[Exploitation/AD] Exécution de commande à distance

Introduction

Lors de vos tests d'intrusion dans des environnements Active Directory, vous aurez souvent besoin d'exécuter des commandes à distance et d'ouvrir des shells (**RCE**).

Par chance, il existe plusieurs outils dont certains seront décrit dans cette fiche.

EvilWinRM

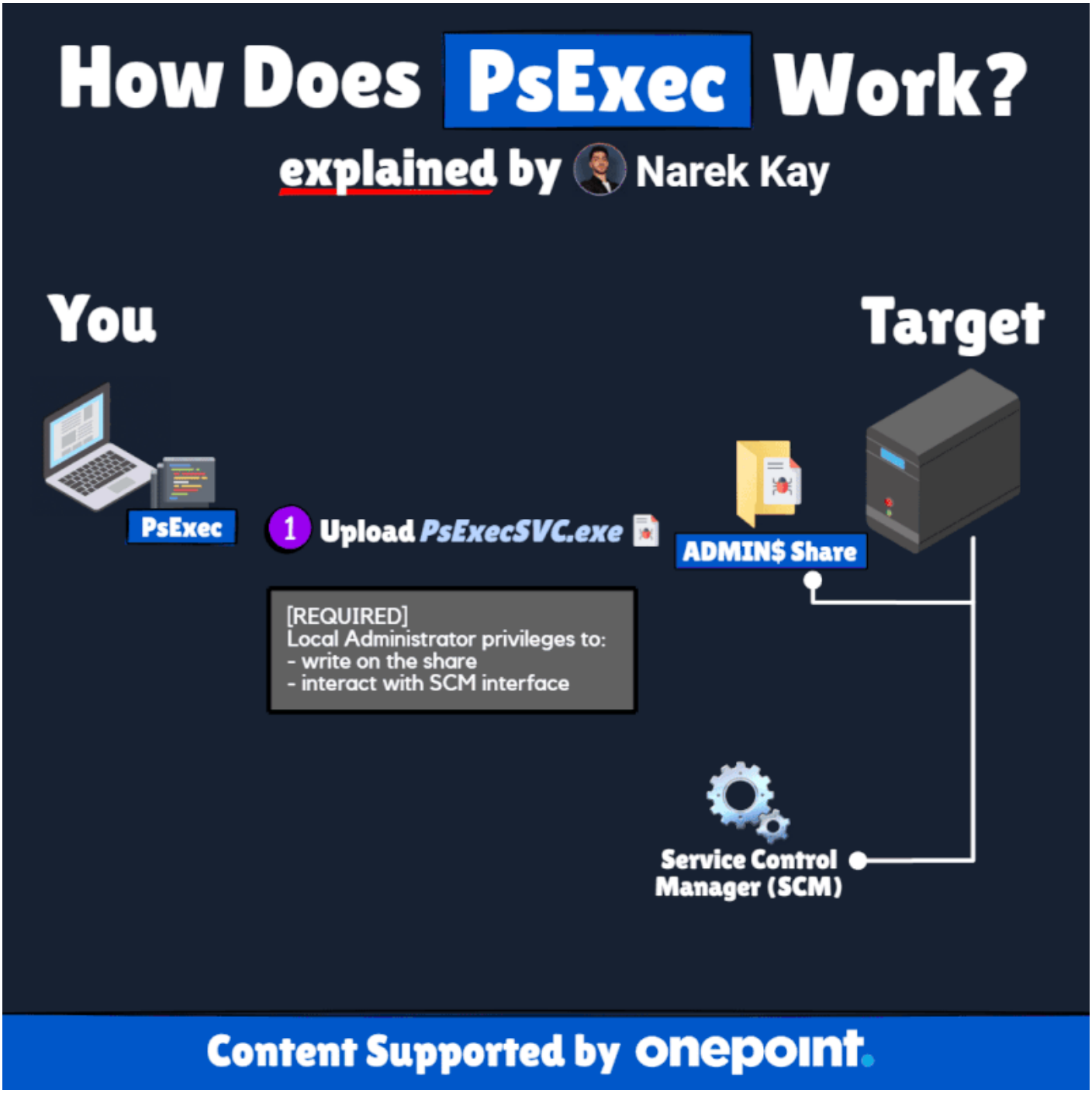
Cet outil utilise le protocole **WinRM** pour ouvrir un shell distant :

```
evilwinrm -u <USER> -p <PASSWORD> -i <IP|FQDN>
```

Suite Impacket

Certains outils de la suite Impacket permettent d'exécuter des commandes à distance via différents protocoles.

PsExec



Il permet d'exécuter des commandes à distances sur des hôtes Windows :

```
psexec.py <DOMAIN>/<USER>:<PASSWORD>@<IP>
```

SMBExec

Avec la même syntaxe, vous pouvez utiliser **smbexec** qui permet la même chose mais nécessite un partage samba accessible en écriture :

```
smbexec.py <DOMAIN>/<USER>:<PASSWORD>@<IP>
```

WMIExec

Toujours avec la même syntaxe et le même objectif, cet outil ne va pas créer de service et ne sera donc pas authentifié avec le compte NT Système :

```
wmiexec.py <DOMAIN>/<USER>:<PASSWORD>@<IP>
```

ATExec

Cet outil va créer une tâche planifiée sur l'hôte distant. Il fonctionne avec la même syntaxe que les trois derniers outils sauf qu'il faut spécifier à la fin la commande que l'on souhaite exécuter :

```
atexec.py <DOMAIN>/<USER>:<PASSWORD>@<IP> <COMMAND>
```

CrackMapExec

Il est capable d'utiliser **Metasploit** ou **Empire** pour lancer des shells.

Meterpreter

- https://ptestmethod.readthedocs.io/en/latest/cme.html#meterpreter

Empire

- https://ptestmethod.readthedocs.io/en/latest/cme.html#meterpreter

---

Revision #6
Created 3 May 2024 15:01:15 by Elieroc
Updated 30 May 2024 15:10:18 by Elieroc