SIGPwny

FA2024 Week 10 • 2024-11-05

Active Directory III

Ronan Boyarski

Table of Contents

- MSSQL Exploitation
- Skeleton Keys
- Domain Controller Exploits
- Anything you need review on

MSSQL & Active Directory

MSSQL Theory

- MSSQL is tied tightly to Active Directory and can be used for a variety of exploits
- MSSQL will have an associated SPN for Kerberos and can be authenticated to with Kerberos or NTLM (AD/Local)
- Two account types (usually): Guest & DBO
- Guest can read some things
  - Worth looking around but not usually a method to do anything crazy
- DBO has full control
  - Read all data, can enable XP_CMDSHELL & run C# assemblies
  - Local/Domain Administrator Account will get DBO login
  - Users in custom SQL admins groups will usually get DBO

MSSQL Theory Pitfall

- MSSQL Logins versus Users
  - Users have permissions over a database
  - Logins have permissions over the **server**
- When we impersonate, we want to use logins
  - Functionally, this means to use impacket-mssqlclient's `exec_as_login sa`
- XP_CMDSHELL
  - Must be enabled before you can just use it
  - If you don't it might be weird as to why it doesn't work even though you have privileges

MSSQL Privilege Escalation

- Impersonation
  - Sometimes MSSQL can have its own impersonate privilege that you can leverage to go from Guest or a low-privilege user to DBO
  - Can run queries to enumerate or use shortcuts with `impacket-mssqlclient`
- Usually as easy as `enum_impersonate` & `impersonate_user`
- From there we usually want to enable `XP_CMDSHELL`
  - Can do this with raw queries or impacket
  - Usually you're going to want to cover your tracks and turn it back off…

MSSQL Links

- MSSQL servers can be linked, meaning they can log into one another
  - Can do a manual query or enum_links with impacket
  - Another tool that can do this sort of thing is SQLrecon, which is a C# assembly (think Rubeus)
- How this works depends on set up. Privileges can differ (e.g. Guest on SVR1 can be DBO on SVR2), so you need to just try it
- Oftentimes linked SQL servers will recognize the linked SQL server machine account as a DBO login

MSSQL in AD

- MSSQL can view UNC paths, so we can use the `xp_dirtree` function to get the SMB hash for the currently logged in user
  - Usually the SQL service
- If we can't crack it, we can relay it
  - Relaying to a linked server is usually a good idea
- Linked AD servers **can cross AD forests**, meaning that if we can get some sort of privileged login on a remote one we can use that to cross a forest boundary
  - Not common but just worth keeping in mind

MSSQL Live Walkthrough

Skeleton Keys

Skeleton Keys

- Very scary persistence method
- Create a second master password that you can log into any account with!
- Use mimikatz on the domain controller and use misc::skeleton
  - This will let you log into any account using the password mimikatz
- This is an in-memory injection, so upon restarting the domain controller, **you will lose your skeleton key**
- **OPSEC NOTE**
  - System Event ID 7045 or Security Event ID 4673
  - LSASS in PPL will give you a very bad day for this specifically
  - Generally don't use mimikatz :)

Authentication Coercion Exploits & DC Vulns

Authentication Coercion

- This is when we can force a target machine to log into us (that's a huge deal!)
- Active Directory Domain Controllers have had a lot of these…
  - Printer Bug, DFSCoerce, ShadowCoerce, PetitPotam
- These all have varying requirements to be practically exploitable because you can't log back into yourself
- Relaying many of these to an ADCS endpoint will result in a different credential type that you **can** use to log back into them since it will come from ADCS
- So, be on the lookout for these! All of them are **vulnerable by default** and require active mitigation

DC Vulnerabilities

- NetExec has modules for a lot of these!
- DFSCoerce, ShadowCoerce, PetitPotam all require ADCS to work
- Printer Bug usually requires unconstrained delegation to exploit
- NoPAC is an instant win <- guy that made this made APTLabs
  - "I am a Domain Controller"
- ZeroLogon <- CVE-2020-1472 (CVSS 10!!!)
  - IV is set to zero (crypto guys know this is bad!)
- Official tutorial on exploiting NoPAC & PrintNightmare

DC Exploit Enumeration

Next Meetings

`2024-11-07` • **This Thursday**

- Splunk

`2024-11-09` • **Next Tuesday**

- Introduction to Antivirus Evasion

`2024-11-14` • **Next Thursday**

- Introduction to Malware