

Информации об учетных записях и SMB в CrackMapExec



CrackMapExec (CME) — популярный инструмент для проведения пентестов в локальной сети и анализа защищенности сетей Windows. Он выполняет сканирование сети и выявляет хосты и службы, а также находит расшаренные (общие) ресурсы, пользователей и группы пользователей. Давайте разберемся, как используя CrackMapExec получить информацию об общих ресурсах, учетных записях и политиках паролей подключенных к сети машин.

Еще по теме: [Список всех модулей CrackMapExec](#)

В качестве примера будут использованы упражнения из [Hack The Box Academy](#).

Для лучшего понимания и углубления, рекомендую изучить наш [мануал по использованию CrackMapExec](#).

Сбор информации об SMB

Инструмент собирает важную SMB-информацию, такую как полное доменное имя (FQDN), которое помогает определить, подключена ли машина к домену, версию и архитектуру Windows (x86/x64), а также версию SMB.

Также можно определить, включена ли функция подписи SMB, что позволяет выявить машины, которые могут быть использованы для кражи хешей и [Relay-атак](#).

Чтобы перечислить информацию о SMB, запустите crackmapexec, укажите протокол SMB и укажите IP-адреса (отдельно в файле или используя диапазоны CIDR).

```
1 crackmapexec smb 10.129.204.177
```

```
(zink0x00@r3dbuck3t) [~/Downloads]
$ crackmapexec smb 10.129.204.177
SMB 10.129.204.177 445 DC01 [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:inlanefreight.htb) (signing:True) (SMBv1:False)
```

На скрине показана информация о SMB целевой машины.

Перечисление учетных записей пользователей

Еще одна вещь, на которую следует обратить внимание при сетевой разведке, — это определение учетных записей пользователей. Можно составить список пользователей машин, на которых разрешены анонимные сессии, а затем провести на них парольные атаки. Или же искать AS-REP учетные записи, которые могут быть взломаны для получения доступа к домену (см. [Атака AS-REP Roasting](#)).

Для перечисления пользователей используется параметр `--users`, который перечисляет всех пользователей на целевых машинах и сохраняет их в файл с помощью параметра `--export`.

Инструмент не предлагает специальной опции для анонимных сессий; вместо этого можно передать пустую строку для имени пользователя (`-u ''`) и пароля (`-p ''`).

```
1 crackmapexec smb 10.129.204.177 -u '' -p '' --users
```

Что мне нравится в опции `--users`, это то, что она отображает не только учетные записи пользователей, но и их описание, где иногда можно найти учетные данные, которые можно использовать, или информацию о типе учетной записи, например, служебные учетные записи.

```
(zink0x00@r3dbuck3t) [~/Downloads]
$ crackmapexec smb 10.129.204.177 -u '' -p '' --users
SMB 10.129.204.177 445 DC01 [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:inlanefreight.htb) (signing:True) (SMBv1:False)
SMB 10.129.204.177 445 DC01 [*] inlanefreight.htb\
SMB 10.129.204.177 445 DC01 [-] Error enumerating domain users using dc ip 10.129.204.177: NTLM needs domain\username and a password
SMB 10.129.204.177 445 DC01 [*] Trying with SAMRPC protocol
SMB 10.129.204.177 445 DC01 [*] Enumerated domain user(s)
SMB 10.129.204.177 445 DC01 inlanefreight.htb\Guest Built-in account for guest access to the computer/domain
SMB 10.129.204.177 445 DC01 inlanefreight.htb\carlos
SMB 10.129.204.177 445 DC01 inlanefreight.htb\grace
SMB 10.129.204.177 445 DC01 inlanefreight.htb\peter
SMB 10.129.204.177 445 DC01 inlanefreight.htb\alina Account for testing HR App. Password: HRApp123!
SMB 10.129.204.177 445 DC01 inlanefreight.htb\noemi
SMB 10.129.204.177 445 DC01 inlanefreight.htb\engels Service Account for testing
SMB 10.129.204.177 445 DC01 inlanefreight.htb\kiosko
SMB 10.129.204.177 445 DC01 inlanefreight.htb\testaccount pwd: Testing123!
SMB 10.129.204.177 445 DC01 inlanefreight.htb\mathew
SMB 10.129.204.177 445 DC01 inlanefreight.htb\svc_mssql
SMB 10.129.204.177 445 DC01 inlanefreight.htb\gmsa_admin
SMB 10.129.204.177 445 DC01 inlanefreight.htb\belkis
SMB 10.129.204.177 445 DC01 inlanefreight.htb\nicole
SMB 10.129.204.177 445 DC01 inlanefreight.htb\jorge
SMB 10.129.204.177 445 DC01 inlanefreight.htb\linda
SMB 10.129.204.177 445 DC01 inlanefreight.htb\shaun
SMB 10.129.204.177 445 DC01 inlanefreight.htb\diana Secret word WeLoveHacking
```

Перечисление политик паролей

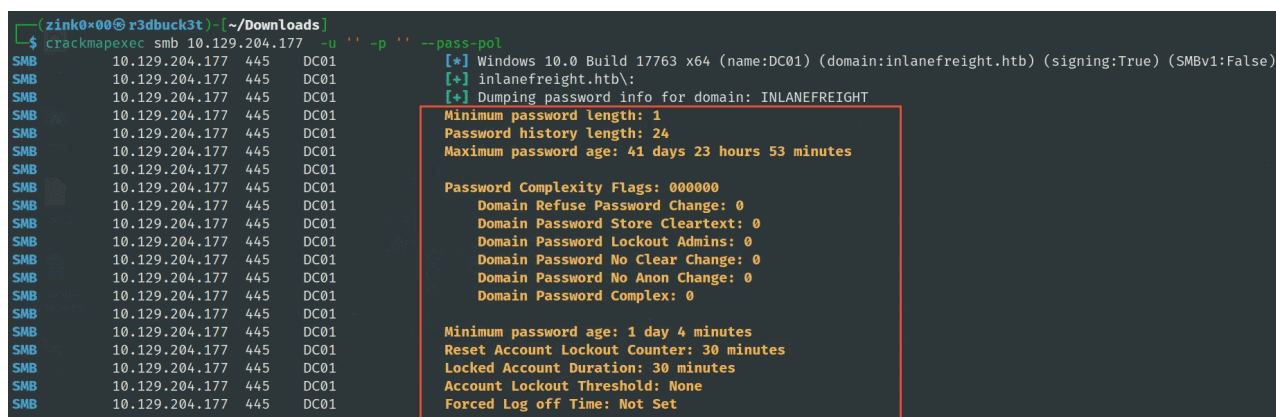
При проведении пенттестов сети распространенной ошибкой является невнимание к политике паролей. Это может привести к блокировке учетных записей или выходу из строя сети.

Понимание политики паролей, особенно порога блокировки, сложности и длины пароля, имеет решающее значение в планировании атак Password Spraying или брутфорса.

Чтобы посмотреть на политику паролей, выполняется crackmapexec с опцией --pass-pol. На скриншоте ниже порог блокировки установлен как None, что означает, что учетные записи никогда не будут заблокированы.

В реальных сценариях некоторые организации могут устанавливать низкий порог в 3 или 5 неудачных попыток, в то время как другие выбирают более высокий порог в 10 или более попыток, чтобы уменьшить количество случайных блокировок.

```
1 crackmapexec smb 10.129.204.177 -u "" -p "" --pass-pol
```



```
zink0x00@r3dbuck3t:~/Downloads
$ crackmapexec smb 10.129.204.177 -u "" -p "" --pass-pol
SMB 10.129.204.177 445 DC01 [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:inlanefreight.htb) (signing:True) (SMBv1:False)
SMB 10.129.204.177 445 DC01 [+] inlanefreight.htb\
SMB 10.129.204.177 445 DC01 [+] Dumping password info for domain: INLANEFREIGHT
SMB 10.129.204.177 445 DC01 Minimum password length: 1
SMB 10.129.204.177 445 DC01 Password history length: 24
SMB 10.129.204.177 445 DC01 Maximum password age: 41 days 23 hours 53 minutes
SMB 10.129.204.177 445 DC01 Password Complexity Flags: 000000
SMB 10.129.204.177 445 DC01 Domain Refuse Password Change: 0
SMB 10.129.204.177 445 DC01 Domain Password Store Cleartext: 0
SMB 10.129.204.177 445 DC01 Domain Password Lockout Admins: 0
SMB 10.129.204.177 445 DC01 Domain Password No Clear Change: 0
SMB 10.129.204.177 445 DC01 Domain Password No Anon Change: 0
SMB 10.129.204.177 445 DC01 Domain Password Complex: 0
SMB 10.129.204.177 445 DC01 Minimum password age: 1 day 4 minutes
SMB 10.129.204.177 445 DC01 Reset Account Lockout Counter: 30 minutes
SMB 10.129.204.177 445 DC01 Locked Account Duration: 30 minutes
SMB 10.129.204.177 445 DC01 Account Lockout Threshold: None
SMB 10.129.204.177 445 DC01 Forced Log off Time: Not Set
```

На скрине политика паролей целевой машины.

Перечисление общих папок SMB

Общие папки — лучшее место для поиска полезной информации; в них можно найти такие важные данные, как конфиденциальные документы, финансовые отчеты или учетные данные привилегированных пользователей, которые помогут проникнуть глубоко в сеть.

Для получения списка доступных общих ресурсов используется команда crackmapexec с параметром --shares и произвольным именем пользователя для параметра -u, например « guest».

Обратите внимание, что утилита не принимает пустые строки в качестве имен пользователей при выполнении опции shares, поэтому необходимо указать случайное имя пользователя.

```
1 crackmapexec smb 10.129.29.43 -u guest -p "" --shares
```

Share	Permissions	Remark
ADMIN\$		Remote Admin
C\$		Default share
CertEnroll		Active Directory Certificate Services share
D\$		Default share
IPC\$	READ	Remote IPC
IT		
K\$		Default share
linux01	READ,WRITE	
NETLOGON		Logon server share
serviceaccount		

На рисунке ниже показана ошибка отказа в доступе при передаче пустых строк в качестве имени пользователя.

```
[*] Error enumerating shares: STATUS_ACCESS_DENIED
```

```
1 crackmapexec smb 10.129.203.121 -u quest -p " --spider IT --regex .
```

```
[*] inlanefreight.htb\grace:Inlanefreight01!  
[*] Started spidering  
[*] Spidering .  
//10.129.14.147/IT/. [dir]  
//10.129.14.147/IT/.. [dir]  
//10.129.14.147/IT/Creds.txt [lastm:'2022-12-01 13:01' size:54]  
//10.129.14.147/IT/Documents [dir]  
//10.129.14.147/IT/IPList.txt [lastm:'2022-12-01 13:01' size:36]  
//10.129.14.147/IT/Documents/. [dir]  
//10.129.14.147/IT/Documents/.. [dir]  
//10.129.14.147/IT/Documents/PCNames.txt [lastm:'2022-12-01 13:01' size:
```

Заключение

В следующих статьях мы рассмотрим другие сценарии использования CrackMapExec, атаки Password Spraying и Relay SMB.

- Способы прописаться в системе при пентесте
- Перечисление и обнаружение SMB в локальной сети

- Эксплуатация уязвимости CVE-2022-27228 и атака NTLM Relay.