- Discovering privileges.
- Accessing resources.

Detection Methods

Event IDs:

- Event ID 4768: Kerberos TGT Requested
- Event ID 4769: Kerberos Service Ticket Requested
- Event ID 4770: Kerberos Service Ticket Renewed

- Key Description Fields aid in detection of possible Pass-the-Ticket attacks.

Mitigation Techniques

Utilize Windows Defender Credential Guard:

- Secures credential storage with virtualization.

Limit Endpoint Administrator Privileges:

- Reduces risk of lateral movement.

Avoid Granting Administrative Privileges Across Security Boundaries:

- Minimizes risk of privilege escalation.

Implement effective measures to counter Pass-the-Ticket attacks and limit potential impact.

THANK YOU