
IMPORTANT ACTIVE DIRECTORY ATTRIBUTE
Some useful ad attributes for red/blue teamer
HADESS
WWW.HADESS.IO

Important Active Directory Attribute

Active Directory attributes play a crucial role in managing user accounts and group memberships within Windows environments. Attributes such as SAMACCOUNTNAME and USERPRINCIPALNAME are often targeted for username enumeration and phishing attacks. The MEMBEROF attribute provides insights into group memberships, which adversaries exploit for lateral movement and privilege escalation. DESCRIPTION fields offer valuable information for reconnaissance and social engineering efforts. EMAIL addresses stored in the MAIL attribute are prime targets for phishing campaigns and reconnaissance. HOMEDIRECTORY paths may expose file system access points, making them potential targets for data exfiltration or manipulation. Understanding these attributes and their associated attack vectors is essential for securing Active Directory environments.

ID	Attribute	Description	Attack Vector
1	SEIMPERSONATEPRIVILEGE	Ability to impersonate a client after authentication	Impacket, atexec.py, Invoke-TokenManipulation
2	SELOADDRIVERPRIVILEGE	Ability to load and unload device drivers	Metasploit, exploit/windows/local/service_permissions
3	SEBACKUPPRIVILEGE	Bypass certain security restrictions for backup and restore ops	Covenant, Invoke-TokenManipulation
4	FORCECHANGEPASSWORD	Force user to change password at next logon	PowerSploit, Invoke-UserHunter, Set-ADAccountPassword
5	GENERICWRITE	Write to any attribute of the target object, bypassing security	SharpHound, Invoke-BloodHound, Set-ADObject
6	SeTakeOwnershipPrivilege	Grants the ability to take ownership of files and directories	PowerSploit, Invoke-TakeOwn
7	SeDebugPrivilege	Allows debugging processes and accessing their memory	Metasploit, exploit/windows/local/bypassuac_eventvwr
8	SeAssignPrimaryTokenPrivilege	Assigns primary tokens to processes	Covenant, Invoke-TokenManipulation
9	SeIncreaseQuotaPrivilege	Adjusts memory quotas for processes	Cobalt Strike, privilege::debug
10	SeChangeNotifyPrivilege	Receives notifications of changes to files or directories	Empire, elevate_privileges
11	SeSystemtimePrivilege	Allows adjusting system time	Mimikatz, sekurlsa::pth /domain:target /user:username /ntlm:hash /run:powershell.exe

ID	Attribute	Description	Attack Vector
12	SeShutdownPrivilege	Grants the ability to shut down the system	CrackMapExec, shutdown /r /t 0
13	SeCreateTokenPrivilege	Allows creating access tokens	SharpSploit, CreateProcessAsUser
14	SAMACCOUNTNAME	SAM account name for a user or group	Username enumeration, brute-force attacks
15	USERPRINCIPALNAME	User principal name (UPN) for a user account	Phishing attacks, Kerberos-based attacks
16	MEMBEROF	List of groups to which the user or group belongs	Lateral movement, privilege escalation
17	DESCRIPTION	Textual description or additional information about an object	Reconnaissance, social engineering
18	MAIL	Email address associated with a user account	Phishing attacks, reconnaissance
19	HOMEDIRECTORY	Network path to the user's home directory	File system access, data exfiltration
20	ACCOUNTLOCKEDOUT	Indicates if the user account is locked out	Account enumeration, brute-force attacks
21	BADPASSWORDTIME	Time of the last invalid password attempt for a user account	Password brute-forcing, detection of brute-force attacks
22	LASTLOGONTIMESTAMP	Last time a user logged onto the domain	Identifying inactive or seldom-used privileged accounts
23	PRIMARYGROUPTOKEN	Primary group token for a user, determines primary group	Privilege escalation, persistence
24	ADMINSID	Security identifier (SID) of the user or group considered admin	Privilege escalation, lateral movement
25	LOGONHOURS	Times during which a user is permitted to log onto the domain	Identifying potential opportunities for unauthorized access
26	USERWORKSTATIONS	Workstations from which a user is	Workstation compromise, lateral movement

ID	Attribute	Description	Attack Vector
		permitted to log onto domain	
27	ADMINCOUNTERS	Administrative counter data, indicates administrative actions	Privilege escalation, detection of unusual activity

SEIMPERSONATEPRIVILEGE

Description

This attribute governs the ability to impersonate a client after authentication. Users or processes with this privilege can act on behalf of another user.

```
MATCH p=(:User)-[:MemberOf*1..]->(:Group)-[:CanImpersonate]->()
RETURN p
```

Code: `SeImpersonatePrivilege`

- **Tool:** Impacket
- **Command:** `atexec.py` with `-k` flag
- **Command:** `Invoke-TokenManipulation` with `-ImpersonateUser` flag

SELOADDRIVERPRIVILEGE

Description

This privilege allows users or processes to load and unload device drivers on a system. It's a sensitive privilege often restricted to administrators.

```
MATCH p=(:User)-[:MemberOf*1..]->(:Group)-[:CanLoadDriver]->()
RETURN p
```

Code: `SeLoadDriverPrivilege`

- **Tool:** Metasploit
- **Module:** `exploit/windows/local/service_permissions`
- **Command:** `Invoke-WMIExec` with `-LoadDriver` flag

SEBACKUPPRIVILEGE

Description

Users or processes with this privilege can bypass certain security restrictions to perform backup and restore operations. Typically granted to backup software or administrators.

```
MATCH p=(:User)-[:MemberOf*1..]->(:Group)-[:CanBackup]->()
RETURN p
```

Code: SeBackupPrivilege

- **Tool:** Covenant
- **Command:** `Invoke-TokenManipulation` with `SeBackupPrivilege`

FORCECHANGEPASSWORD

Description

This attribute controls whether a user must change their password at the next logon. Setting this flag forces users to update their password immediately.

```
MATCH p=(:User)-[:CanChangePassword]->()
RETURN p
```

Code: UserMustChangePassword

- **Tool:** PowerSploit
- **Command:** `Invoke-UserHunter` with `-ForcePasswordReset` flag
- - **Command:** `Set-ADAccountPassword`

GENERICWRITE

Description:

This attribute allows the specified user or group to write to any attribute of the target object in Active Directory, bypassing attribute-level security.

```
MATCH p=(:User)-[:MemberOf*1..]->(:Group)-[:CanGenericWrite]->()
RETURN p
```

Code: `ADS_RIGHT_GENERIC_WRITE`

- **Tool:** SharpHound
- **Command:** `Invoke-BloodHound` with `-Find GenericWrite` option
- **Command:** `Set-ADObject` with `-Add` or `-Replace` flag

SeTakeOwnershipPrivilege

Description

Grants the ability to take ownership of files and directories.

```
MATCH p=(:User)-[:MemberOf*1..]->(:Group)-[:CanTakeOwnership]->()
RETURN p
```

Exploitation

- Gain ownership of critical files to manipulate permissions.
- Useful for privilege escalation.
- **Tool:** PowerSploit
- **Command:** `Invoke-TakeOwn`

Mitigation

Limit this privilege to trusted administrators.

SeDebugPrivilege

Description

Allows debugging processes and accessing their memory.

```
MATCH p=(:User)-[:MemberOf*1..]->(:Group)-[:CanDebug]->()
RETURN p
```

Exploitation

- Debugging can lead to code execution or privilege escalation.
- **Tool:** Metasploit
- **Module:** `exploit/windows/local/bypassuac_eventvwr`

Mitigation

Limit this privilege to trusted administrators.

SeImpersonatePrivilege

Description

Enables impersonating other users.

```
MATCH p=(:User)-[:MemberOf*1..]->(:Group)-[:CanImpersonate]->()
RETURN p
```

Exploitation

- Impersonate privileged accounts for unauthorized actions.
- **Tool:** Impacket
- **Command:** `wmiexec.py` with `-k` flag

Mitigation

Restrict this privilege to necessary accounts.

SeAssignPrimaryTokenPrivilege

Description

Assigns primary tokens to processes.

```
MATCH p=(:User)-[:MemberOf*1..]->(:Group)-[:CanAssignPrimaryToken]->()
RETURN p
```

- **Tool:** Covenant
- **Command:** `Invoke-TokenManipulation`

Exploitation

- Manipulate token assignments for privilege escalation.

Mitigation

Limit this privilege to trusted processes.

SeIncreaseQuotaPrivilege

Description

Adjusts memory quotas for processes.

```
MATCH p=(:User)-[:MemberOf*1..]->(:Group)-[:CanIncreaseQuota]->()
RETURN p
```

Exploitation

- Modify memory quotas to evade restrictions.
- **Tool:** Cobalt Strike
- **Module:** `privilege::debug`

Mitigation

Limit this privilege to trusted processes.

SeChangeNotifyPrivilege

Description

Receives notifications of changes to files or directories.

```
MATCH p=(:User)-[:MemberOf*1..]->(:Group)-[:CanChangeNotify]->()
RETURN p
```

Exploitation

- Monitor file changes for sensitive data.
- **Tool:** Empire
- **Command:** `elevate_privileges`

Mitigation

Limit this privilege to necessary accounts.

SeSystemtimePrivilege

Description

Allows adjusting system time.

```
MATCH p=(:User)-[:MemberOf*1..]->(:Group)-[:CanChangeSystemTime]->()
RETURN p
```

Exploitation

- Manipulate system time for various attacks.
- **Tool:** Mimikatz
- **Command:** `sekurlsa::pth /domain:target /user:username /ntlm:hash /run:powershell.exe`

Mitigation

Limit this privilege to trusted administrators.

SeShutdownPrivilege

Description

Grants the ability to shut down the system.

```
MATCH p=(:User)-[:MemberOf*1..]->(:Group)-[:CanShutdown]->()
RETURN p
```

Exploitation

- Unauthorized system shutdown.
- **Tool:** CrackMapExec
- **Command:** `cme smb <target> -u <username> -p <password> --exec-command "shutdown /r /t 0"`

Mitigation

Limit this privilege to trusted administrators.

SeCreateTokenPrivilege

Description

Allows creating access tokens.

```
MATCH p=(:User)-[:MemberOf*1..]->(:Group)-[:CanCreateToken]->()
RETURN p
```

Exploitation

- Create custom tokens for privilege escalation.
- **Tool:** SharpSploit
- **Command:** `CreateProcessAsUser`

Mitigation

Limit this privilege to trusted processes.

ACCOUNTDISABLE

- **Command:** PowerShell command `Set-ADAccountControl`
- **Description:** This attribute determines whether the user account is disabled or enabled. When set to `TRUE`, the account is disabled, and the user cannot log in.
- **Code:** `ADS_UF_ACCOUNTDISABLE`
- **Example:**

`Set-ADAccountControl -Identity "username" -AccountDisabled $true`

LOCKOUTTIME

- **Command:** PowerShell command `Get-ADUser`
- **Description:** This attribute indicates the time when the user account was locked out due to exceeding the account lockout threshold. It's represented as a large integer value.
- **Code:** `lockoutTime`
- **Example:**

`Get-ADUser -Identity "username" -Properties lockoutTime | Select-Object -ExpandProperty lockoutTime`

LASTLOGON

- **Command:** PowerShell command `Get-ADUser`
- **Description:** This attribute records the timestamp of the user's last successful logon to the domain. It helps administrators track user activity and identify inactive accounts.

- **Code:** `lastLogon`
- **Example:**

```
Get-ADUser -Identity "username" -Properties lastLogon | Select-Object -ExpandProperty lastLogon
```

PWDLASTSET

- **Command:** PowerShell command `Get-ADUser`
- **Description:** This attribute stores the timestamp when the user's password was last changed. It's used for enforcing password expiration policies and determining when a password change is required.
- **Code:** `pwdLastSet`
- **Example:**

```
Get-ADUser -Identity "username" -Properties pwdLastSet | Select-Object -ExpandProperty pwdLastSet
```

MEMBEROF

- **Command:** PowerShell command `Get-ADUser` or `Get-ADGroup`
- **Description:** This attribute lists the groups to which the user or group object belongs. It helps manage access permissions and group membership.
- **Code:** `memberOf`
- **Example:**

```
Get-ADUser -Identity "username" -Properties memberOf | Select-Object -ExpandProperty memberOf
```

SAMACCOUNTNAME

- **Command:** PowerShell command `Get-ADUser` or `Get-ADGroup`
- **Description:** This attribute represents the SAM account name for a user or group, which is a unique identifier used in Windows authentication protocols.
- **Code:** `sAMAccountName`
- **Example:**

```
Get-ADUser -Identity "username" | Select-Object -ExpandProperty sAMAccountName
```

USERPRINCIPALNAME

- **Command:** PowerShell command `Get-ADUser`
- **Description:** This attribute represents the user principal name (UPN) for a user account. UPN is formatted as username@domain.com and is used for user logon.
- **Code:** `userPrincipalName`
- **Example:**

```
Get-ADUser -Identity "username" | Select-Object -ExpandProperty userPrincipalName
```

DESCRIPTION

- **Command:** PowerShell command `Get-ADUser` or `Get-ADGroup`

- **Description:** This attribute provides a textual description or additional information about a user or group object within Active Directory.
- **Code:** `description`
- **Example:**

```
Get-ADUser -Identity "username" | Select-Object -ExpandProperty description
```

MAIL

- **Command:** PowerShell command `Get-ADUser`
- **Description:** This attribute stores the email address associated with a user account. It's commonly used for email communication and address book integration.
- **Code:** `mail`
- **Example:**

```
Get-ADUser -Identity "username" | Select-Object -ExpandProperty mail
```

HOMEDIRECTORY

- **Command:** PowerShell command `Get-ADUser`
- **Description:** This attribute specifies the network path to the user's home directory. It's used for automatically mapping network drives and providing user-specific storage.
- **Code:** `homeDirectory`
- **Example:**

```
Get-ADUser -Identity "username" | Select-Object -ExpandProperty homeDirectory
```

ACCOUNTLOCKEDOUT

- **Command:** PowerShell command `Get-ADUser`
- **Description:** This attribute indicates whether the user account is currently locked out. It's a boolean attribute where `TRUE` means the account is locked out.
- **Code:** `IsAccountLockedOut`
- **Example:**

```
(Get-ADUser -Identity "username").IsAccountLockedOut
```

BADPASSWORDTIME

- **Command:** PowerShell command `Get-ADUser`
- **Description:** This attribute records the time of the last invalid password attempt for a user account. It helps in detecting potential brute-force attacks.
- **Code:** `badPasswordTime`
- **Example:**

```
Get-ADUser -Identity "username" -Properties badPasswordTime | Select-Object -ExpandProperty badPasswordTime
```

ADMINCOUNT

- **Command:** PowerShell command `Get-ADUser` or `Get-ADGroup`
- **Description:** This attribute indicates whether the user or group has been marked as having elevated privileges, typically by being a member of a built-in administrative group. Penetration testers often look for objects with `ADMINCOUNT` set to identify potential targets for privilege escalation.
- **Code:** `adminCount`
- **Example:**

```
Get-ADUser -Identity "username" -Properties adminCount |
```

LASTLOGOFF

Description

This attribute indicates the last time a user logged off from the domain. Penetration testers may use this attribute in conjunction with other data to identify potential times of low activity for performing stealthy operations.

Detection

```
Get-ADUser -Identity "username" -Properties lastLogoff | Select-Object -ExpandProperty lastLogoff
```

AUDITFLAG

Description

This attribute specifies the audit settings for an Active Directory object, including whether auditing is enabled and which events are being audited. Penetration testers may identify misconfigured audit settings for potential security weaknesses.

Detection

```
Get-ADObject -Identity "DN of Object" -Properties auditFlag | Select-Object -ExpandProperty auditFlag
```

GROUPPOLICYNAMESPACE

Description

This attribute specifies the namespace of a Group Policy Object (GPO), which defines the scope and settings applied by the GPO. Penetration testers may analyze GPO namespaces for misconfigurations that could lead to privilege escalation or execution.

Detection

```
Get-ADGroupPolicy -Identity "GPOName" -Properties gPCNNameSpace | Select-Object -ExpandProperty gPCNNameSpace
```

GROUPPOLICYLINKS

Description

This attribute specifies the Group Policy Objects (GPOs) linked to an organizational unit (OU) or the entire domain. Penetration testers may analyze GPO links for misconfigurations or vulnerabilities that could be exploited.

Detection

```
Get-ADOrganizationalUnit -Identity "OUName" -Properties gPLink | Select-Object -ExpandProperty gPLink
```

MACHINEACCOUNTQUOTA

Description

This attribute specifies the maximum number of machine accounts (e.g., computer objects) that can be created in the domain. Penetration testers may exploit misconfigurations in machine account quotas for resource exhaustion attacks or unauthorized access.

Detection

```
Get-ADDomain | Select-Object -ExpandProperty ms-DS-MachineAccountQuota
```

USERACCOUNTCONTROL

Description

This attribute controls various account options for a user account, including whether the account is enabled, disabled, locked out, or requires a password change. Penetration testers may manipulate these settings for privilege escalation or execution.

Detection

```
Get-ADUser -Identity "username" -Properties userAccountControl | Select-Object -ExpandProperty userAccountControl
```

ALLOWEDTOACTONBEHALFOFOTHERIDENTITIES

Description

This attribute determines whether the user is allowed to impersonate other identities for delegation purposes. Red team operators may abuse this privilege for lateral movement or privilege escalation.

Detection

```
(Get-ADUser -Identity "username" -Properties msDS-AllowedToActOnBehalfOfOtherIdentity).msDS-AllowedToActOnBehalfOfOtherIdentity
```

GROUPPOLICYNAMESPACE (Repeated)

Description

This attribute specifies the namespace of a Group Policy Object (GPO), which defines the scope and settings applied by the GPO. Red team operators may analyze GPO namespaces for misconfigurations that could lead to privilege

escalation or execution.

Detection

```
Get-ADGroupPolicy -Identity "GPOName" -Properties gPCNNameSpace | Select-Object -ExpandProperty gPCNNameSpace
```

GROUPPOLICYLINKS (Repeated)

Description

This attribute specifies the Group Policy Objects (GPOs) linked to an organizational unit (OU) or the entire domain. Red team operators may analyze GPO links for misconfigurations or vulnerabilities that could be exploited.

Detection

```
Get-ADOrganizationalUnit -Identity "OUName" -Properties gPLink | Select-Object -ExpandProperty gPLink
```

USERPRINCIPALNAME

Description

This attribute represents the user principal name (UPN) for a user account. Red team operators may abuse UPNs for targeted phishing attacks or Kerberos-based attacks.

Detection

```
Get-ADUser -Identity "username" | Select-Object -ExpandProperty userPrincipalName
```

SIDHISTORY

Description

This attribute stores security identifiers (SIDs) from trusted domains that the user or group has previously been a member of. Red team operators may exploit SID history to gain access to resources in trusted domains.

Detection

```
Get-ADUser -Identity "username" -Properties sIDHistory | Select-Object -ExpandProperty sIDHistory
```

SUPPLEMENTALCREDENTIALS

Description

This attribute stores additional credential information for a user, such as cached credentials. Red team operators may target this attribute for credential theft or lateral movement.

Detection

```
Get-ADUser -Identity "username" -Properties supplementalCredentials | Select-Object -ExpandProperty supplementalCredentials
```

GROUPMEMBERSHIP

Description

This attribute lists the groups to which the user belongs. Red team operators may analyze group membership for potential targets for privilege escalation or lateral movement.

Detection

```
Get-ADUser -Identity "username" -Properties memberOf | Select-Object -ExpandProperty memberOf
```

PWDHISTORYLENGTH

Description

This attribute specifies the number of previous passwords stored in the password history. Red team operators may analyze this setting to determine the password reuse policy and identify potential avenues for credential reuse attacks.

Detection

```
Get-ADDomain | Select-Object -ExpandProperty msDS-PSOAppliesTo
```
