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.

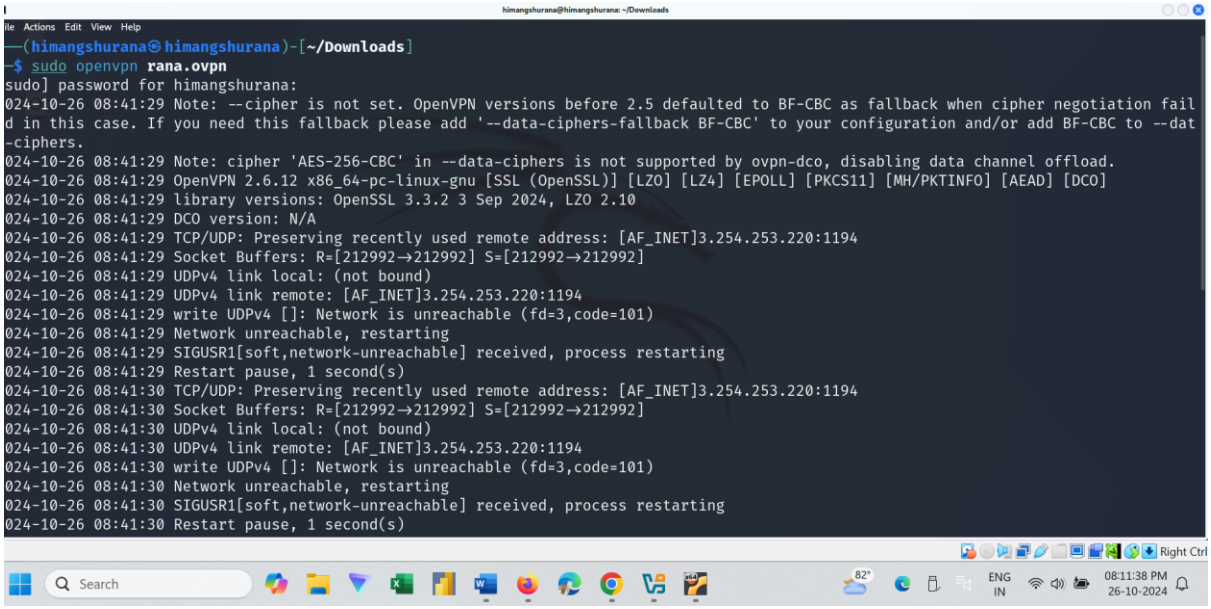
The primary attack consisted of several stages:

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.

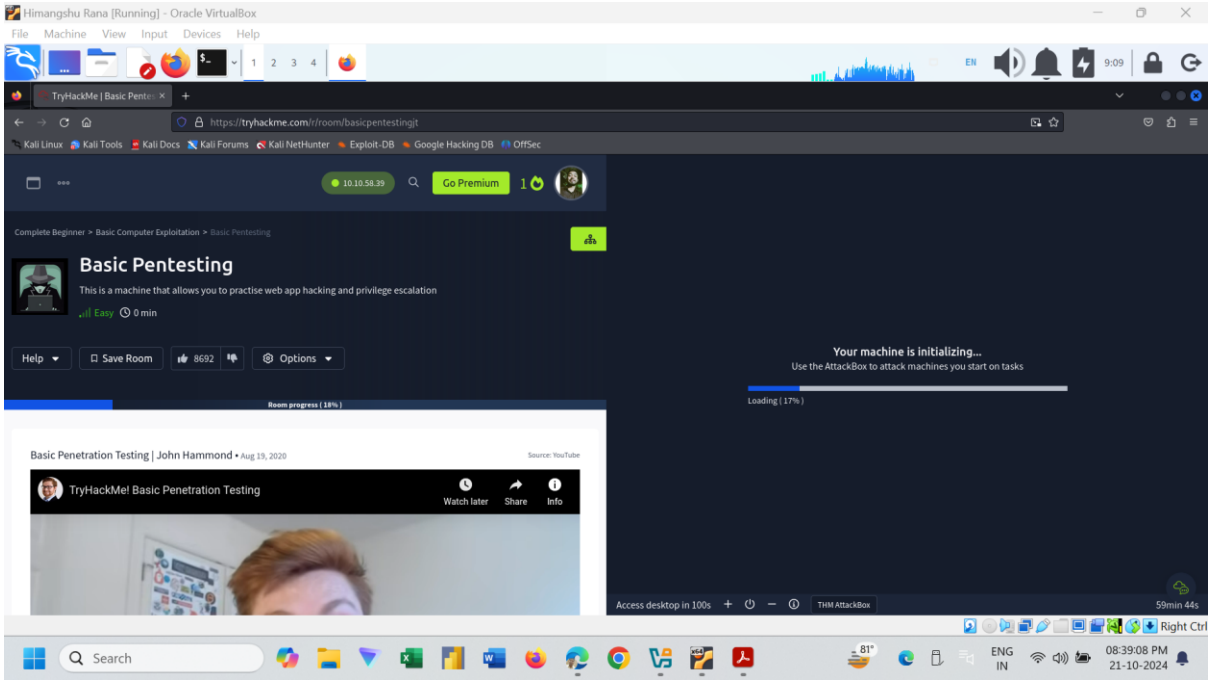
4. Steps to Reproduce

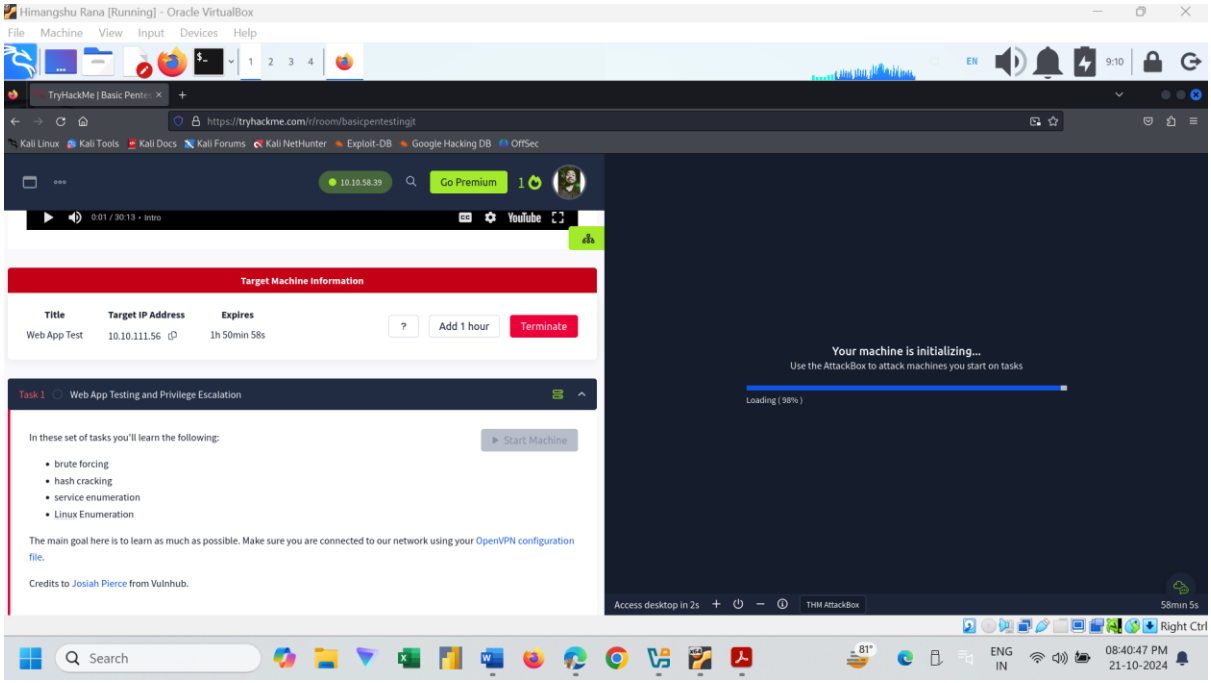
Task 1: Deploy the machine and connect to our network

Step 1: Start VPN Connection



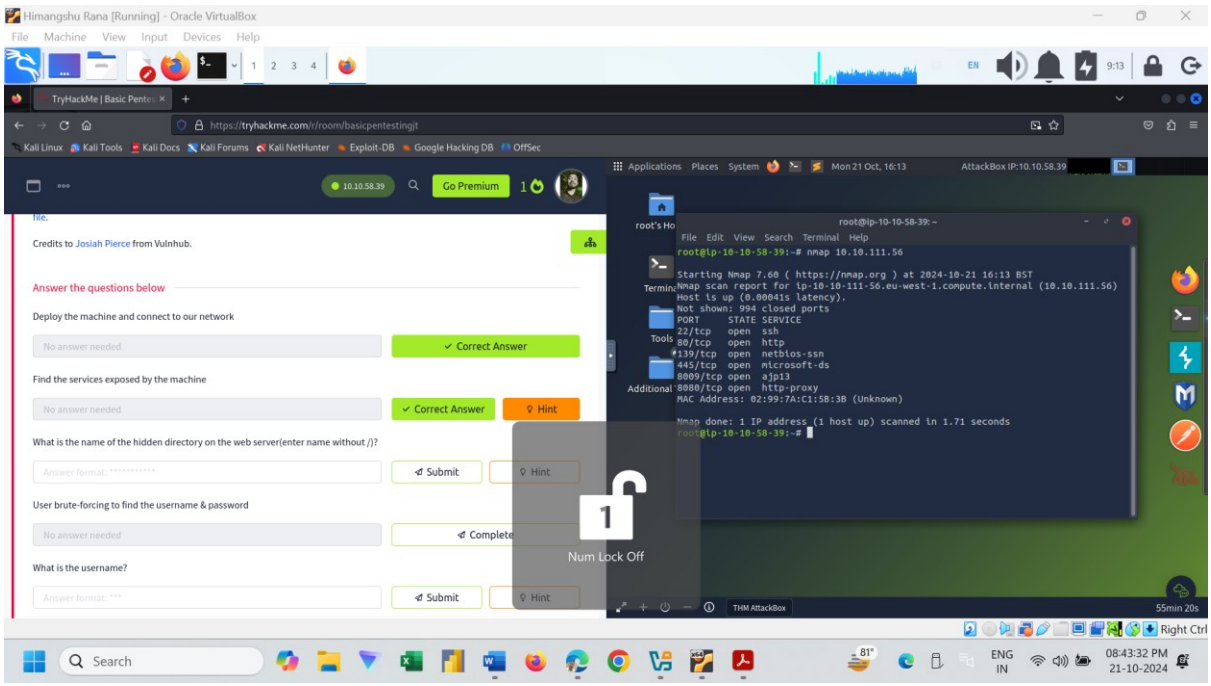
Step 2: Start the Machine



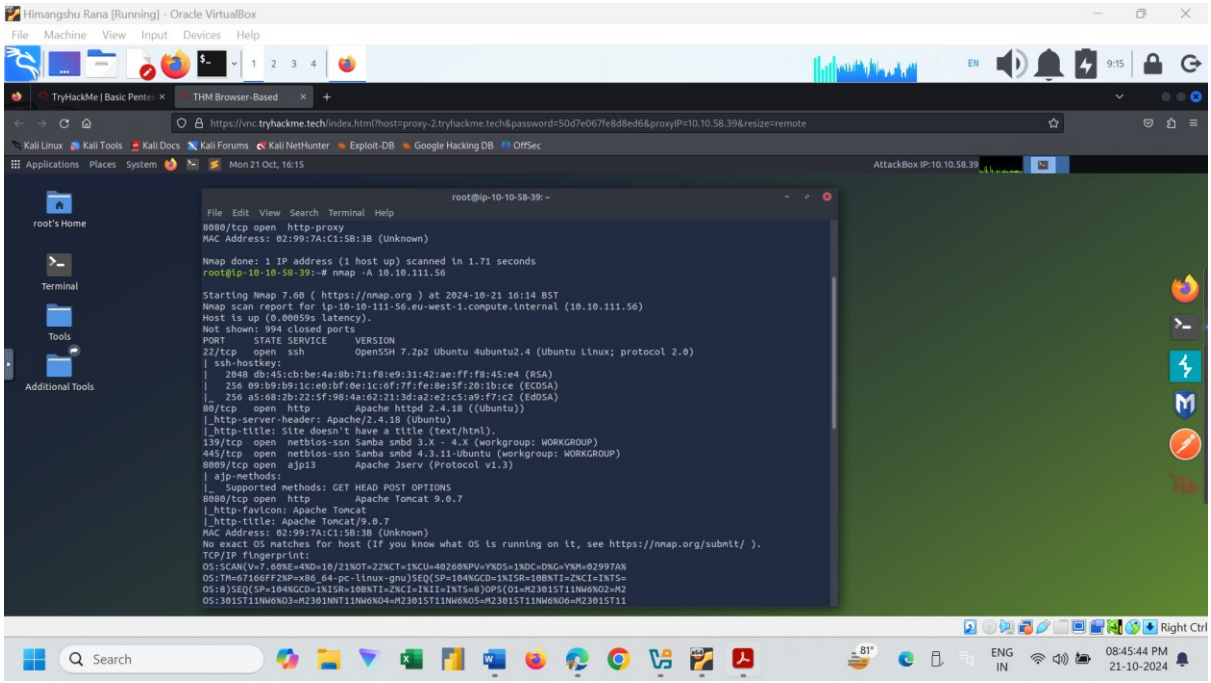


Task 2: Find the services exposed by the machine.

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



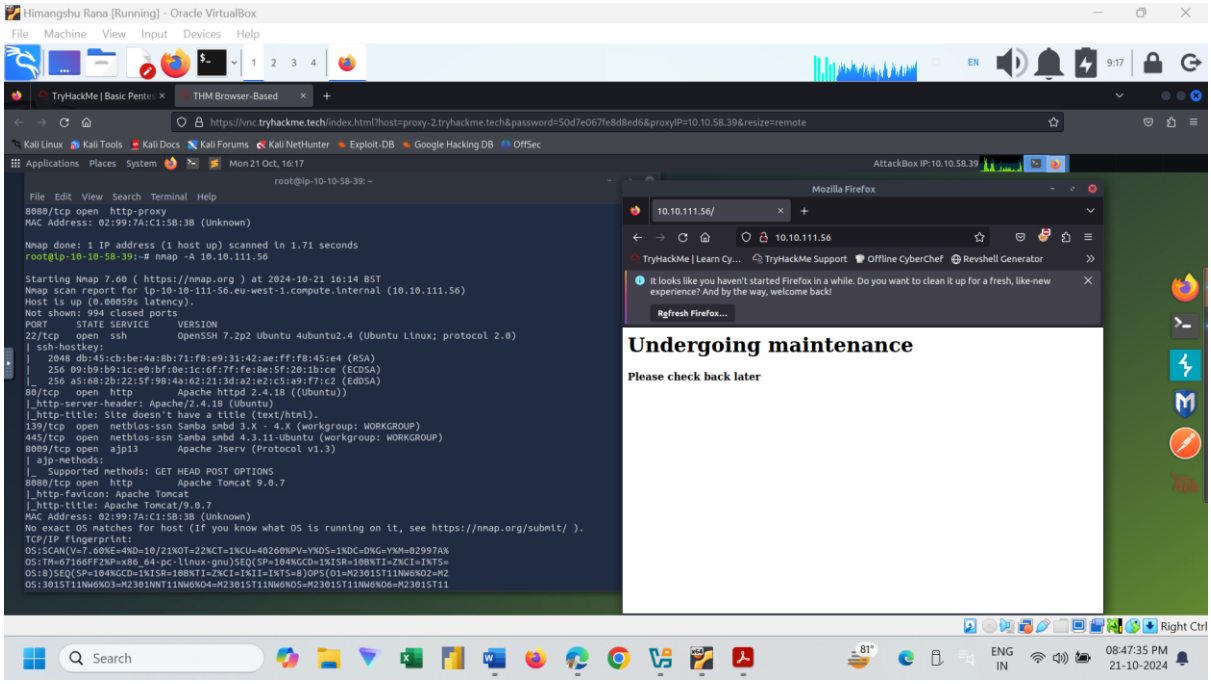
Step 2: Again, Run aggressive Nmap and it provide information about the open ports, services, OS detection, version detection, script scanning, and traceroute.(Use command – nmap -A 10.10.111.56)



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

Answer is : development

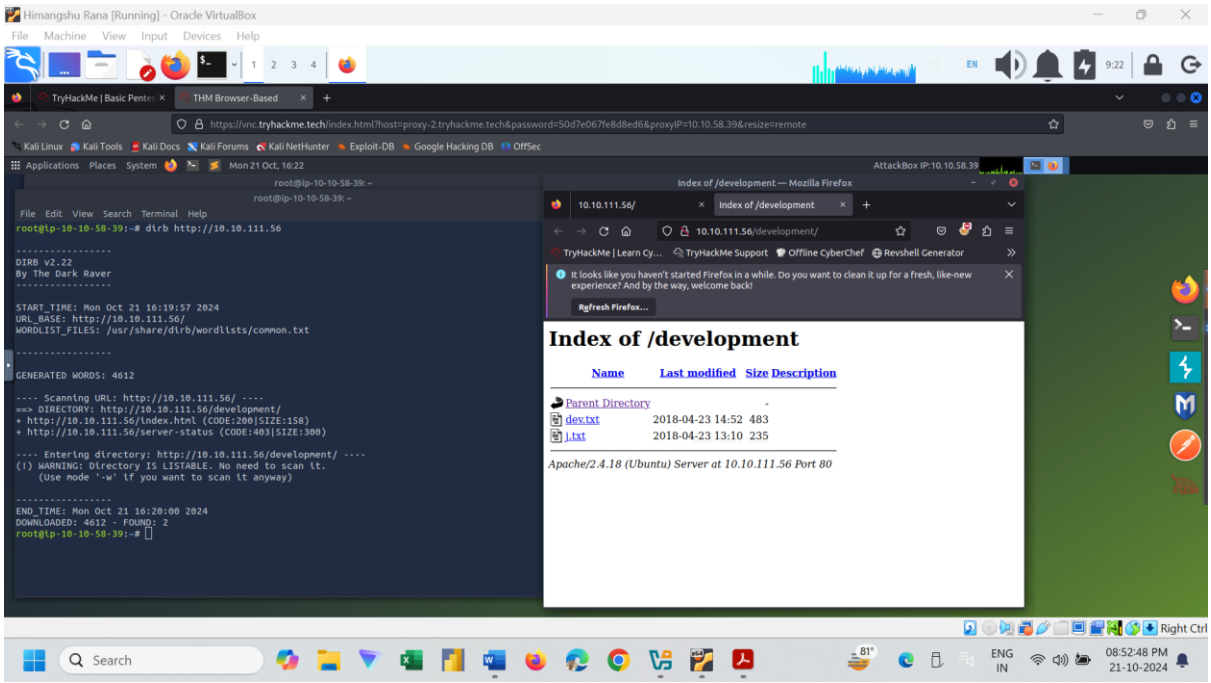
Step 1: Search the IP in Broswer



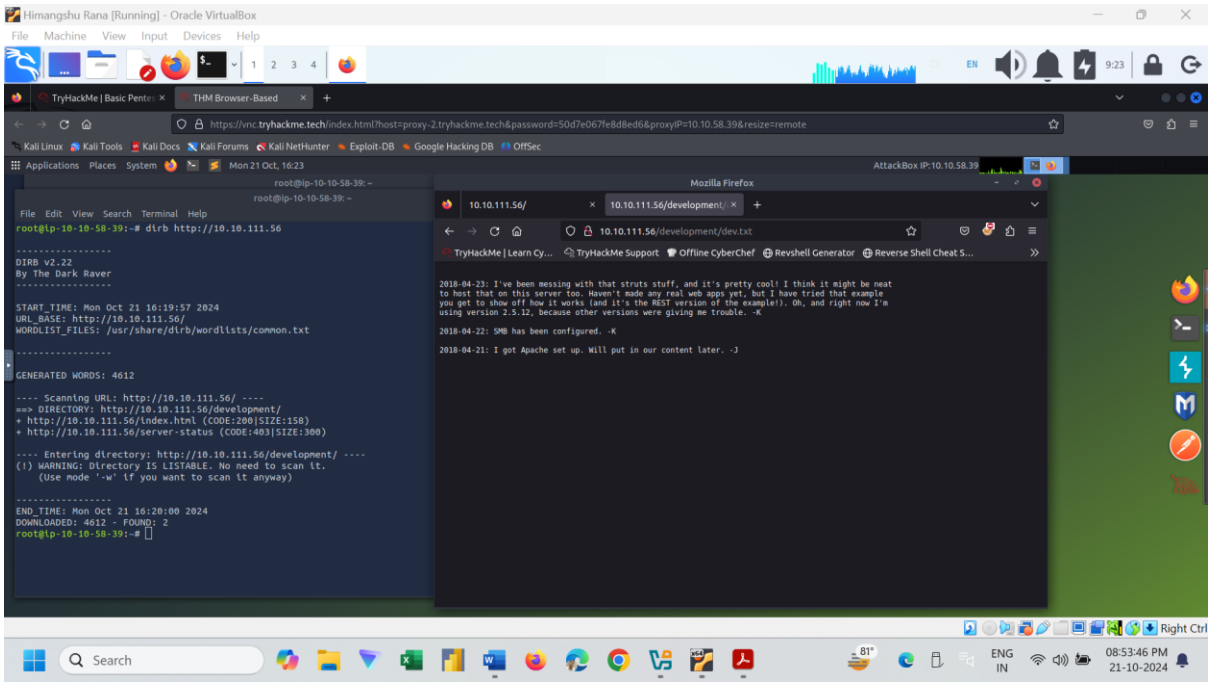
Step 2: There are probably some changes on the home page. Now check the page source.

```
<html>

<h1>Undergoing maintenance</h1>

<h4>Please check back later</h4>

<!-- Check our dev note section if you need to know what to work on. -->


</html>

```

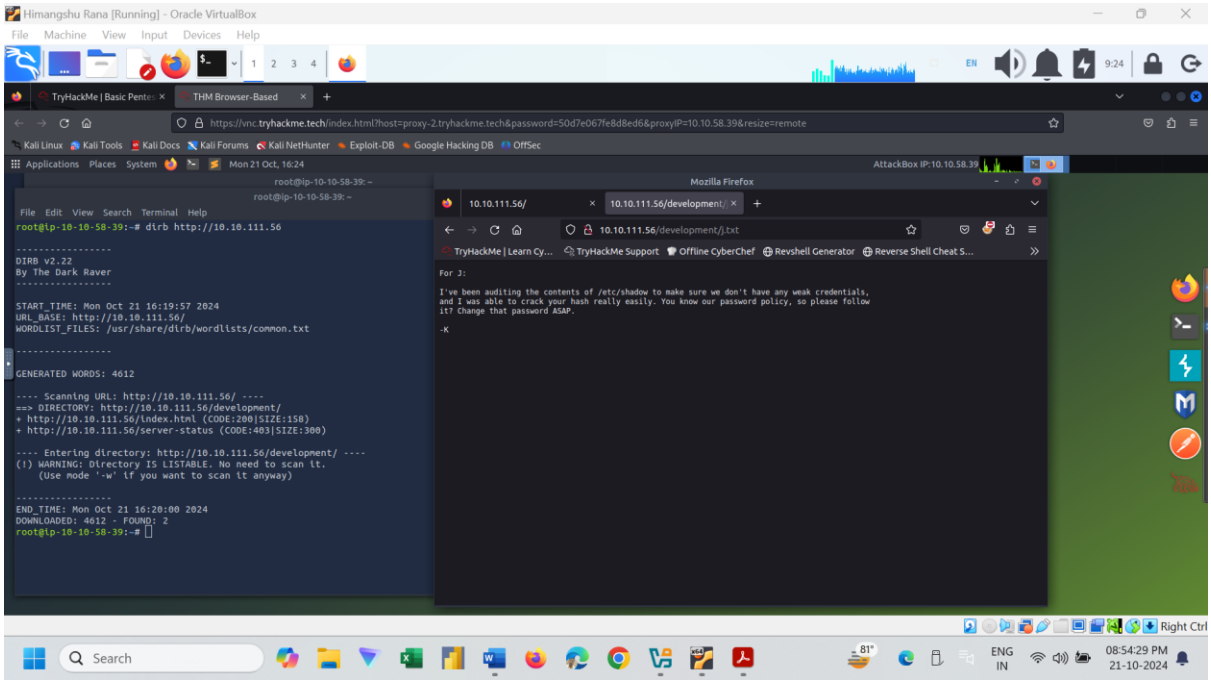
Step 3: Use Dirb tool to find hidden section in a website(Use Command- dirb http://10.10.111.56). Now Goto the Hidden Directory (http://10.10.111.56/development/)



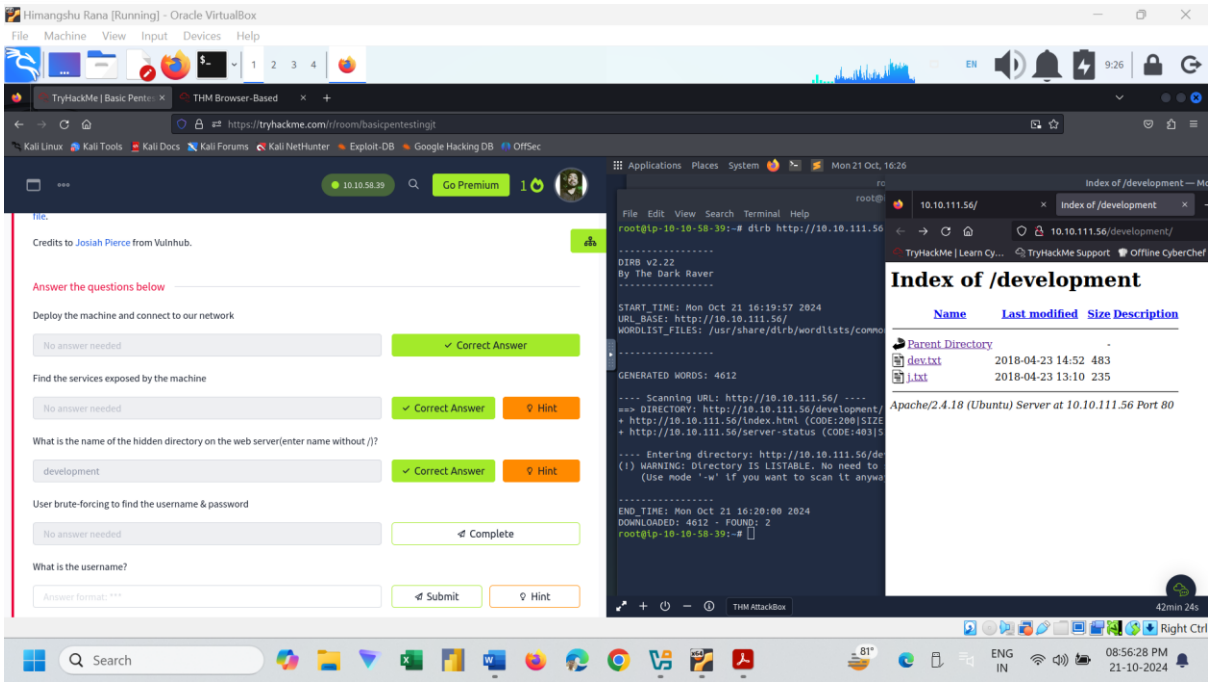
Step 4: Open the dev.txt



Step 5: Now open the j.txt

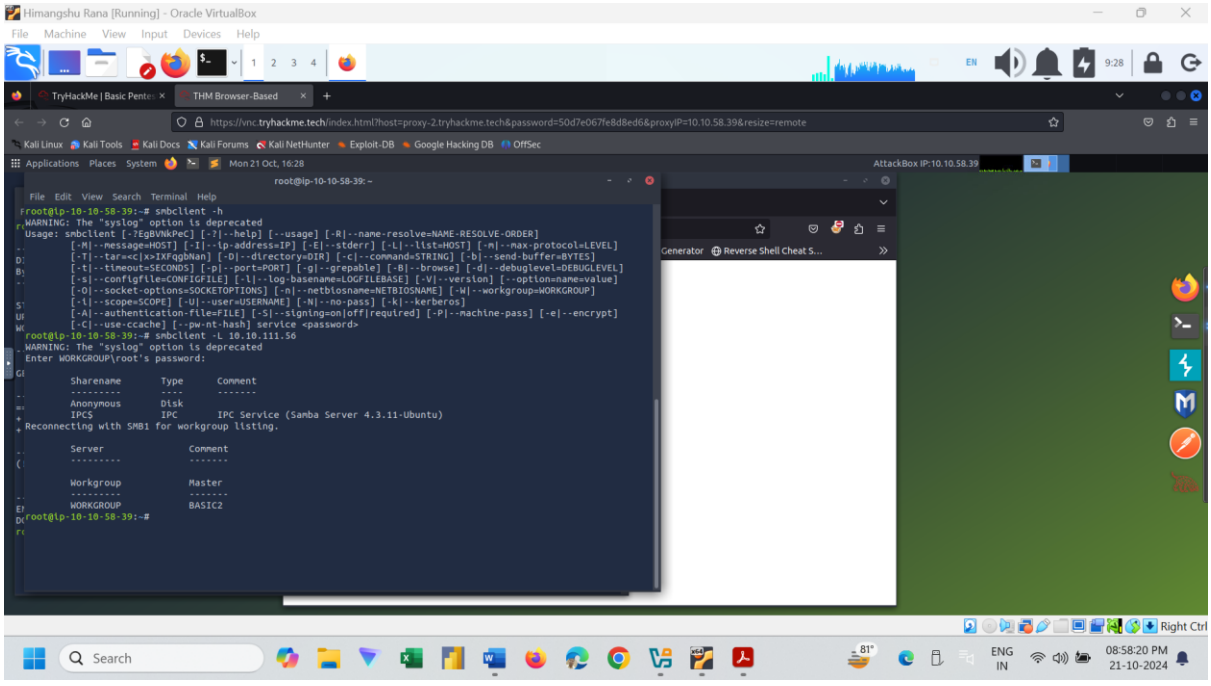


Step 6: Fill the Answer



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

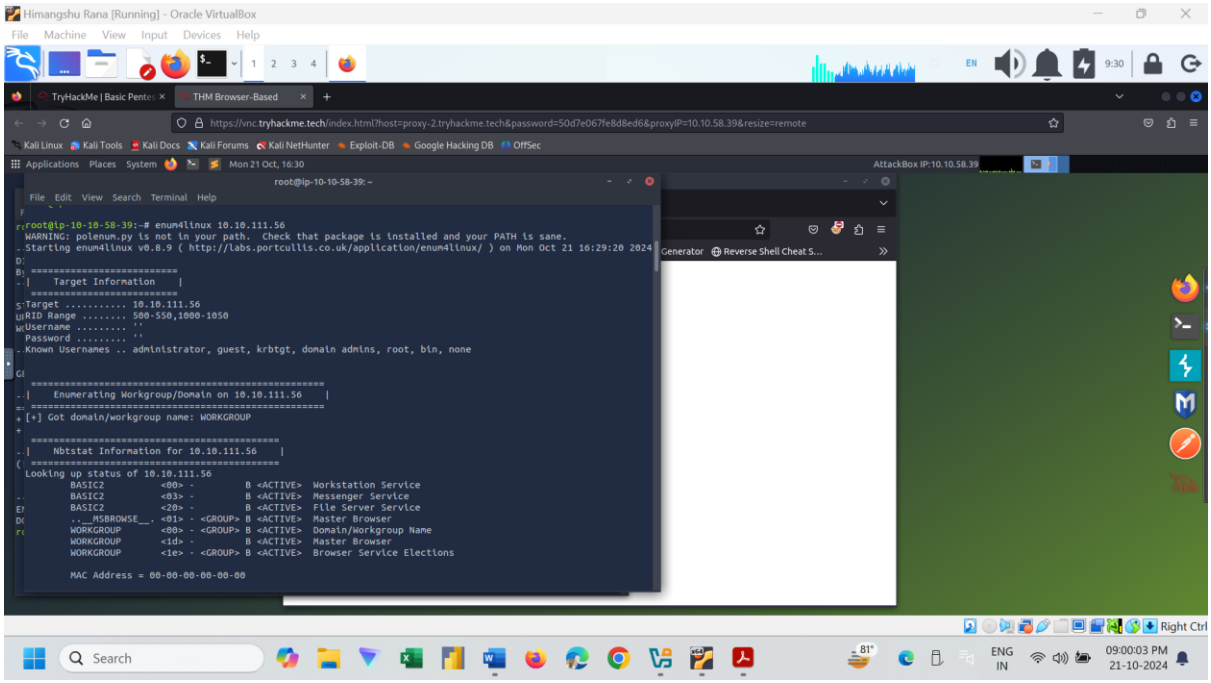
Now use smb command to interact with host because of the smb port is open. (Use command – smbclient -L 10.10.111.56). There is an one Anonymous login is enabled.



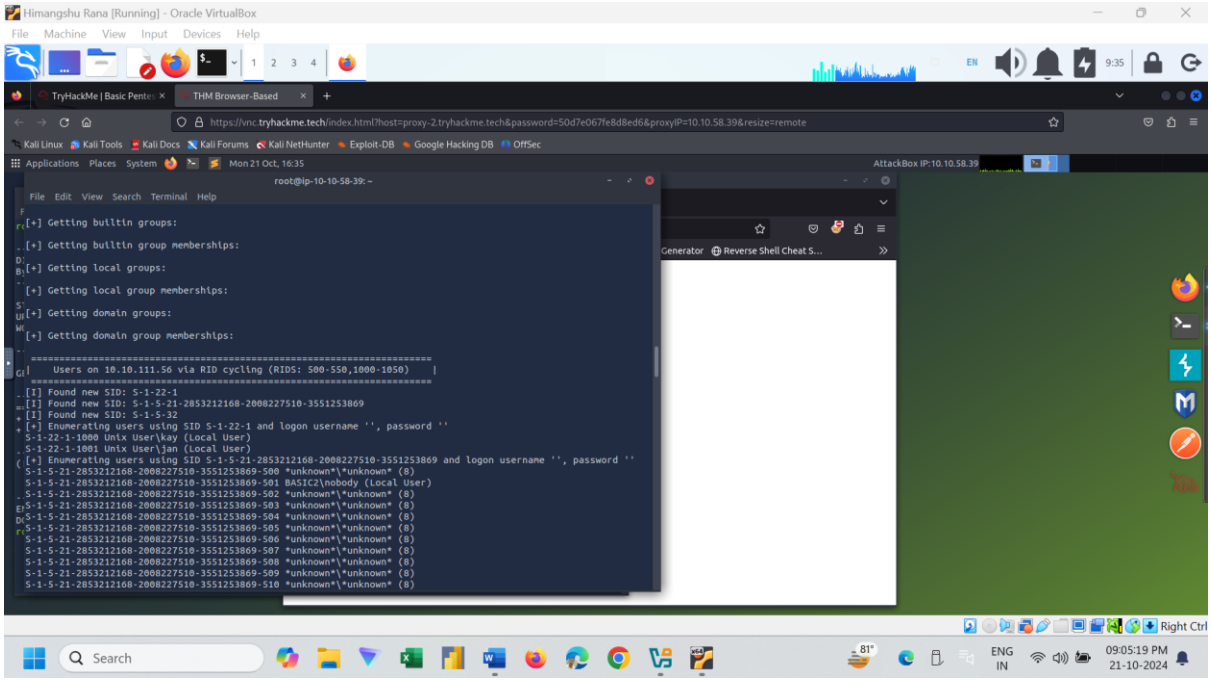
Task 5: What is the username?

Answer is : jan

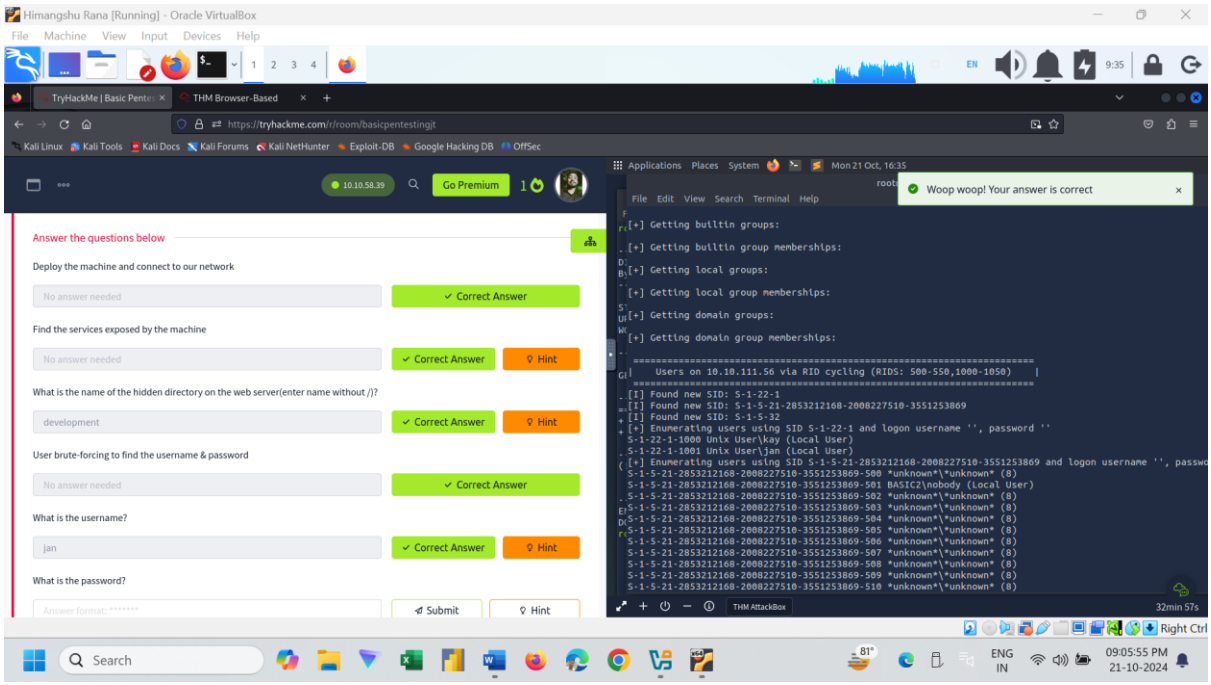
Now use the enum4linux for collecting details about users (use command enum4linux 10.10.111.56)



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



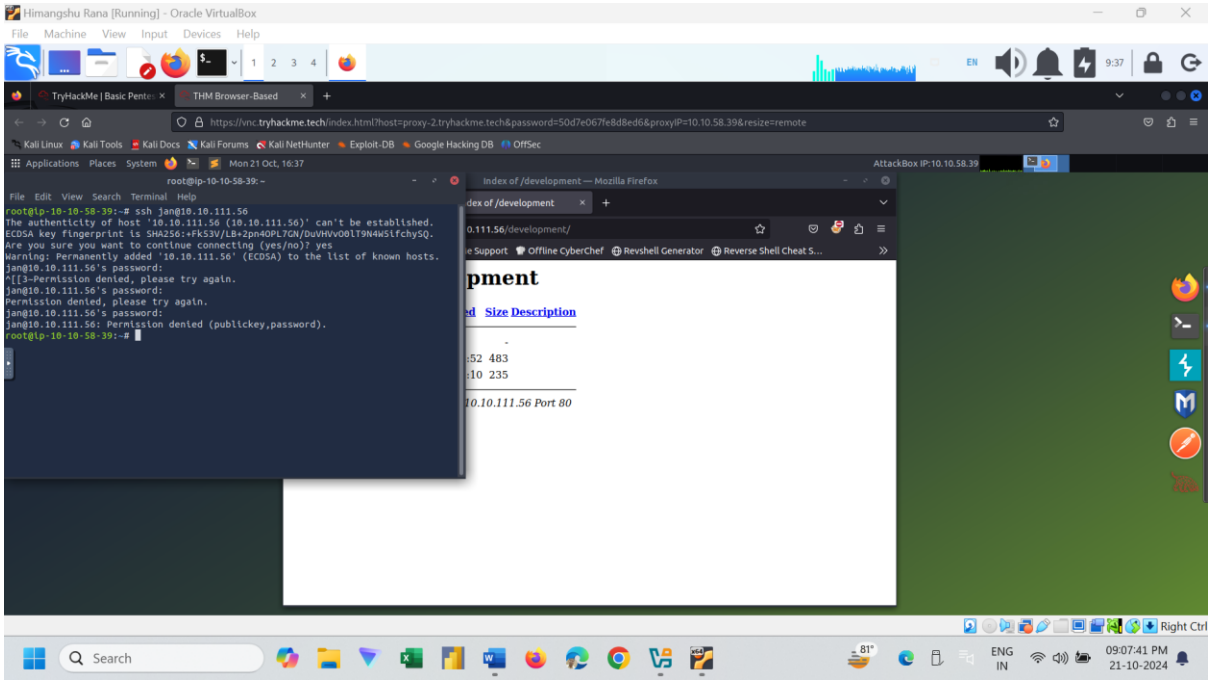
Fill the answer



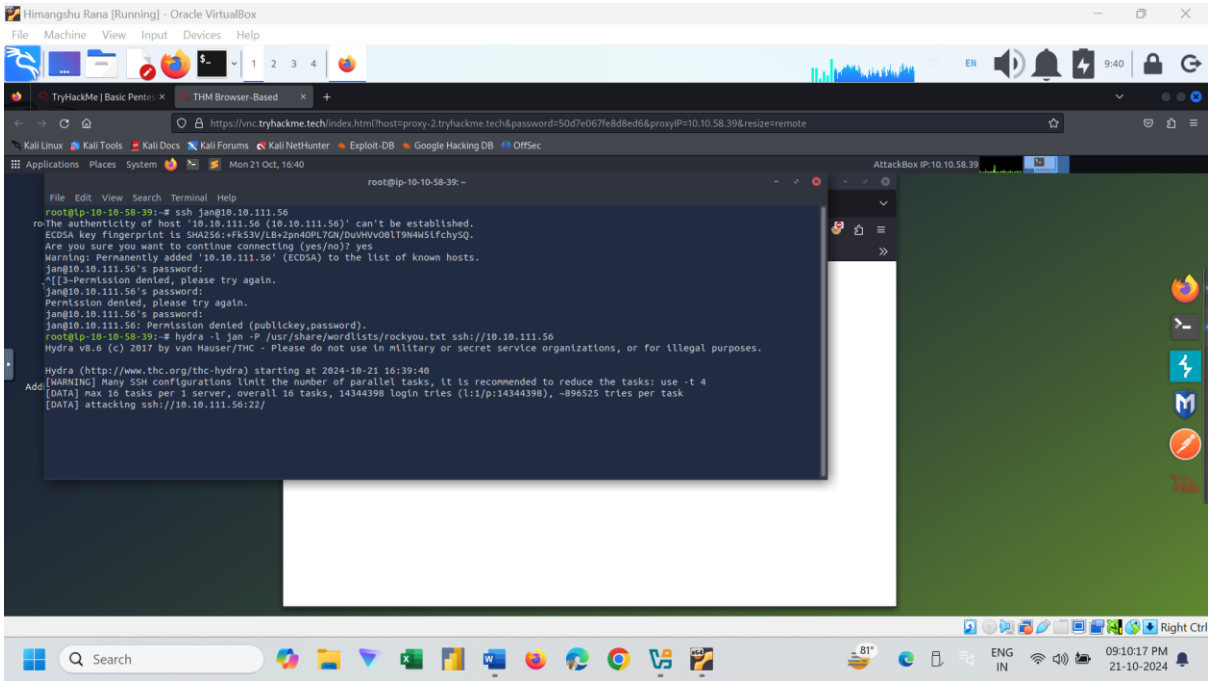
Task 6: What is the password?

Answer is : armando

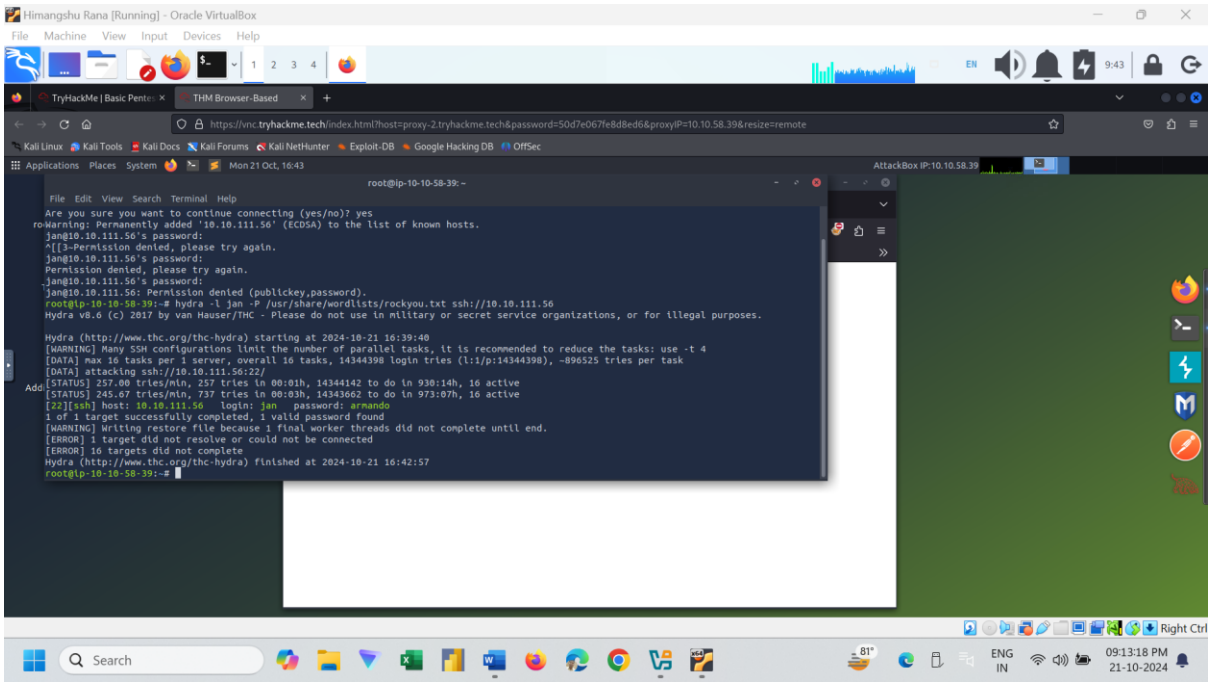
Step 1: From Nmap scan result, found that the SSH service was running on port 22. But we need username and password to connect. Try to run SSH command (ssh jan@10.10.111.56)



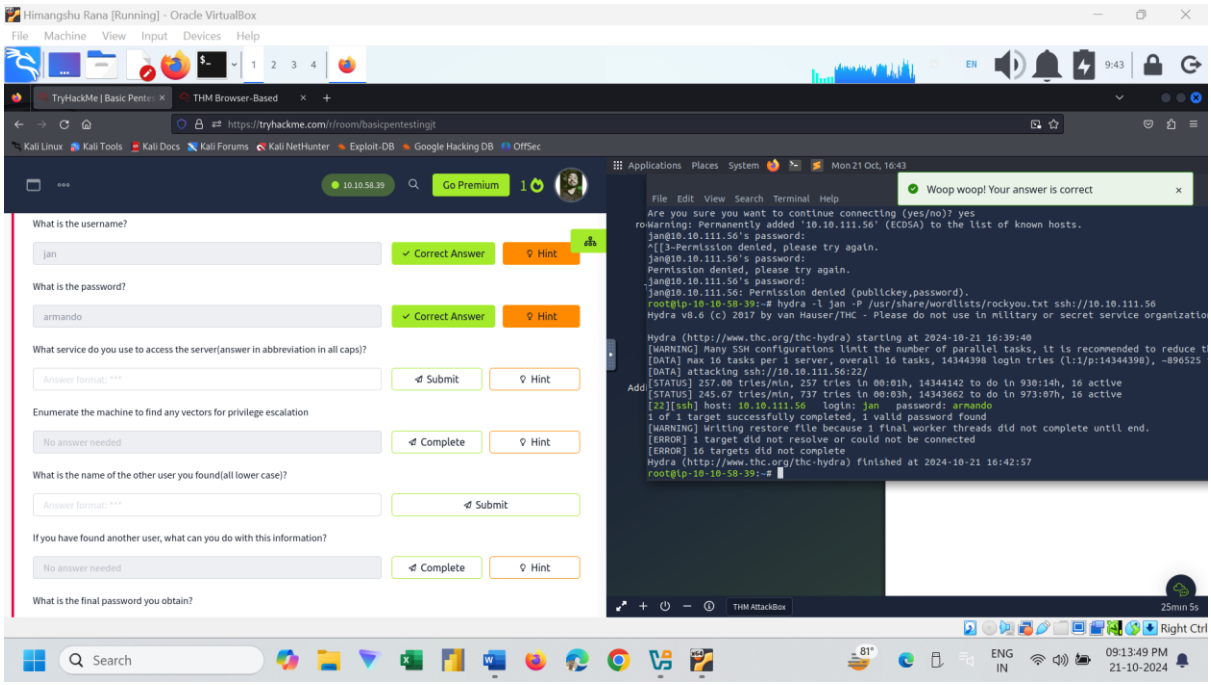
Step 2: Now use Hydra to Brute-Force the Password (use command- hydra -l jan -P /usr/share/wordlists/rockyou.txt ssh:// 10.10.111.56)



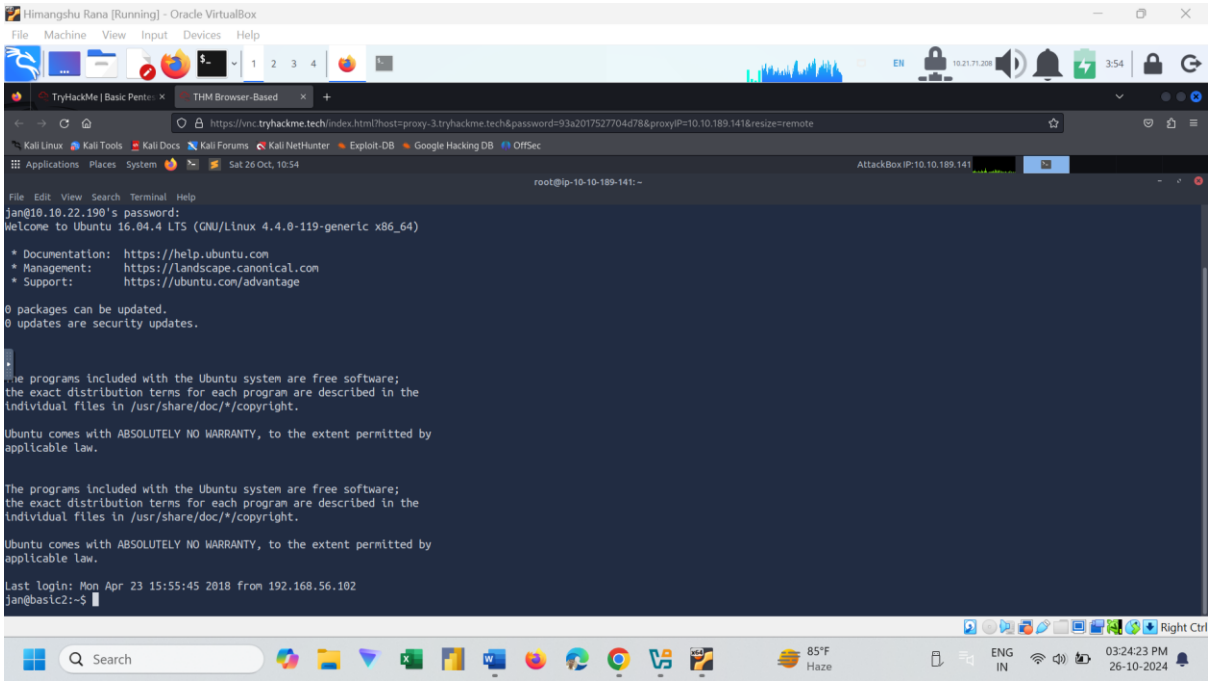
And the Password is armando



Step 3: Fill the Answer



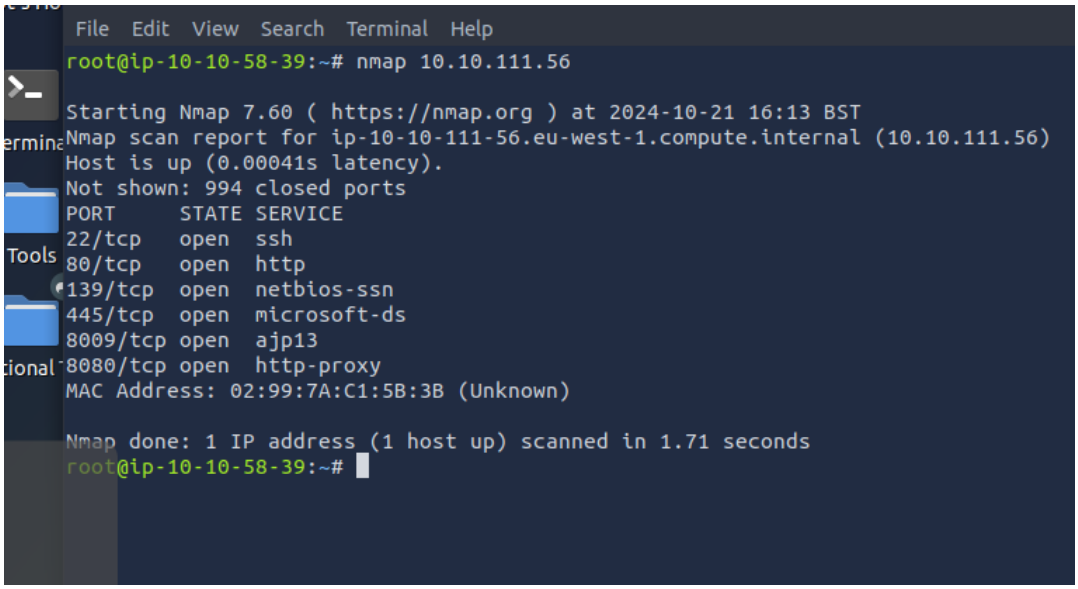
Step 4: Connect to the system via SSH using Jan's credentials.(use command- ssh jan@10.10.111.56)



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

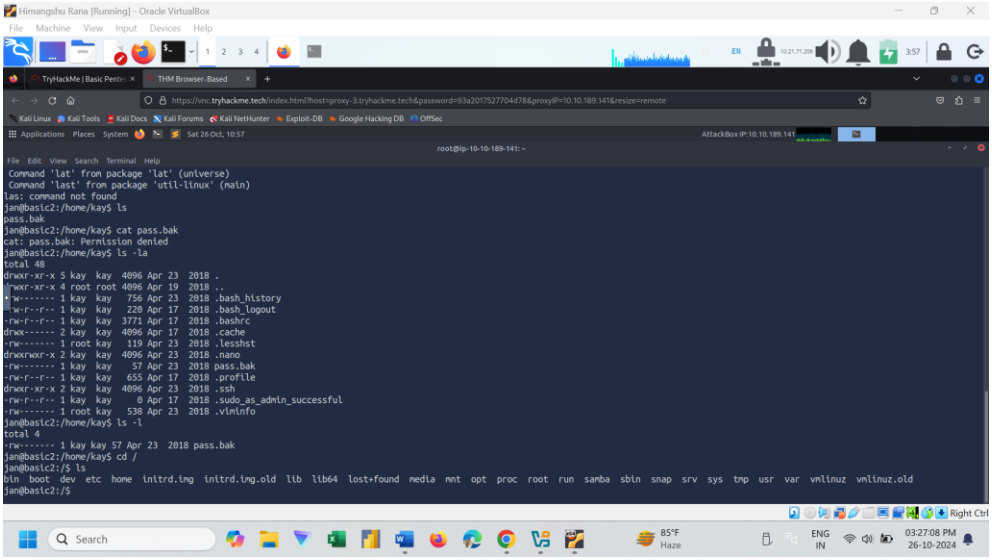
Answer is- SSH

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.

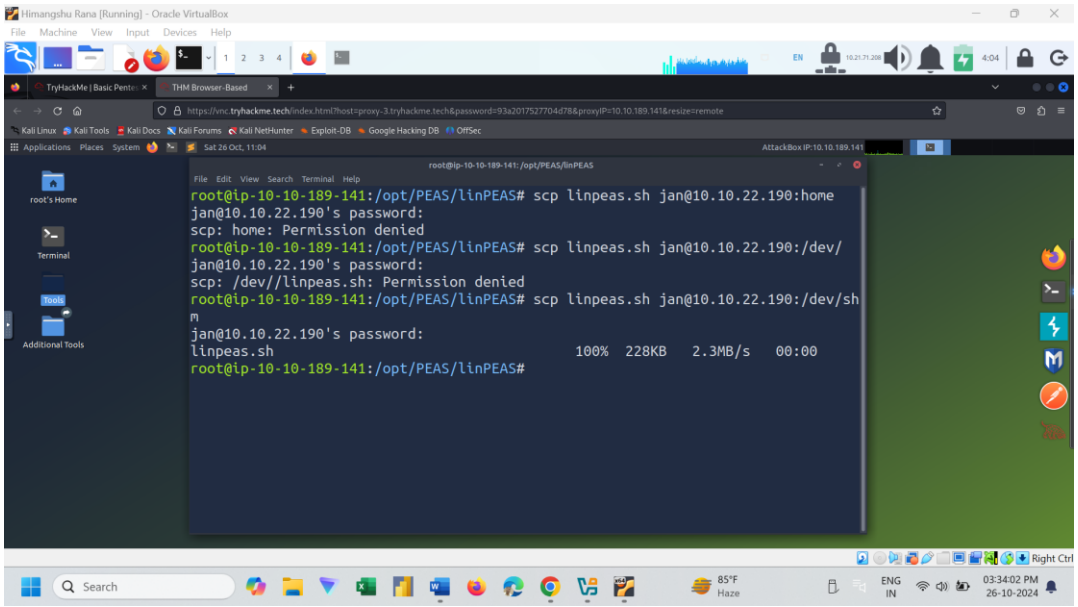


Task 8: Enumerate the machine to find any vectors for privilege escalation

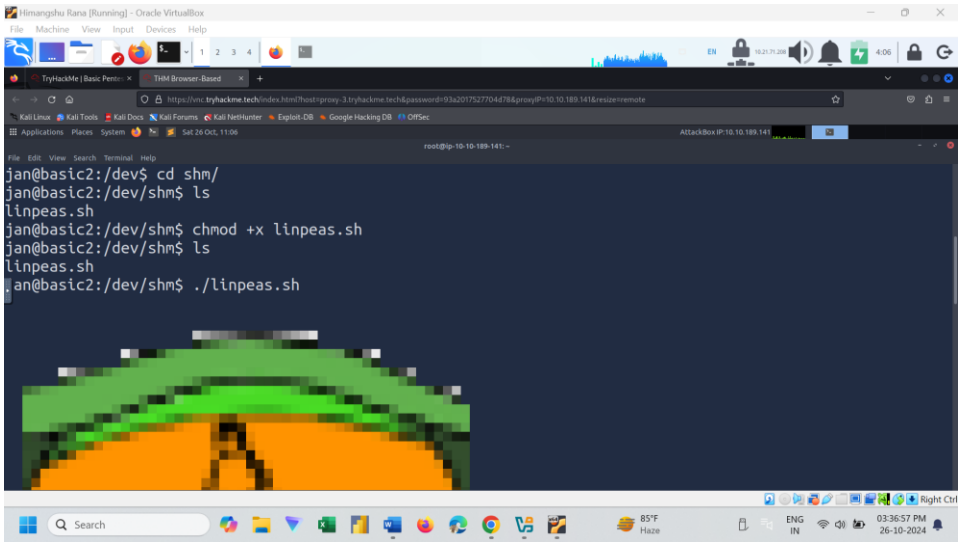
Step 1: As already connect to the system now Explore the system There is a file name pass.bak. Use the cat command to view the file content and But to open it we need root permission. Jan don`t have the permission to access it.



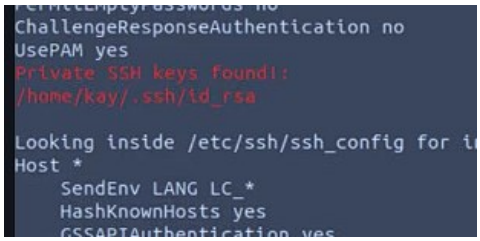
Step 2: Now we use linpeas.sh for privilege escalation auditing. First of all, I have to Copy the Linpeas.sh file to the Target Machine. I Use SCP command to Copy.



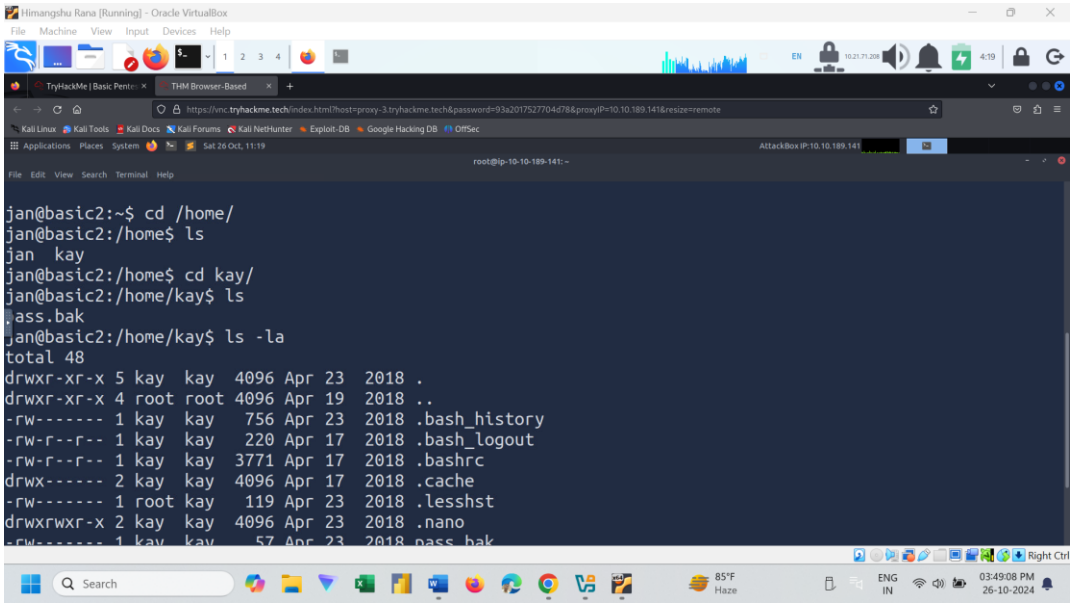
Step 3: Now I have to give Execute Permission to the linpeas.sh file. And Run the linpeas.sh file for Privilege Escalation auditing.

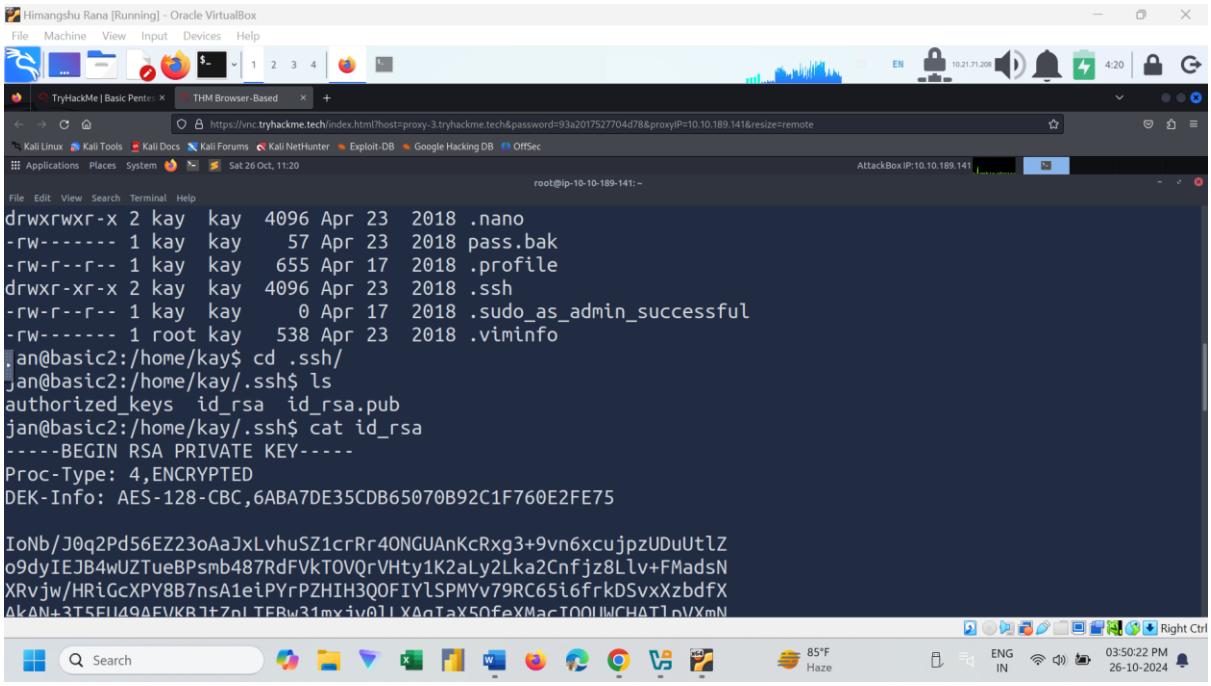


Step 4: In the Software Information section I found SSH Key and we can use this to perform Privilege Escalation



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



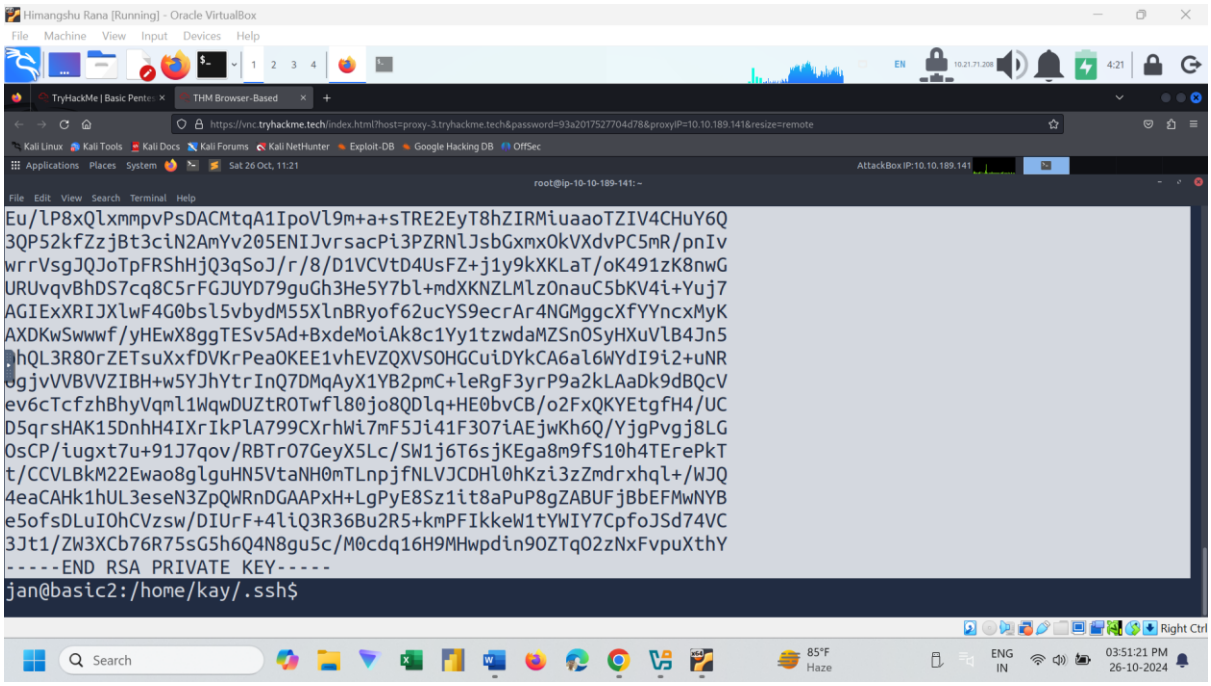

Himangshu Rana [Running] - Oracle VirtualBox
File Machine View Input Devices Help
TryHackMe | Basic Pente
THM Browser-Based
https://vnc.tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=93a2017527704d78&proxyIP=10.10.189.141&resize=remote
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Applications Places System Sat 26 Oct, 11:20
AttackBox IP:10.10.189.141
root@ip-10-10-189-141: ~
File Edit View Search Terminal Help
drwxrwxr-x 2 kay kay 4096 Apr 23 2018 .nano
-rw------- 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 0 Apr 17 2018 .sudo_as_admin_successful
-rw------- 1 root kay 538 Apr 23 2018 .viminfo
jan@basic2:/home/kay$ cd .ssh/
jan@basic2:/home/kay/.ssh$ ls
authorized_keys id_rsa id_rsa.pub
jan@basic2:/home/kay/.ssh$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75
IoNb/J0q2Pd56EZ23oAaJxLvhuSZ1crRr4ONGUAnKcRxg3+9vn6xcujpzUDuUtlZ
o9dyIEJB4wUZTueBPsmb487RdFVkTOVQrVHty1K2aLy2Lka2Cnfjz8Llv+FMadsN
XRvjw/HRiGcXPY8B7nsA1eiPYrPZHIH3QOFIYlSPMYv79RC65i6frkDSvxXzbdfX
Search
85°F Haze
ENG IN
03:50:22 PM 26-10-2024
Right Ctrl

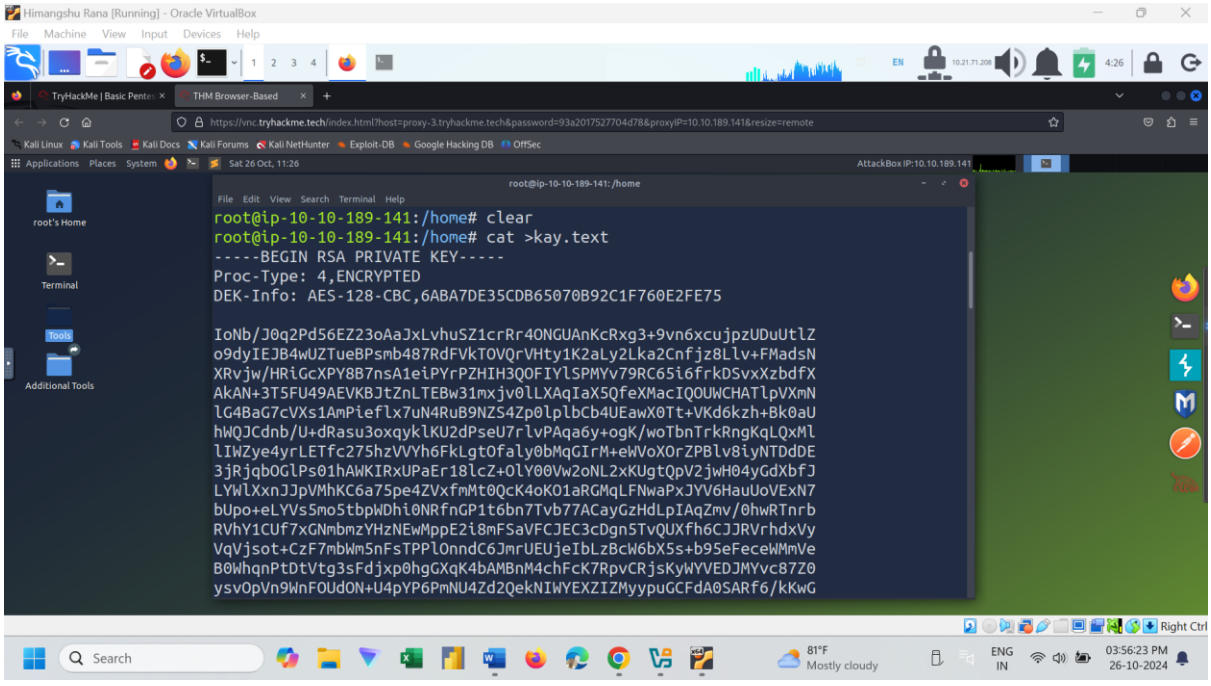
Task 9: What is the name of the other user you found ?

Answer is: kay

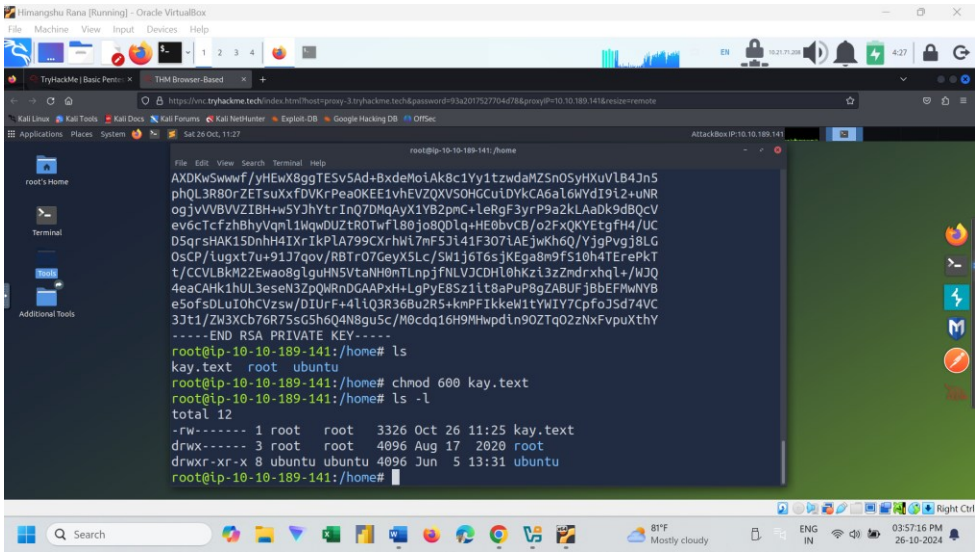
Task 10: If you have found another user, what can you do with this information?

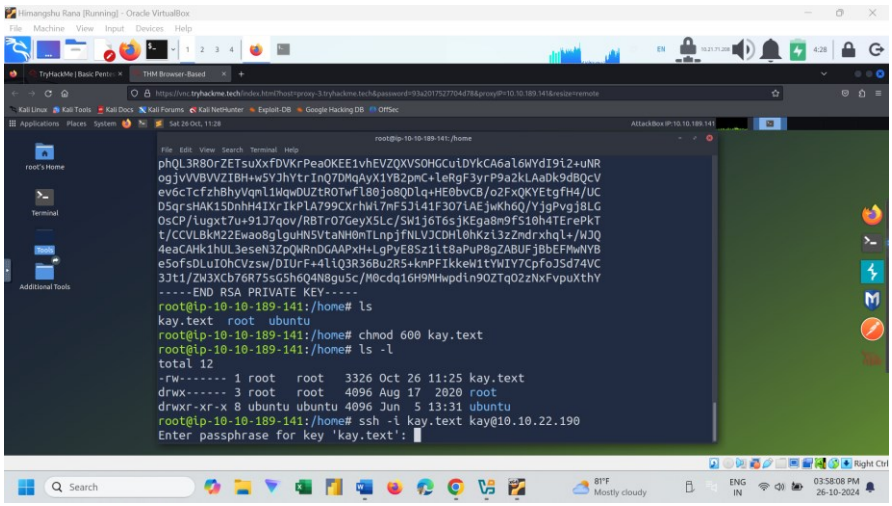
Step 1: Now I have the Private key. Lets Copy it my Terminal and create a file name kay.text

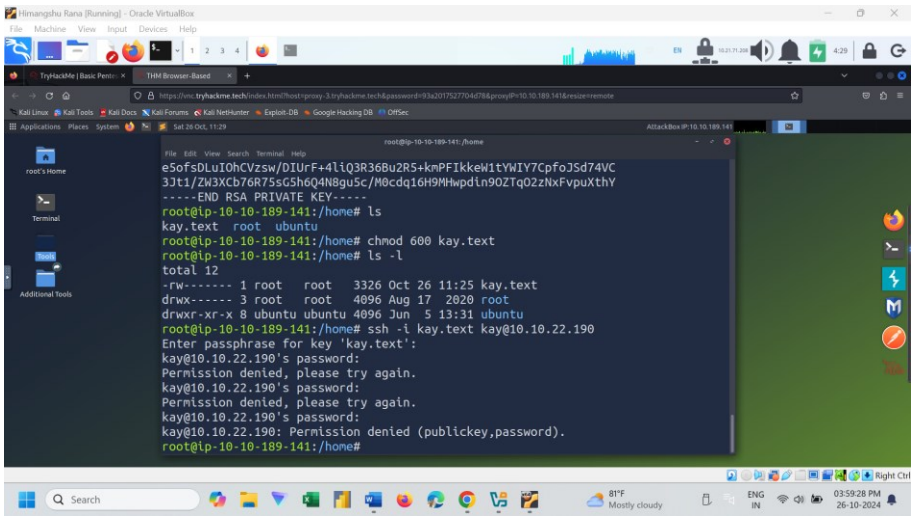




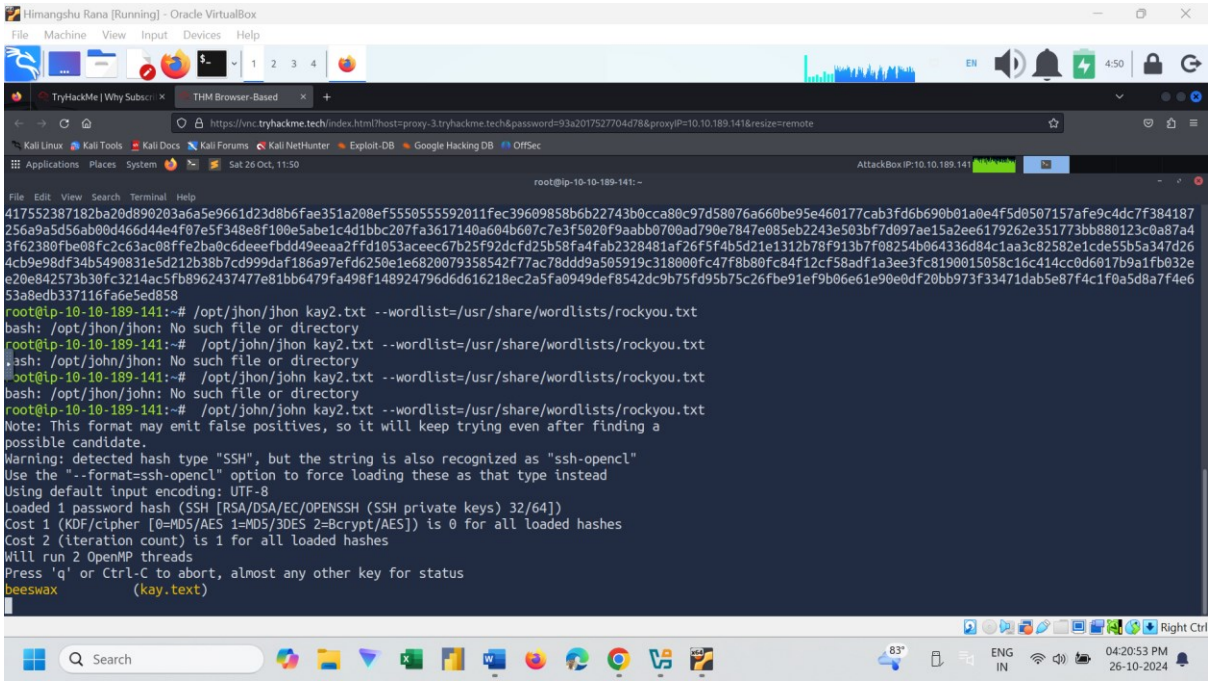
Step 2: I use SSH Private Key to access the Target Machine. And also, I have to give read write Permission to the kay.text file.



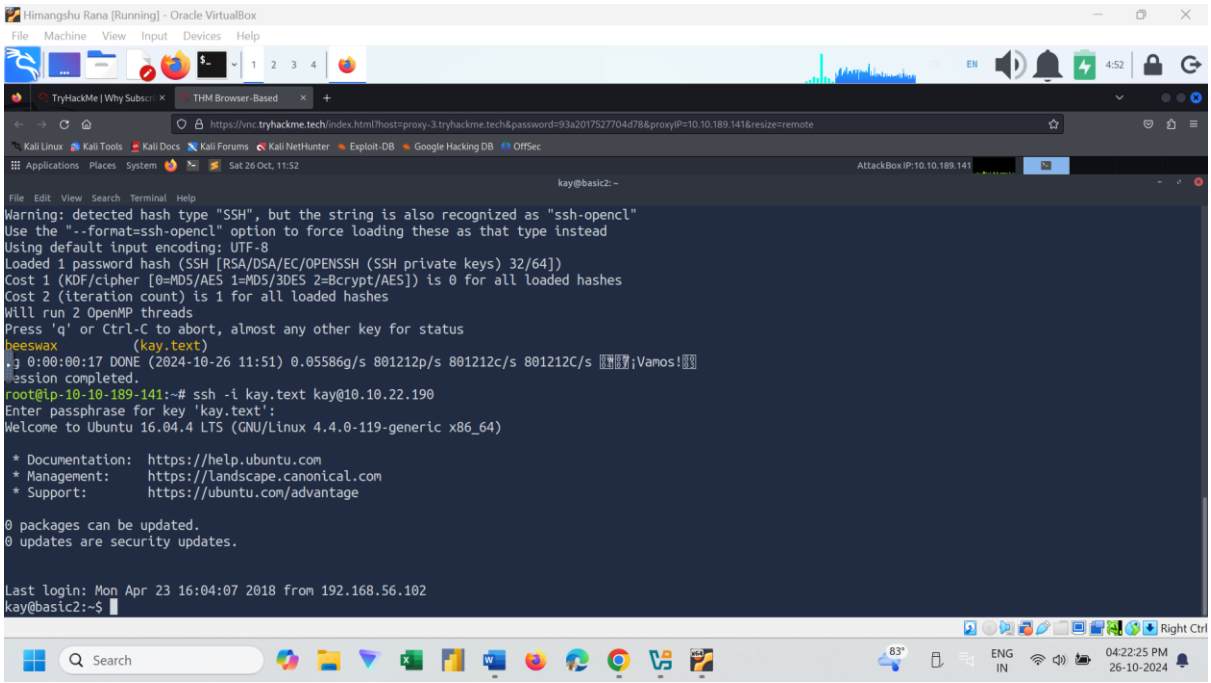




Step 3: I need the Password for the Private key and Now I use John The Ripper to crack this hash and extract the SSH private key password.



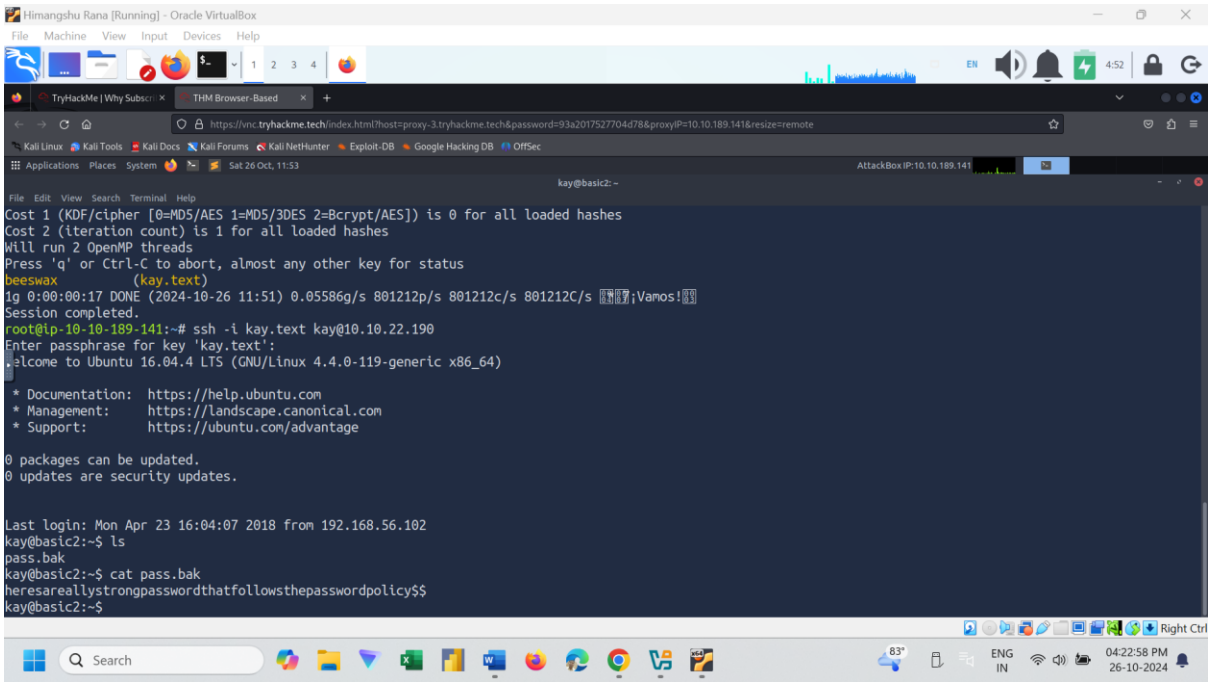
Step 4: Now we can Access the Targer Machine using SSH Private Key



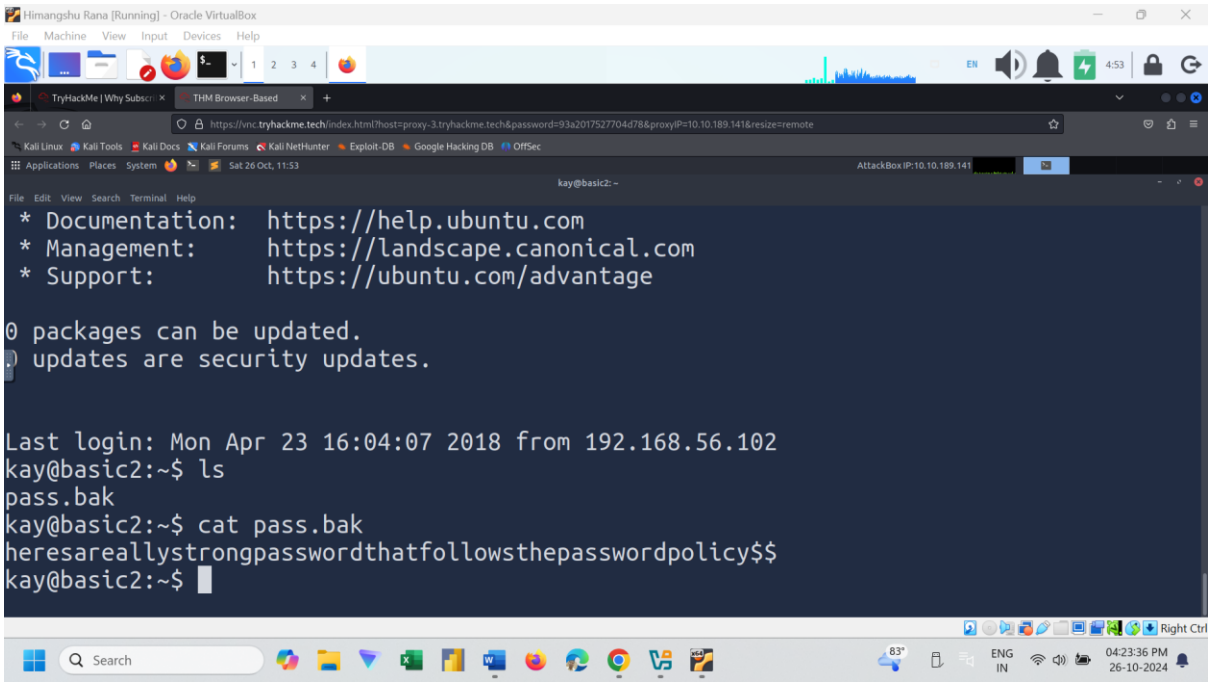
Task 11 : What is the final password you obtain?

Answer is : heresareallystrongpasswordthatfollowsthepasswordpolicy$$

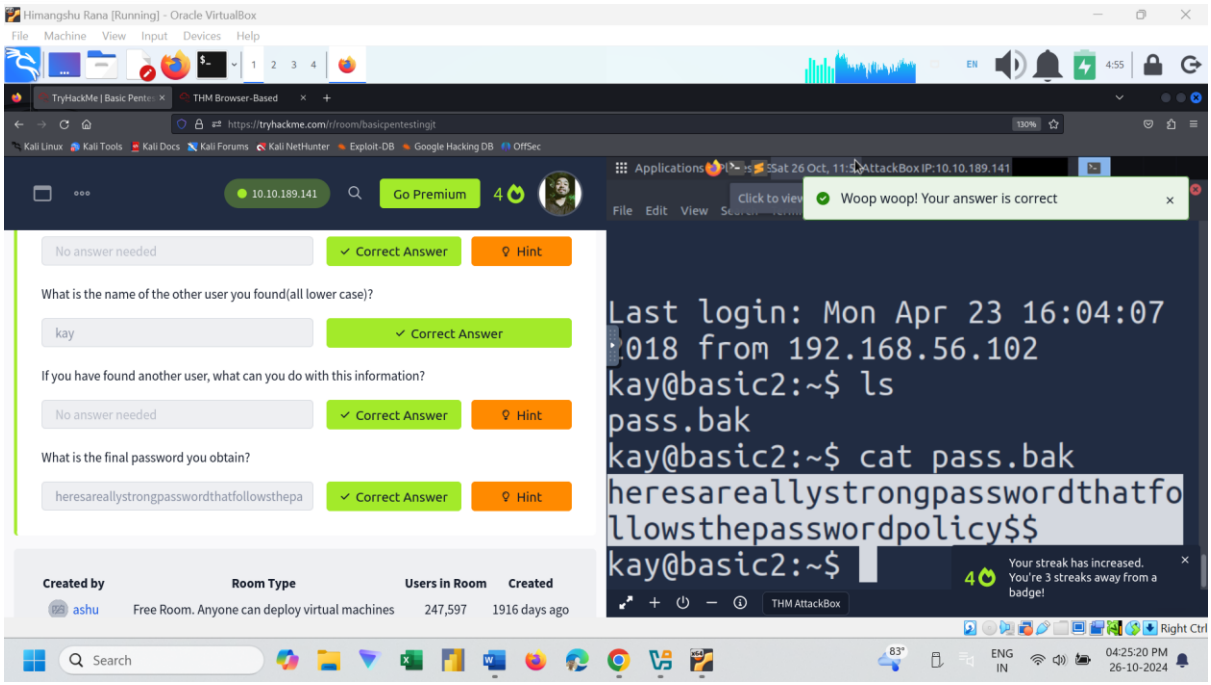
Using kay find that pass.bak file and open it to get the final Password

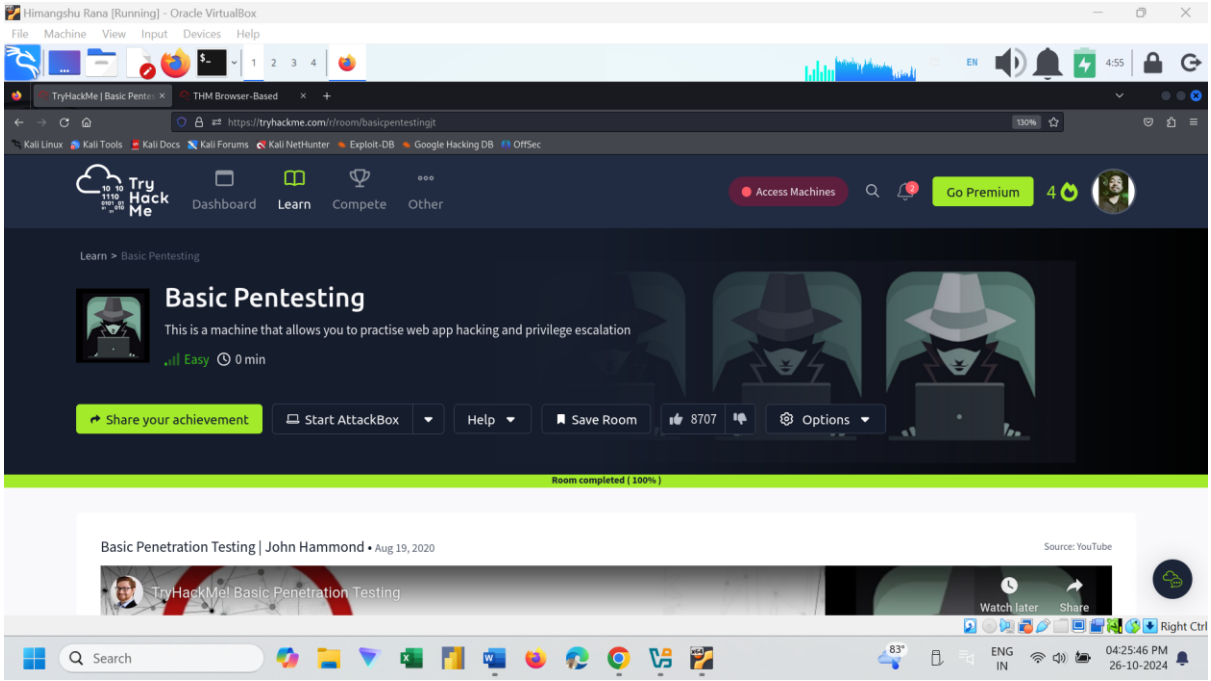


The Final Password is heresareallystrongpasswordthatfollowsthepasswordpolicy$$



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://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