8-Passwor Spraying: Enumerating & Retrieving Password Policies

1-Enumerating the Password Policy - from Linux - Credentialed

As stated in the previous section, we can pull the domain password policy in several ways, depending on how the domain is configured and whether or not we have valid domain credentials. With valid domain credentials, the password policy can also be obtained remotely using tools such as CrackMapExec or `rpcclient`.

بص يا عم، لو إنت عايز تطلع سياسة الباسوردات اللي شغالة على الدومين (Domain Password Policy)، في كذا طريقة تعمل كده، وده بيعتمد على إذا كان عندك صلاحيات على الدومين أو لا.

لو معاك بيانات دخول (Valid Domain Credentials)، تقدر تسحب السياسة دي عن بُعد باستخدام أدوات زي **CrackMapExec** أو **rpcclient**. الأدوات دي بتقدر تعمل اتصال بالسيرفر بتاع الدومين وتطلع التفاصيل زي طول الباسورد المسموح بيه، عدد المحاولات قبل ما يتقفل الحساب، وحاجات زي كده.

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

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
SMB         172.16.5.5      445    ACADEMY-EA-DC01  [+] Dumping password info for domain: INLANEFREIGHT
SMB         172.16.5.5      445    ACADEMY-EA-DC01  Minimum password length: 8
SMB         172.16.5.5      445    ACADEMY-EA-DC01  Password history length: 24
SMB         172.16.5.5      445    ACADEMY-EA-DC01  Maximum password age: Not Set
SMB         172.16.5.5      445    ACADEMY-EA-DC01
SMB         172.16.5.5      445    ACADEMY-EA-DC01  Password Complexity Flags: 000001
SMB         172.16.5.5      445    ACADEMY-EA-DC01      Domain Refuse Password Change: 0
SMB         172.16.5.5      445    ACADEMY-EA-DC01      Domain Password Store Cleartext: 0
SMB         172.16.5.5      445    ACADEMY-EA-DC01      Domain Password
Lockout Admins: 0
SMB         172.16.5.5      445    ACADEMY-EA-DC01      Domain Password No
Clear Change: 0
SMB         172.16.5.5      445    ACADEMY-EA-DC01      Domain Password No
Anon Change: 0
SMB         172.16.5.5      445    ACADEMY-EA-DC01      Domain Password
Complex: 1
SMB         172.16.5.5      445    ACADEMY-EA-DC01
SMB         172.16.5.5      445    ACADEMY-EA-DC01  Minimum password age: 1
day 4 minutes
SMB         172.16.5.5      445    ACADEMY-EA-DC01  Reset Account Lockout
Counter: 30 minutes
SMB         172.16.5.5      445    ACADEMY-EA-DC01  Locked Account Duration:
30 minutes
SMB         172.16.5.5      445    ACADEMY-EA-DC01  Account Lockout
Threshold: 5
SMB         172.16.5.5      445    ACADEMY-EA-DC01  Forced Log off Time: Not
Set
```

2-Enumerating the Password Policy - from Linux - SMB NULL Sessions : no Credentialed

Null Session Attack : Connect to the server without username and password (null)وده نوع من الهجمات اللي بتحاول تعمل اتصال بالسيرفر أو بمعنى تاني: اتصال فاضي أو) الجهاز المستهدف من غير ما تستخدم اسم مستخدم أو باسورد "null").

Without credentials, we may be able to obtain the password policy via an SMB NULL session or LDAP anonymous bind. The first is via an SMB NULL session. **SMB NULL sessions allow an unauthenticated attacker to retrieve information from the domain, such as a complete listing of users, groups, computers, user account attributes, and the domain password policy.** SMB NULL session misconfigurations are often the result of legacy Domain Controllers being upgraded in place, ultimately bringing along insecure configurations, which existed by default in older versions of Windows Server.

When creating a domain in earlier versions of Windows Server, anonymous access was granted to certain shares, which allowed for domain enumeration. An SMB NULL session can be enumerated easily. For enumeration, we can use tools such as `enum4linux`, `CrackMapExec`, `rpcclient`, etc.

We can use rpcclient to check a Domain Controller for SMB NULL session access.

Once connected, we can issue an RPC command such as `querydominfo` to obtain information about the domain and confirm NULL session access.

Using rpcclient

-U : username

-N : no password --> Don't ask for a password

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

rpcclient $> querydominfo
Domain:         INLANEFREIGHT
Server:
Comment:
Total Users:    3650
Total Groups:   0
Total Aliases:  37
Sequence No:    1
Force Logoff:   -1
Domain Server State:    0x1
Server Role:    ROLE_DOMAIN_PDC
Unknown 3:      0x1

Obtaining the Password Policy using rpcclient

rpcclient $> getdompwinfo
min_password_length: 8
password_properties: 0x00000001
    DOMAIN_PASSWORD_COMPLEX
```

Let's try this using enum4linux. `enum4linux` is a tool built around the Samba suite of tools `nmblookup`, `net`, `rpcclient` and `smbclient` to use for enumeration of windows hosts and domains. It can be found pre-installed on many different penetration testing distros, including Parrot Security Linux. Below we have an example output displaying information that can be provided by `enum4linux`. Here are some common enumeration tools and the ports they use:

Tool	Ports
nmblookup	137/UDP
nbtstat	137/UDP
net	139/TCP, 135/TCP, TCP and UDP 135 and 49152-65535
rpcclient	135/TCP

Tool	Ports
smbclient	445/TCP

Using enum4linux

```
0xAmr0zZakaria@htb[/htb]$ enum4linux -P 172.16.5.5

<SNIP>

 ==================================================
|    Password Policy Information for 172.16.5.5    |
 ==================================================

[+] Attaching to 172.16.5.5 using a NULL share
[+] Trying protocol 139/SMB...

    [!] Protocol failed: Cannot request session (Called Name:172.16.5.5)

[+] Trying protocol 445/SMB...
[+] Found domain(s):

    [+] INLANEFREIGHT
    [+] Builtin

[+] Password Info for Domain: INLANEFREIGHT

    [+] Minimum password length: 8
    [+] Password history length: 24
    [+] Maximum password age: Not Set
    [+] Password Complexity Flags: 000001

        [+] Domain Refuse Password Change: 0
        [+] Domain Password Store Cleartext: 0
        [+] Domain Password Lockout Admins: 0
        [+] Domain Password No Clear Change: 0
        [+] Domain Password No Anon Change: 0
        [+] Domain Password Complex: 1

    [+] Minimum password age: 1 day 4 minutes
    [+] Reset Account Lockout Counter: 30 minutes
    [+] Locked Account Duration: 30 minutes
    [+] Account Lockout Threshold: 5
    [+] Forced Log off Time: Not Set
[+] Retieved partial password policy with rpcclient:

Password Complexity: Enabled
Minimum Password Length: 8

enum4linux complete on Tue Feb 22 17:39:29 2022
```

The tool enum4linux-ng is a rewrite of `enum4linux` in Python, but has additional features such as the ability to export data as YAML or JSON files which can later be used to process the data further or feed it to other tools. It also supports colored output, among other features

Using enum4linux-ng

-oA --> output file

-P --> password policy

```
0xAmr0zZakaria@htb[/htb]$ enum4linux-ng -P 172.16.5.5 -oA ilfreight

ENUM4LINUX - next generation

<SNIP>

 =======================================
|    RPC Session Check on 172.16.5.5    |
 =======================================
[*] Check for null session
[+] Server allows session using username '', password ''
[*] Check for random user session
[-] Could not establish random user session: STATUS_LOGON_FAILURE

 =================================================
|    Domain Information via RPC for 172.16.5.5    |
 =================================================
[+] Domain: INLANEFREIGHT
[+] SID: S-1-5-21-3842939050-3880317879-2865463114
[+] Host is part of a domain (not a workgroup)
 =========================================================
|    Domain Information via SMB session for 172.16.5.5    |
========================================================
[*] Enumerating via unauthenticated SMB session on 445/tcp
[+] Found domain information via SMB
NetBIOS computer name: ACADEMY-EA-DC01
NetBIOS domain name: INLANEFREIGHT
```

```
DNS domain: INLANEFREIGHT.LOCAL
FQDN: ACADEMY-EA-DC01.INLANEFREIGHT.LOCAL

 =======================================
|    Policies via RPC for 172.16.5.5    |
 =======================================
[*] Trying port 445/tcp
[+] Found policy:
domain_password_information:
  pw_history_length: 24
  min_pw_length: 8
  min_pw_age: 1 day 4 minutes
  max_pw_age: not set
  pw_properties:
  - DOMAIN_PASSWORD_COMPLEX: true
  - DOMAIN_PASSWORD_NO_ANON_CHANGE: false
  - DOMAIN_PASSWORD_NO_CLEAR_CHANGE: false
  - DOMAIN_PASSWORD_LOCKOUT_ADMINS: false
  - DOMAIN_PASSWORD_PASSWORD_STORE_CLEARTEXT: false
  - DOMAIN_PASSWORD_REFUSE_PASSWORD_CHANGE: false
domain_lockout_information:
  lockout_observation_window: 30 minutes
  lockout_duration: 30 minutes
  lockout_threshold: 5
domain_logoff_information:
  force_logoff_time: not set

Completed after 5.41 seconds
```

Enum4linux-ng provided us with a bit clearer output and handy JSON and YAML output using the `-oA` flag.

```
0xAmr0zZakaria@htb[/htb]$ cat ilfreight.json

{
    "target": {
        "host": "172.16.5.5",
        "workgroup": ""
    },
    "credentials": {
        "user": "",
        "password": "",
        "random_user": "yxditqpc"
    },
    "services": {
        "SMB": {
            "port": 445,
            "accessible": true
        },
        "SMB over NetBIOS": {
            "port": 139,
            "accessible": true
        }
    },
    "smb_dialects": {
        "SMB 1.0": false,
        "SMB 2.02": true,
        "SMB 2.1": true,
        "SMB 3.0": true,
        "SMB1 only": false,
        "Preferred dialect": "SMB 3.0",
        "SMB signing required": true
    },
    "sessions_possible": true,
    "null_session_possible": true,

<SNIP>
```

3-Enumerating Null Session - from Windows

It is less common to do this type of null session attack from Windows, but we could use the command `net use \\host\ipc$ "" /u:""` to establish a null session from a windows machine and confirm if we can perform more of this type of attack.

Establish a null session from windows

net use: is command on windows use if you want to connect with network or resource sharing or printer sharing

- `\\host\ipc$`: ده معناه إنك بتحاول تتصل بالـ **IPC$ share** على جهاز اسمه "host".
  - **IPC$ هو اختصار لـ "Inter-Process Communication"، وهو مسار خاص بيستخدمه ويندوز لتبادل البيانات بين العمليات (processes).**
- `""`: هنا بتحدد إنك مش بتستخدم باسورد (الباسورد فاضي).
- `/u:""`: دي معناها إنك مش بتستخدم اسم مستخدم (اليوزرنيم فاضي).

الفكرة:

الأمر ده بيجرب يشوف هل السيرفر يسمح باتصال null session ولا لأ. لو الاتصال نجح، ده معناه إنك ممكن تستغل الموضوع علشان تعمل هجمات أكتر، زي:

- تسحب معلومات من السيرفر.
- تكتشف مشاركة الموارد اللي عليه.
- تشوف المستخدمين الموجودين في الدومين.

```
C:\htb> net use \\DC01\ipc$ "" /u:""
The command completed successfully.
```

We can also use a username/password combination to attempt to connect. Let's see some common errors when trying to authenticate:

Error: Account is Disabled

```
C:\htb> net use \\DC01\ipc$ "" /u:guest
System error 1331 has occurred.

This user can't sign in because this account is currently disabled.
```

Error: Password is Incorrect

```
C:\htb> net use \\DC01\ipc$ "password" /u:guest
System error 1326 has occurred.

The user name or password is incorrect.
```

Error: Account is locked out (Password Policy)

```
C:\htb> net use \\DC01\ipc$ "password" /u:guest
System error 1909 has occurred.

The referenced account is currently locked out and may not be logged on to.
```

4-Enumerating the Password Policy - from Linux - LDAP Anonymous Bind

يعني إيه LDAP Anonymous Bind؟

LDAP (Lightweight Directory Access Protocol) هو بروتوكول بيُستخدم لإدارة واستعراض المعلومات المخزنة في قواعد بيانات الدليل (Directory Services) زي Active Directory.

يعني إنك بتتصل بالسيرفر بدون ما تقدم أي بيانات تسجيل دخول (اسم مستخدم أو باسورد). ا**لهدف منه يكون عادة **Anonymous Bind استعراض بيانات عامة أو التحقق من اتصالك بالسيرفر.

شرح أكتر:

لما أي جهاز يحاول يتصل بسيرفر **LDAP**، لازم الأول يعمل "Bind" (يعني: عملية تسجيل الدخول). الـ Bind ده بيكون على 3 أشكال:

1. **Simple Bind**: باستخدام اسم مستخدم وباسورد.
2. **SASL Bind**: استخدام آلية متقدمة للتوثيق.
3. Anonymous Bind: بدون توثيق، وده موضوعنا.

ازاي بيشتغل Anonymous Bind؟

1. **بيبعت طلب للسيرفر من غير بيانات مستخدم (Client) العميل.**
2. **السيرفر بيشوف لو الـ Anonymous Access مسموح:**
   - **لو مسموح: السيرفر يرد بالمعلومات العامة المتاحة (Public Data).**
   - **لو مش مسموح: السيرفر يرفض الاتصال.**

ليه بنستخدم Anonymous Bind؟

- **لاستعراض بيانات عامة زي أسماء المستخدمين أو المعلومات الأساسية عن الدومين.**
- **لفحص إعدادات السيرفر وتجربة إذا كان بيسمح باتصالات مجهولة (غالبًا ضمن اختبارات الأمان).**
- **تأكيد إن السيرفر شغال.**

With an LDAP anonymous bind, we can use LDAP-specific enumeration tools such as `windapsearch.py`, `ldapsearch`, `ad-ldapdomaindump.py`, etc., to pull the password policy. With ldapsearch, it can be a bit cumbersome but doable. One example command to get the password policy is as follows:

Using ldapsearch

ldapsearch للتواصل مع خادم **LDAP** بهدف البحث عن قيمة **pwdHistoryLength**، وهي خاصية تُظهر عدد كلمات المرور القديمة التي يجب أن تُحفظ لمنع المستخدم من إعادة استخدامها.

شرح الأجزاء:

1. `ldapsearch`:
   - أداة تُستخدم لاستعلام خادم **LDAP** واسترداد البيانات بناءً على معايير محددة.
2. `-h 172.16.5.5`:
   - عنوان **IP** الخاص بخادم **LDAP** الذي سيتم الاتصال به.
3. `-x`:

    - يُشير إلى استخدام **Anonymous Bind** (اتصال بدون بيانات اعتماد).

4. `-b "DC=INLANEFREIGHT,DC=LOCAL"`:
    - **Base DN** (Distinguished Name): النقطة التي يبدأ منها البحث.
    - في هذا المثال، يتم البحث في المجال (Domain) "INLANEFREIGHT.LOCAL".
5. `-s sub`:
    - يُحدد نطاق البحث:
        - **sub**: البحث في **Base DN** وكل الحقول الفرعية تحته (Subtree).
6. `"*"`:
    - يُطلب إرجاع جميع الخصائص (Attributes) الموجودة في السجلات.
7. `| grep -m 1 -B 10 pwdHistoryLength`:
    - يقوم بتصفية النتائج باستخدام **grep**.
    - `pwdHistoryLength`: يبحث عن هذا الحقل في النتائج.
    - `-m 1`: يتوقف عند أول نتيجة مطابقة.
    - `-B 10`: يعرض 10 أسطر قبل السطر المطابق لإعطاء سياق.

```
0xAmr0zZakaria@htb[/htb]$ ldapsearch -h 172.16.5.5 -x -b
"DC=INLANEFREIGHT,DC=LOCAL" -s sub "*" | grep -m 1 -B 10 pwdHistoryLength

forceLogoff: -9223372036854775808
lockoutDuration: -18000000000
lockOutObservationWindow: -18000000000
lockoutThreshold: 5
maxPwdAge: -9223372036854775808
minPwdAge: -864000000000
minPwdLength: 8
modifiedCountAtLastProm: 0
nextRid: 1002
pwdProperties: 1
pwdHistoryLength: 24
```

pwdHistoryLength: 24 هذا يعني أن النظام يحتفظ بآخر 24 كلمات مرور للمستخدم، ولا يُسمح بإعادة استخدامها

Here we can see the minimum password length of 8, lockout threshold of 5, and password complexity is set (`pwdProperties` set to `1`).

Enumerating the Password Policy - from Windows

If we can authenticate to the domain from a Windows host, we can use built-in Windows binaries such as `net.exe` to retrieve the password policy. We can also use various tools such as PowerView, CrackMapExec ported to Windows, SharpMapExec, SharpView, etc.

Using built-in commands is helpful if we land on a Windows system and cannot transfer tools to it, or we are positioned on a Windows system by the client, but have no way of getting tools onto it. One example using the built-in net.exe binary is:

Using net.exe

```
C:\htb> net accounts

Force user logoff how long after time expires?:       Never
Minimum password age (days):                          1
Maximum password age (days):                          Unlimited
Minimum password length:                              8
Length of password history maintained:                24
Lockout threshold:                                    5
Lockout duration (minutes):                           30
Lockout observation window (minutes):                 30
Computer role:                                        SERVER
The command completed successfully.
```

Here we can glean the following information:

- Passwords never expire (Maximum password age set to Unlimited)
- The minimum password length is 8 so weak passwords are likely in use
- The lockout threshold is 5 wrong passwords
- Accounts remained locked out for 30 minutes

This password policy is excellent for password spraying. The eight-character minimum means that we can try common weak passwords such as `Welcome1`. The ==lockout threshold of 5 means that we can attempt 2-3 (==to be safe) sprays every 31 minutes without the risk of locking out any accounts. If an account has been locked out, it will automatically unlock (without manual intervention from an admin) after 30 minutes, but we should avoid locking out `ANY` accounts at all costs.

PowerView is also quite handy for this:

Using PowerView

```
PS C:\htb> import-module .\PowerView.ps1
PS C:\htb> Get-DomainPolicy

Unicode        : @{Unicode=yes}
```

```
SystemAccess    : @{MinimumPasswordAge=1; MaximumPasswordAge=-1;
MinimumPasswordLength=8; PasswordComplexity=1;
                  PasswordHistorySize=24; LockoutBadCount=5;
ResetLockoutCount=30; LockoutDuration=30;
                  RequireLogonToChangePassword=0;
ForceLogoffWhenHourExpire=0; ClearTextPassword=0;
                  LSAAnonymousNameLookup=0}
KerberosPolicy : @{MaxTicketAge=10; MaxRenewAge=7; MaxServiceAge=600;
MaxClockSkew=5; TicketValidateClient=1}
Version         : @{signature="$CHICAGO$"; Revision=1}
RegistryValues :
@{MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=System.Object[]}
Path            : \\INLANEFREIGHT.LOCAL\sysvol\INLANEFREIGHT.LOCAL\Policies\
{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHI
                  NE\Microsoft\Windows NT\SecEdit\GptTmpl.inf
GPOName         : {31B2F340-016D-11D2-945F-00C04FB984F9}
GPODisplayName : Default Domain Policy
```

PowerView gave us the same output as our `net accounts` command, just in a different format but also revealed that password complexity is enabled (`PasswordComplexity=1`).

Analyzing the Password Policy

We've now pulled the password policy in numerous ways. Let's go through the policy for the INLANEFREIGHT.LOCAL domain piece by piece.

- **The minimum password length is 8 (8 is very common, but nowadays, we are seeing more and more organizations enforce a 10-14 character password, which can remove some password options for us, but does not mitigate the password spraying vector completely)**
- **The account lockout threshold is 5 (it is not uncommon to see a lower threshold such as 3 or even no lockout threshold set at all)**
- **The lockout duration is 30 minutes (this may be higher or lower depending on the organization), so if we do accidentally lockout (avoid!!) an account, it will unlock after the 30-minute window passes**
- **Accounts unlock automatically (in some organizations, an admin must manually unlock the account). We never want to lockout accounts while performing password spraying, but we especially want to avoid locking out accounts in an organization where an admin would have to intervene and unlock hundreds (or thousands) of accounts by hand/script**

- **Password complexity is enabled, meaning that a user must choose a password with 3/4 of the following: an uppercase letter, lowercase letter, number, special character (`Password1` or `Welcome1` would satisfy the "complexity" requirement here, but are still clearly weak passwords).**

The default password policy when a new domain is created is as follows, and there have been plenty of organizations that never changed this policy:

Policy	Default Value
Enforce password history	24 days
Maximum password age	42 days
Minimum password age	1 day
Minimum password length	7
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled
Account lockout duration	Not set
Account lockout threshold	0
Reset account lockout counter after	Not set