Master 2 SeCReTS
Sécurité Windows

# TP : Intrusion et Contre-mesures

Mars 2018

## Première partie
# Généralités

## 1 Objectifs du TP

L'objectif de ce TP est de se familiariser avec la gestion d'un parc windows, le déploiement d'une politique de sécurité et d'appréhender l'intrusion en environnement Windows.

Dans la première partie nous déploierons des GPO facilitant l'administration du parc, tandis que la seconde partie met en évidence les différentes étapes d'une intrusion et les contre-mesures applicables.

## 2 Pré-requis

Vous devez avoir monté l'architecture vue dans les TPs précédents, avec à minima :
- La machine virtuelle Windows Server 2012, ayant notamment les rôles de contrôleur de domaine et de serveur DNS ;
- La machine virtuelle Windows 7, membre du domaine Active Drectory ;
- Une machine virtuelle linux (kali, machine hôte, ou autre).

Les 3 (à minima les deux premières) sont sur un même réseau (hostonly de préférence).

## 3 Manipulation de GPO

### 3.1 Utilisateurs

Sur le contrôleur de domaine, créez 2 utilisateurs : alice et bob, chacun avec un mot de passe différent. Utilisez pour cela la mmc "Active Directory Users and Computers" (dsa.msc).

### 3.2 Politique par défaut

Pour plus de commodité, simplifiez la politique de mots de passe en modifiant la Politique par Défaut du Domaine (outil gpmc.msc). Pour rappel, la politique de mot de passe est dans : Computer Configuration, Policies, Winows Settings, Security Settings, Account Policies, Password Policy. Désactivez ainsi les contraintes de complexité et réduisez la taille minimale d'un mot de passe. Vous pourrez ensuite mettre des mots de passe facile à utiliser pour alice et bob.

En affichant les paramètres de cette GPO, mettez en évidence l'absence de génération du hash LM.

### 3.3 Administration à distance

Créez une nouvelle GPO, appelée RemoteAdmin qui :

- Désactive le pare-feu local (Computer Configuration, Policies, Windows Settings, Security Settings, Windows Firewall).
- Active l'accès à distance en RDP (Computer Configuration, Administrative Templates, Windows Components, Remote Desktop Service, Remote Desktop Session Host, Connections, paramètre "Allow users to connect remotely by using remote desktop services")
- Autorise l'utilisation de WinRM (Administrative Templates, Windows Components, Windows Remote Management, WinRM Service), en autorisant n'importe quel ip source.

Cette même GPO dois également lancer automatiquement les Services WinRM et RemoteRegistry au démarrage de la machine (Computer Configuration, Preferences, Control Panel Settings).

### 3.4 Admins des Stations

Enfin, créer une dernière GPO qui positionne l'utilisateur de domaine bob dans le groupe des Administrateurs de notre station.

Validez la bonne application de vos GPO :

- Accédez à la base de registre du Windows 7 depuis le contrôleur de domaine ;
- L'accès en RDP
- La désactivation du pare-feu
- La connexion à distance via l'outil winrm (winrs /r :win7 cmd.exe)

## 4 Intrusion

### 4.1 ms17_010 et mimikatz

En utilisant metasploit, exploiter la vulnérabilité ms17_010 présente sur la station Windows 7. Vous devrez pour cela utiliser l'exploit "exploit/windows/smb/ms17_010_eternalblue" et positionner les options suivantes :

- RHOST : Machine cible, soit l'IP de la station win7
- PAYLOAD : windows/x64/meterpreter/bind_tcp

Vous pourrez utilisez meterpreter et le module mimikatz pour voler le mot de passe de l'utilisateur alice, connecté à ce moment sur la station. Ainsi que le hash du mot de passe du compte administrateur de domaine, qui s'est précédemment connecté en RDP.

Pour ceux qui ne l'on pas encore fait, profitez en pour voler le hash du compte Administrateur Local via hashdump ou reg save.

### 4.2 PassTheHash et Dump AD

En utilisant la commande pth-smbclient, accéder au disque C : du serveur active directory avec le hash du compte administrateur de domaine.

En utilisant le module psexec et le hash du mot de passe du compte administrateur, récupérez une session interactive sur le DC.

Le dump des comptes de l'AD se fait en récupérant le fichier ntds.dit. Utilisez l'outil ntdsutil pour récupérer ce fichier.

```
ntdsutil
activate instance ntds
ifm
create full c:\dump_ntds
```

Vous aurez également besoin de récupérer la ruche system (via reg save). Récupérez les différents fichiers avec pth-smbclient.

Une autre possibilité de récupérer des comptes de l'AD, est d'utiliser le module kiwi et la commande dcsync (vous devrez en revanche migrer vers un process qui tourne avec des credentials admin de domaine). Récupérez le hash NTLM du compte krbtgt.

### 4.3 Bonus : Golden Ticket