Basic_Pentesting

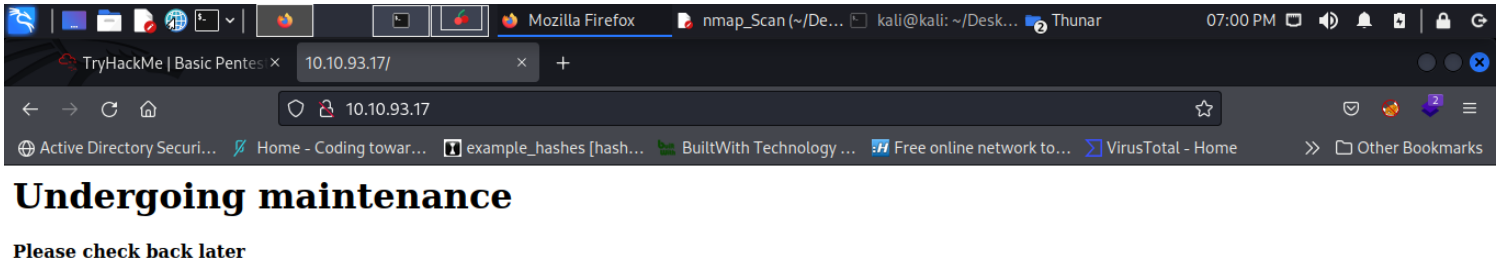
nmap_Scan

```
nmap -T4 -A -p- 10.10.233.127 > Nmap_Scan
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-18 22:52 EDT
Warning: 10.10.233.127 giving up on port because retransmission cap hit (6).
Stats: 0:00:52 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 12.92% done; ETC: 22:59 (0:05:44 remaining)
Stats: 0:00:52 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 12.94% done; ETC: 22:59 (0:05:50 remaining)
Nmap scan report for 10.10.233.127
Host is up (0.51s latency).
Not shown: 4900 closed tcp ports (conn-refused), 96 filtered tcp ports (no-response)
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 db:45:cb:be:4a:8b:71:f8:e9:31:42:ae:ff:f8:45:e4 (RSA)
|   256 09:b9:b9:1c:e0:bf:0e:1c:6f:7f:fe:8e:5f:20:1b:ce (ECDSA)
|_  256 a5:68:2b:22:5f:98:4a:62:21:3d:a2:e2:c5:a9:f7:c2 (ED25519)
80/tcp  open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: 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)
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h19m54s, deviation: 2h18m34s, median: -5s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2022-03-19T02:58:28
|_  start_date: N/A
|_nbstat: NetBIOS name: BASIC2, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: basic2
|   NetBIOS computer name: BASIC2\x00
|   Domain name: \x00
|   FQDN: basic2
|_  System time: 2022-03-18T22:58:27-04:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 363.72 seconds
```

Notes

After our nmap scan we see 4 ports open 22 ssh, 80 http, 139,445 smb/netbios.
Lets take a look at port 80 first.

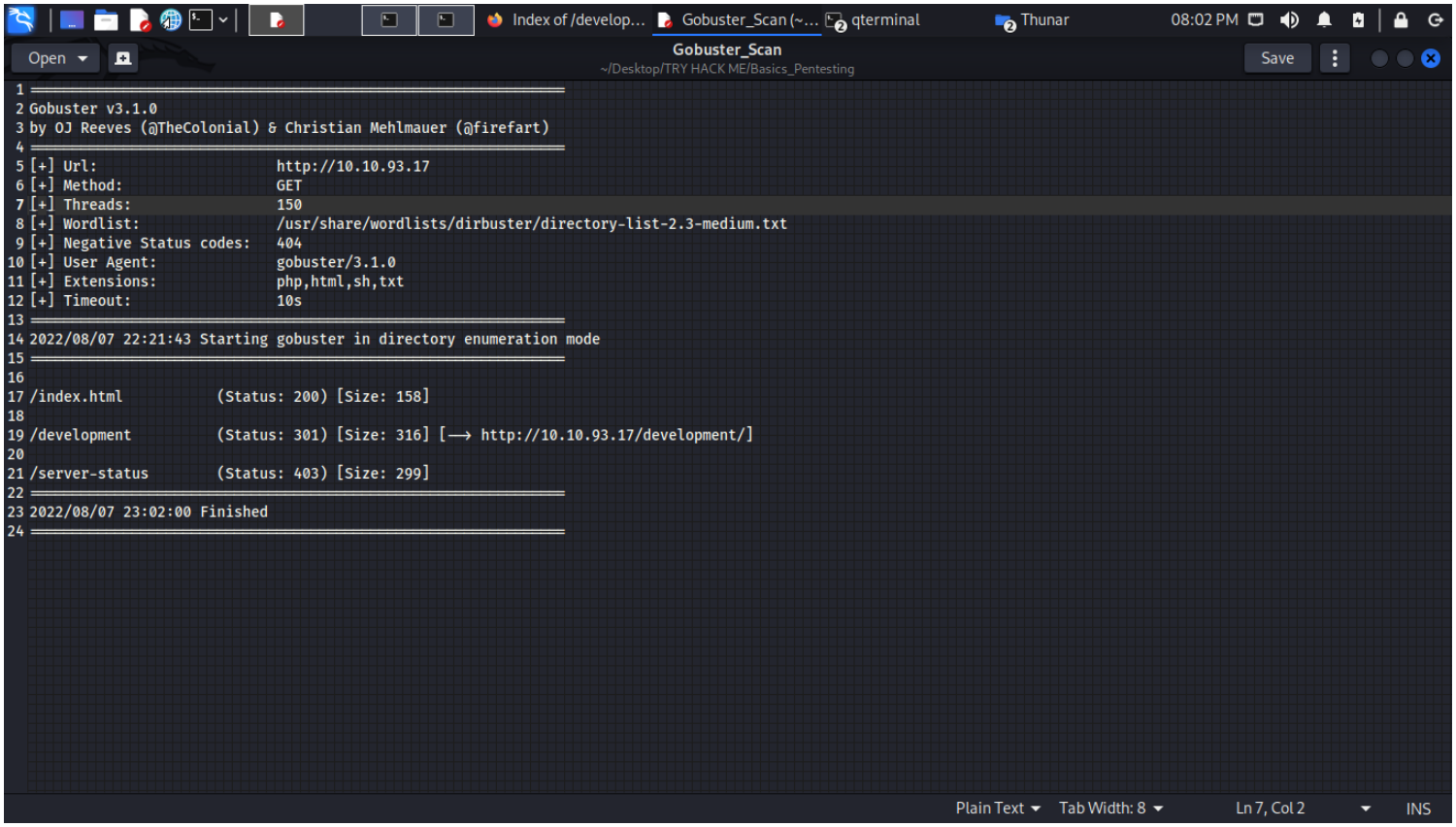
Webpage



Notes

We travel over to the website and see it is under maintenance.
I also viewd the source code but found nothing. Lets see if we can find some hidden directories with dobuster.

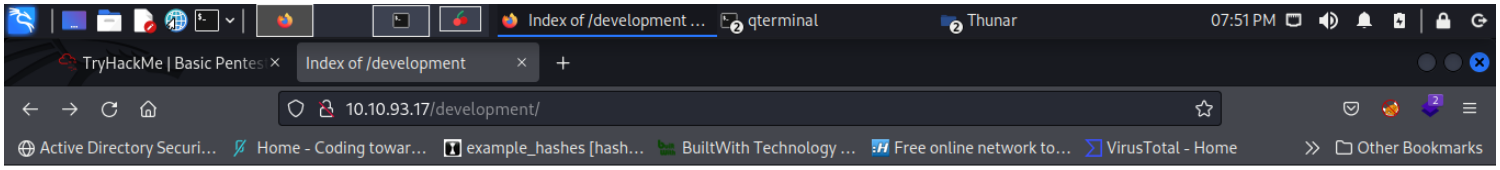
Gobuster_Scan



Notes

We find 2 directories, /development, and index.html.
Command used: gobuster dir -u http://10.10.93.17 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,sh,txt -t 150 > Gobuster_Scan

/development

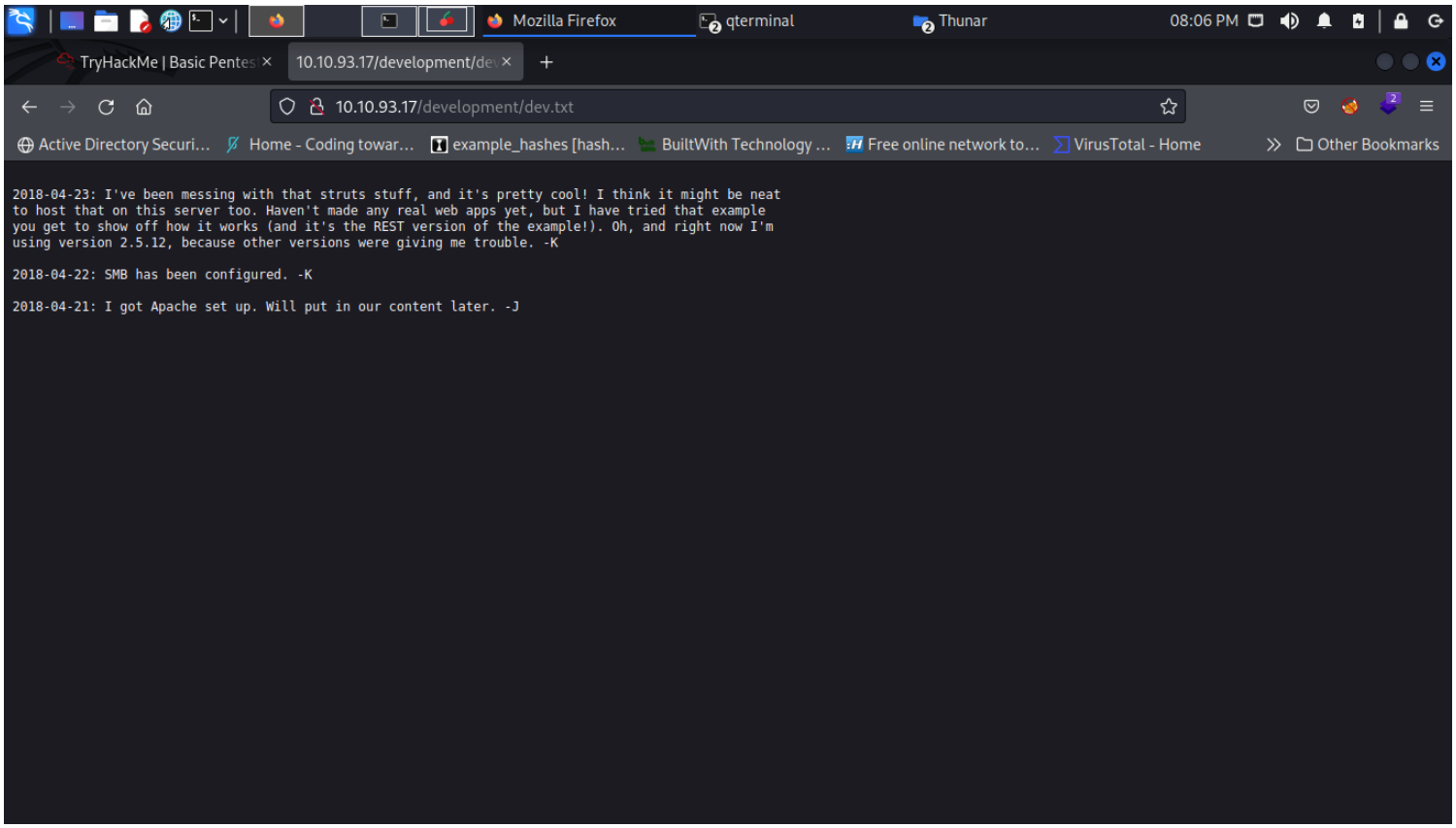


Index of /development

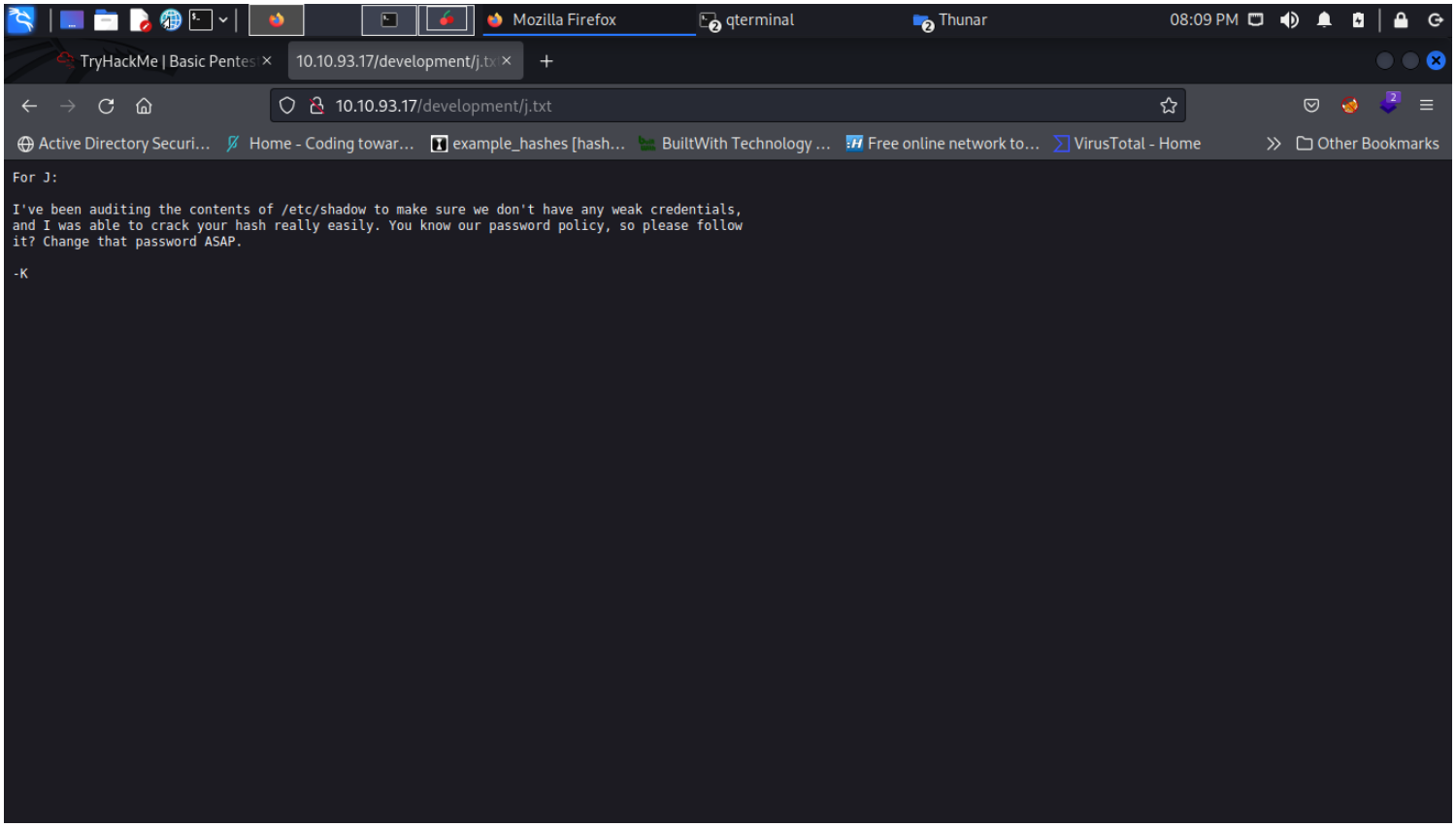
Name	Last modified	Size	Description
Parent Directory		-	
dev.txt	2018-04-23 14:52	483	
j.txt	2018-04-23 13:10	235	

Apache/2.4.18 (Ubuntu) Server at 10.10.93.17 Port 80

Dev_Note



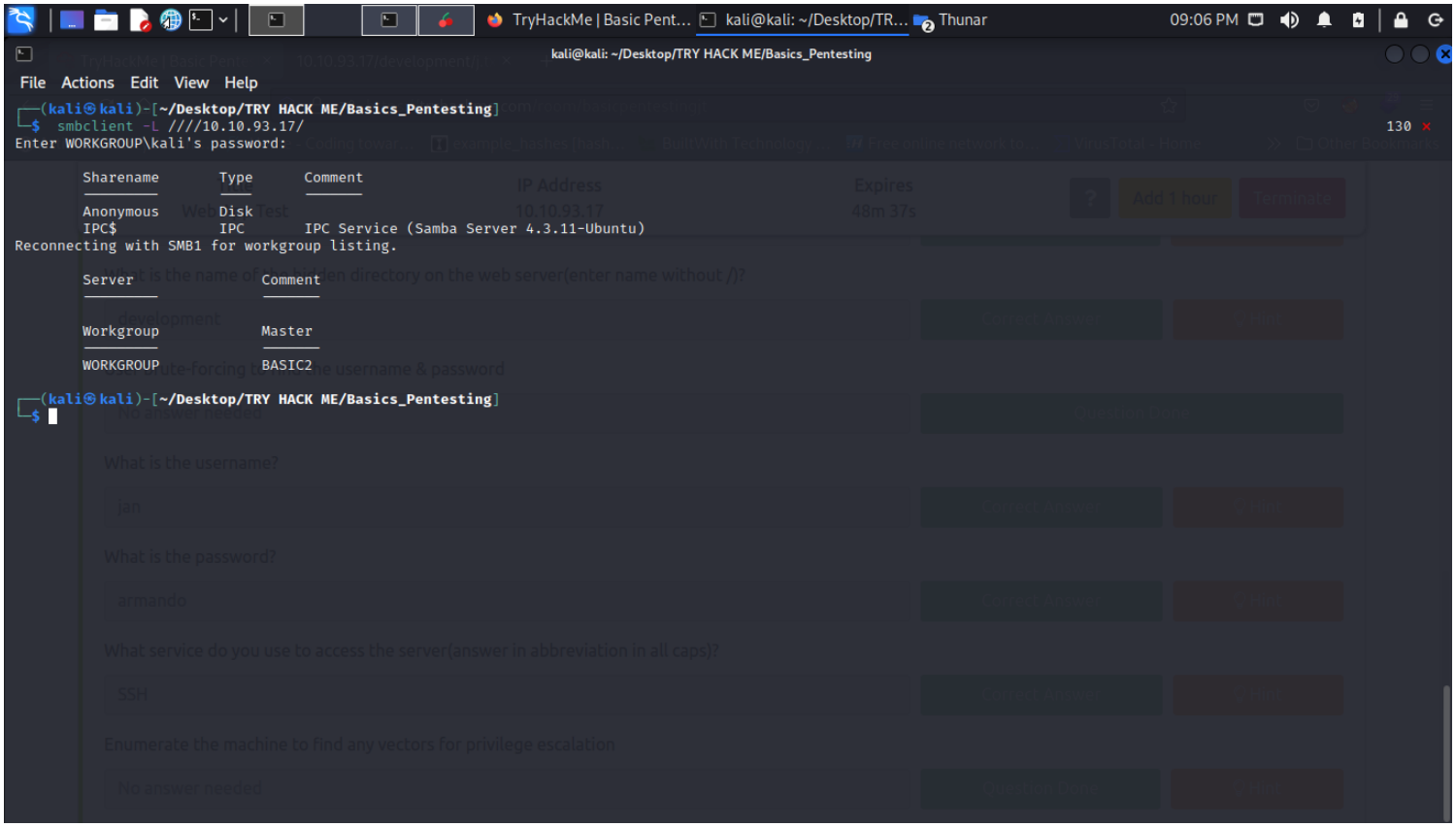
J.txt



Notes

In dev.txt we find a version 2.5.12, that smb has been configured , and that they are using Apache.
In j.txt we find that they may have weak passwords.
Lets now take a look at smb.

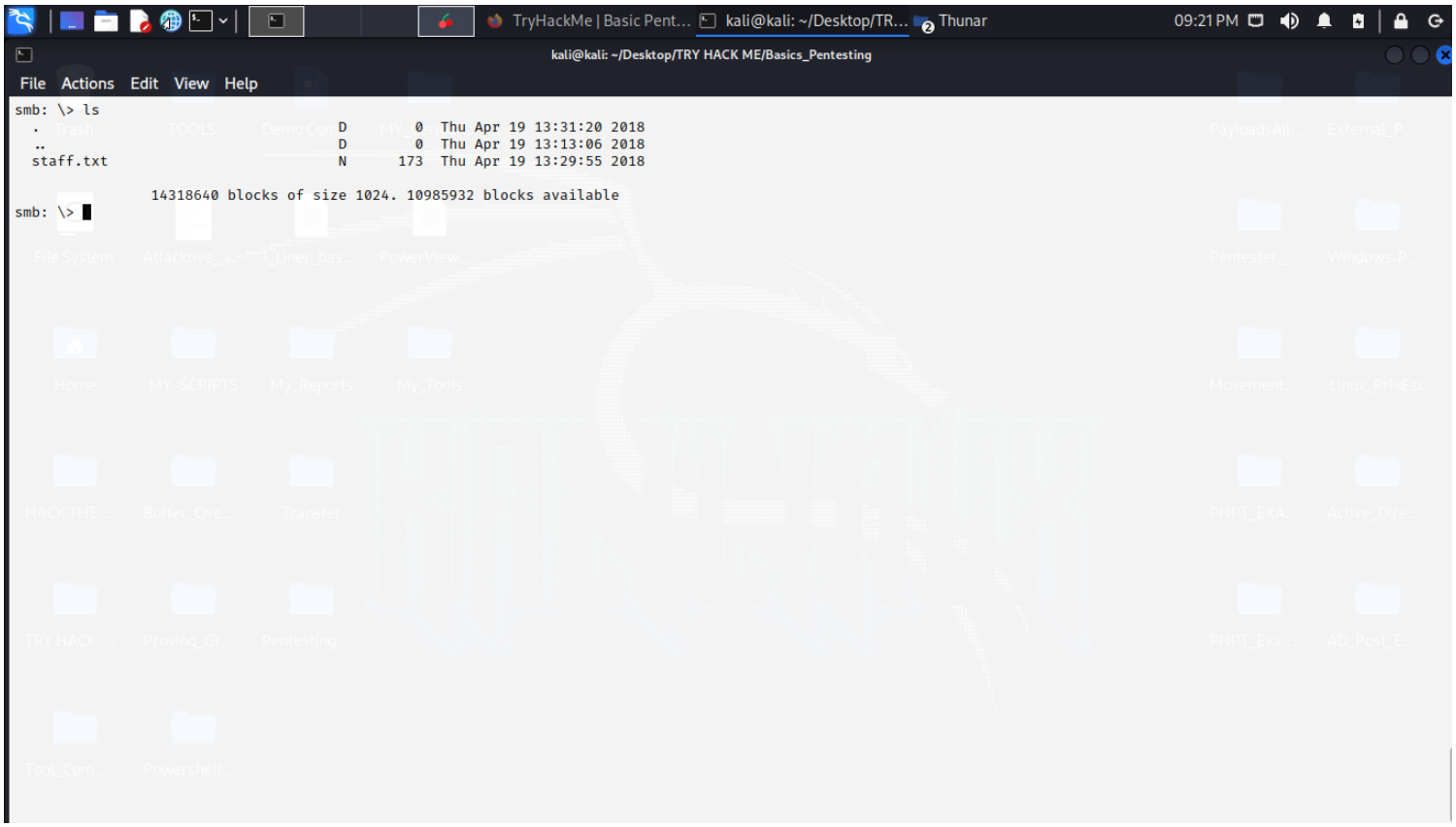
SMB



Notes

I use smbclient -L ////10.10.97.17/ to check and see if we have anonymous login. We do so lets login. I will try to login to the anonymous share.

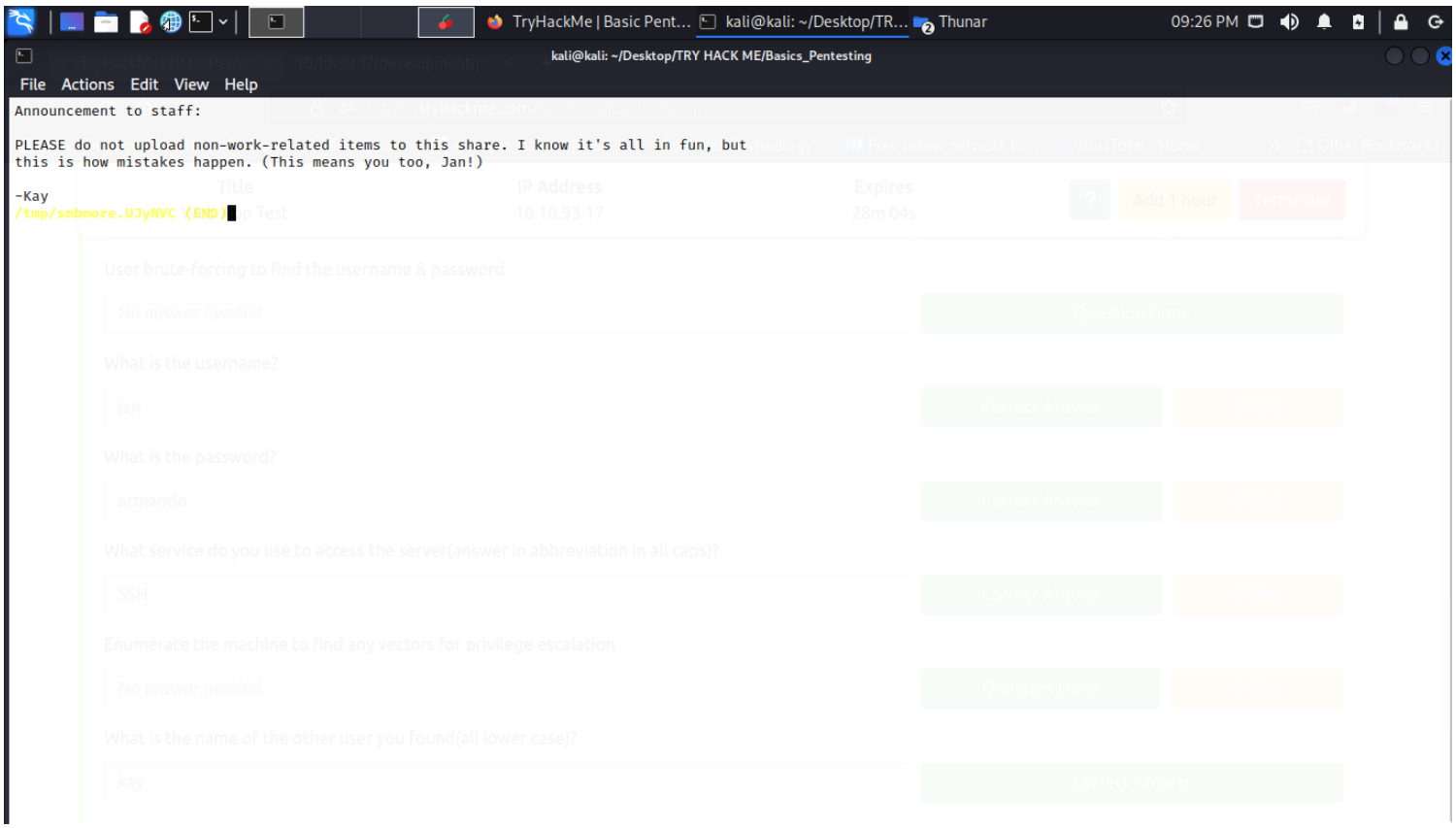
SMB_Anonymous_Login



Notes

We see a staff.txt file.

Staff.txt



Notes

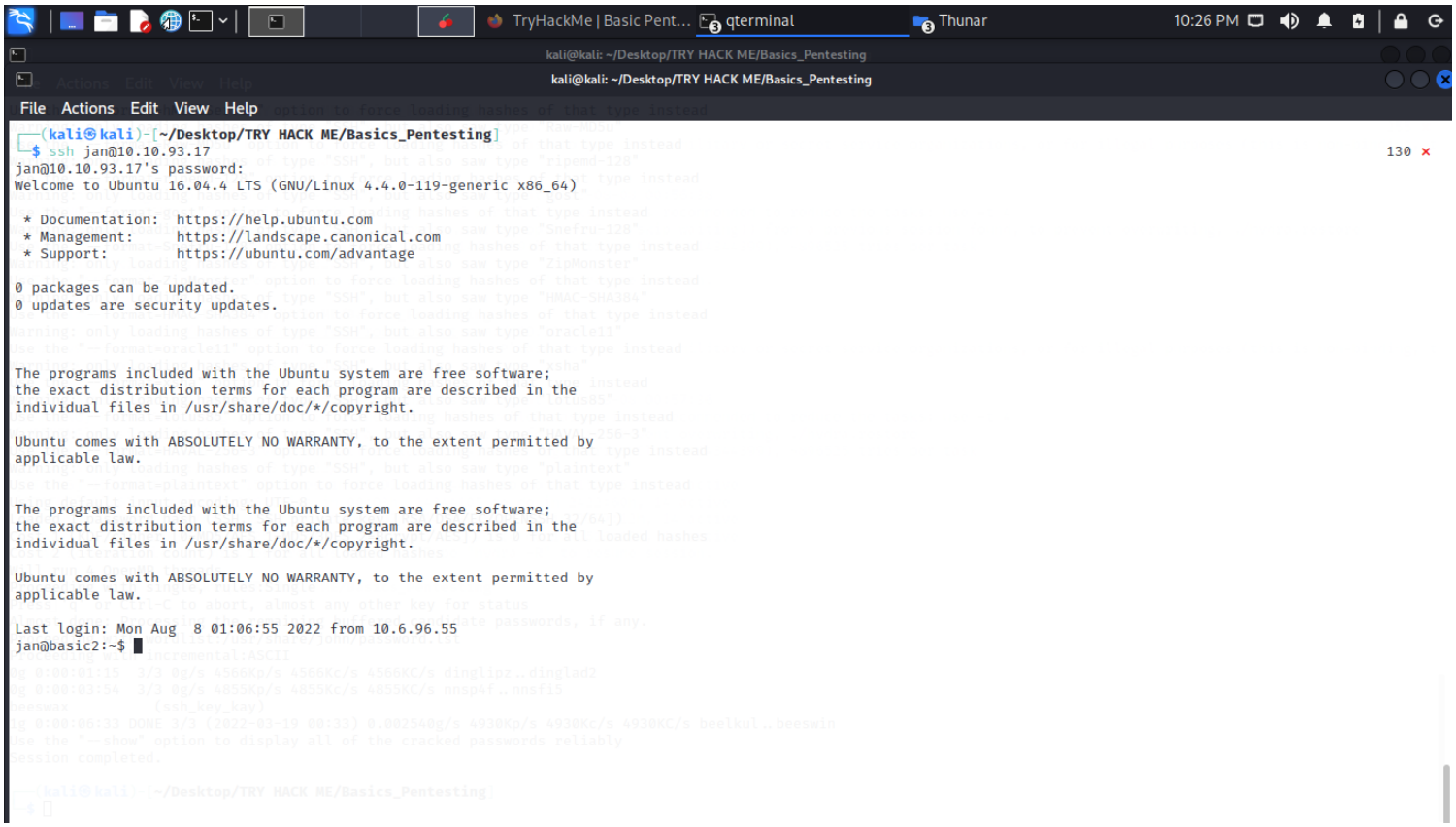
We find 2 usernames kay and jan. We also can see that they have the ability to upload files. With this information that we have gathered, we can try to bruteforce ssh.

BruteForce_SSH

Notes

I used hydra to crack the password for jan, I tried to crack kay but had no success.
so logged into ssh with jan.

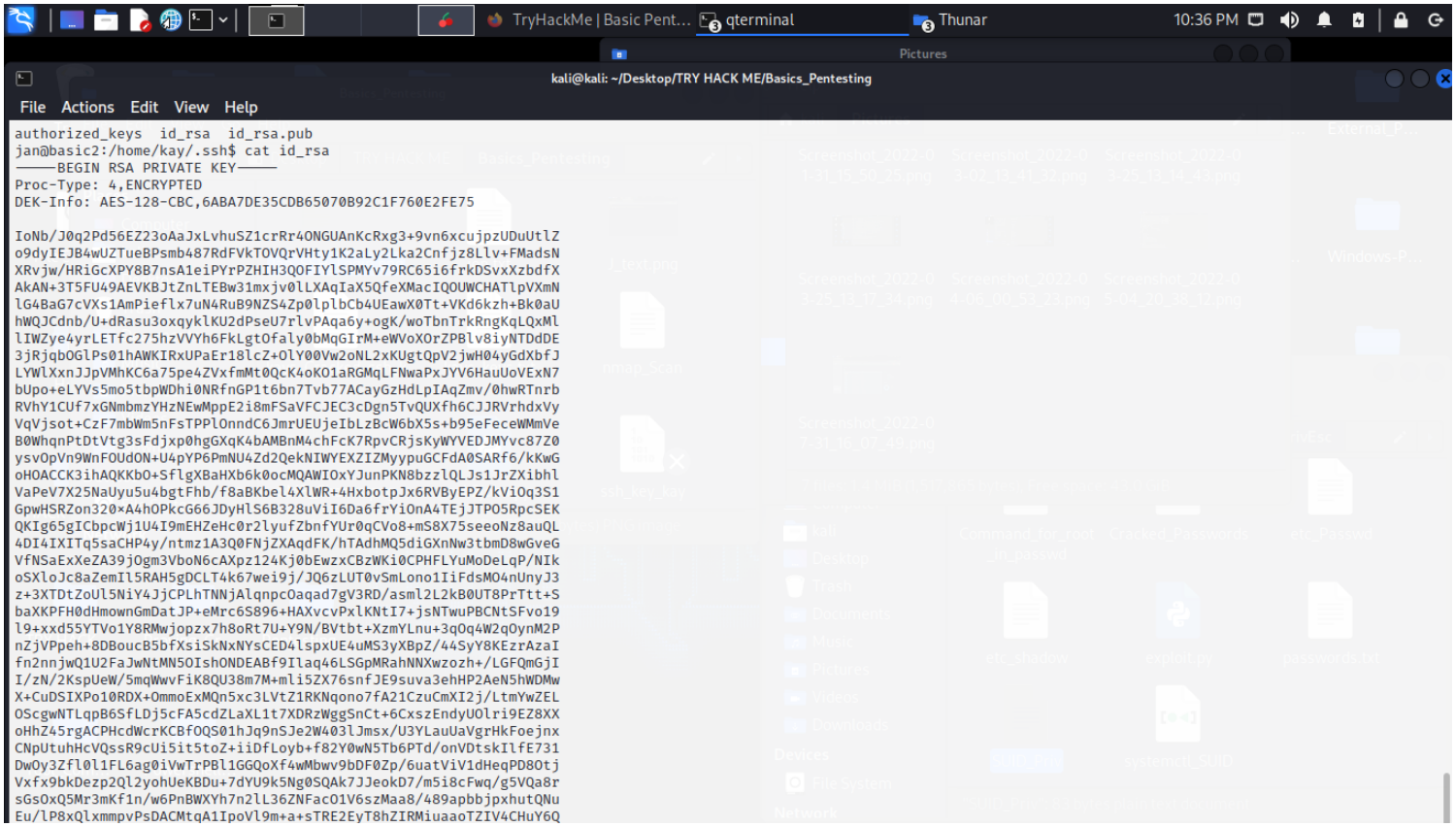
SSH_Shell_jan



Notes

I searched jans directories but didn't find much.I went to kay directory and did ls -la and found id_rsa key.

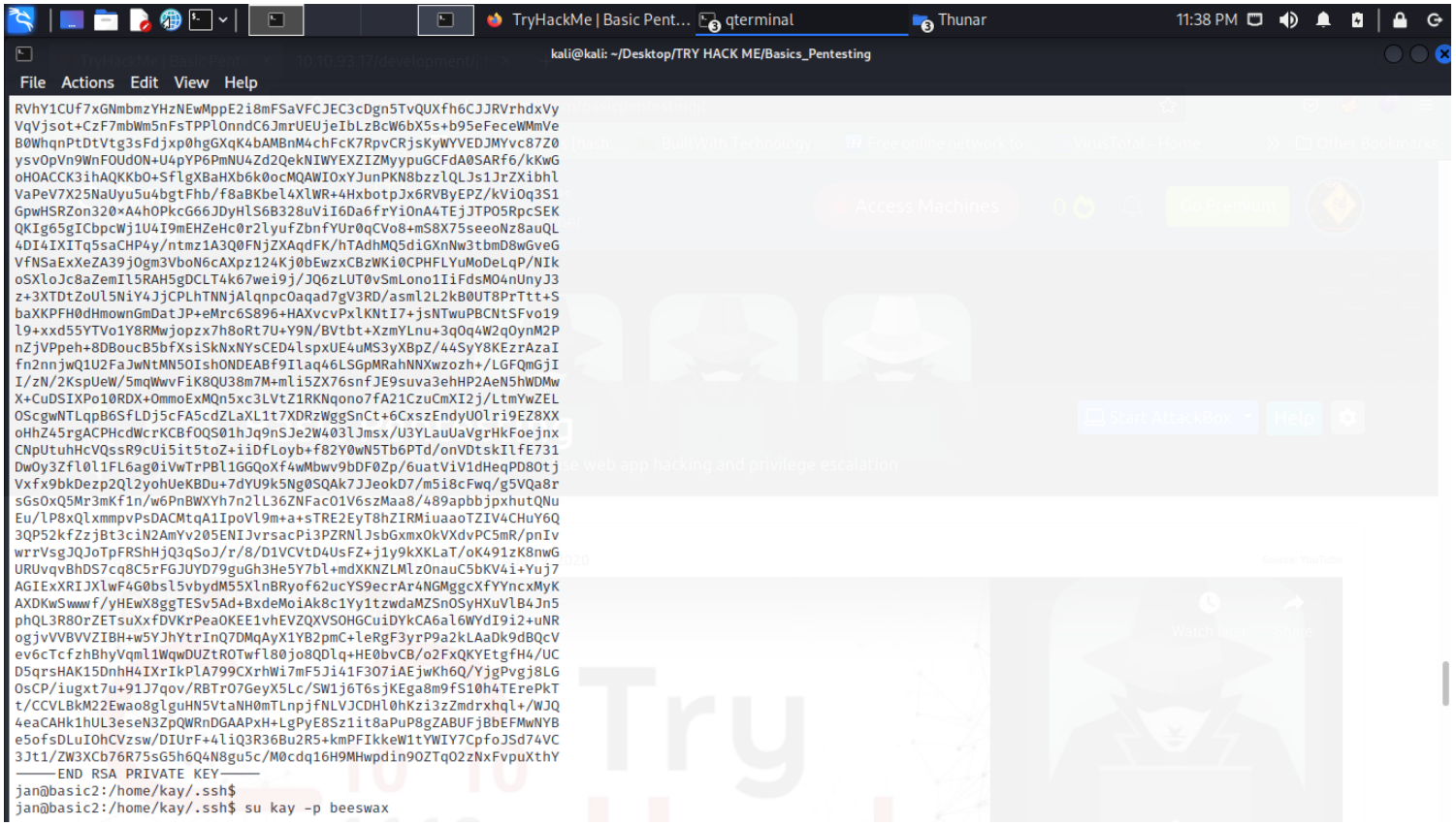
kay_id_rsa_key



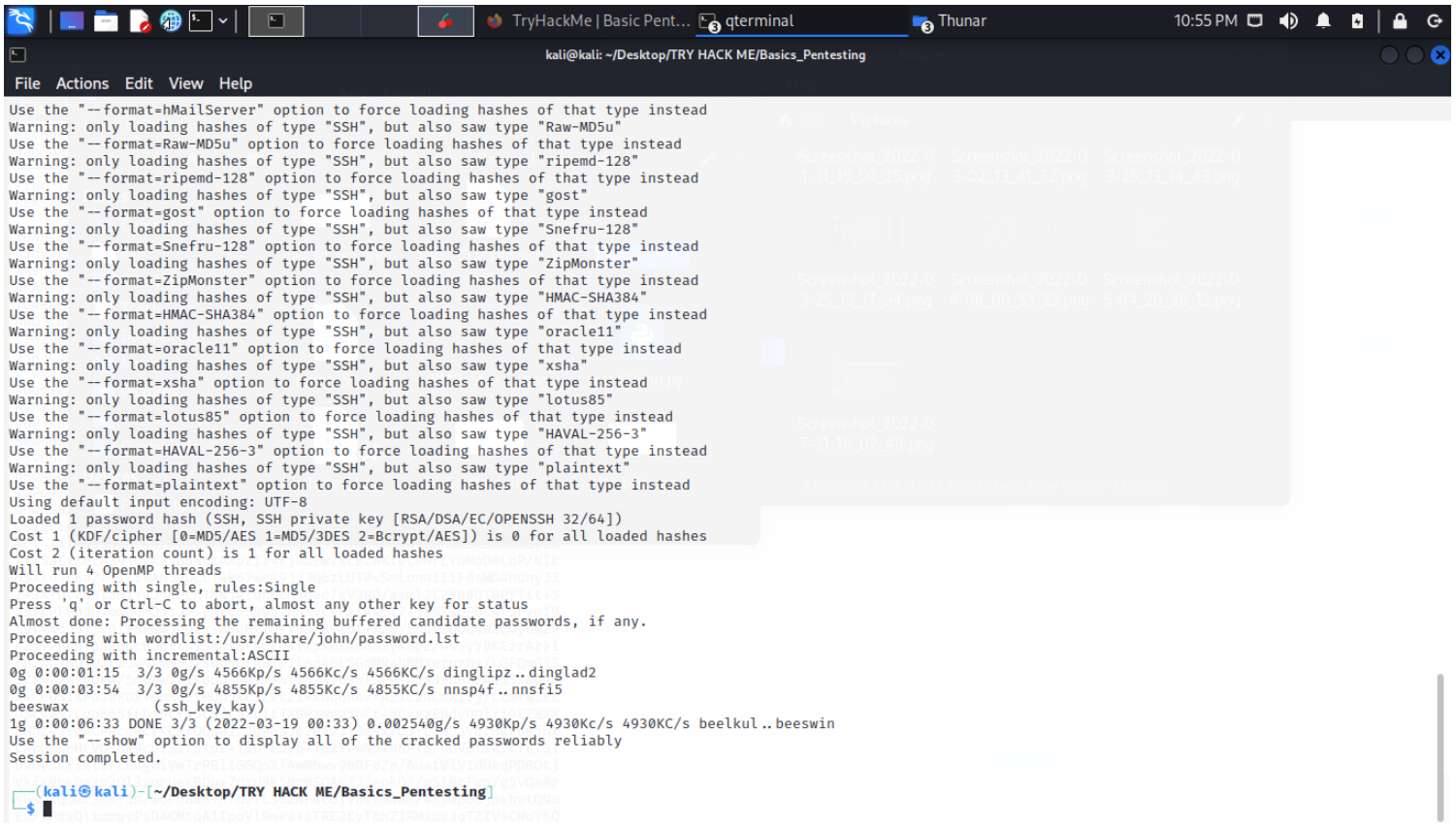
Notes

We can copy this key and create a file called id_rsa then do ssh2john id_rsa > kays_key
This will make it to where you can use john the ripper and crack the key.
The key was too big for the screen shot lol.

Second_half_of_Key



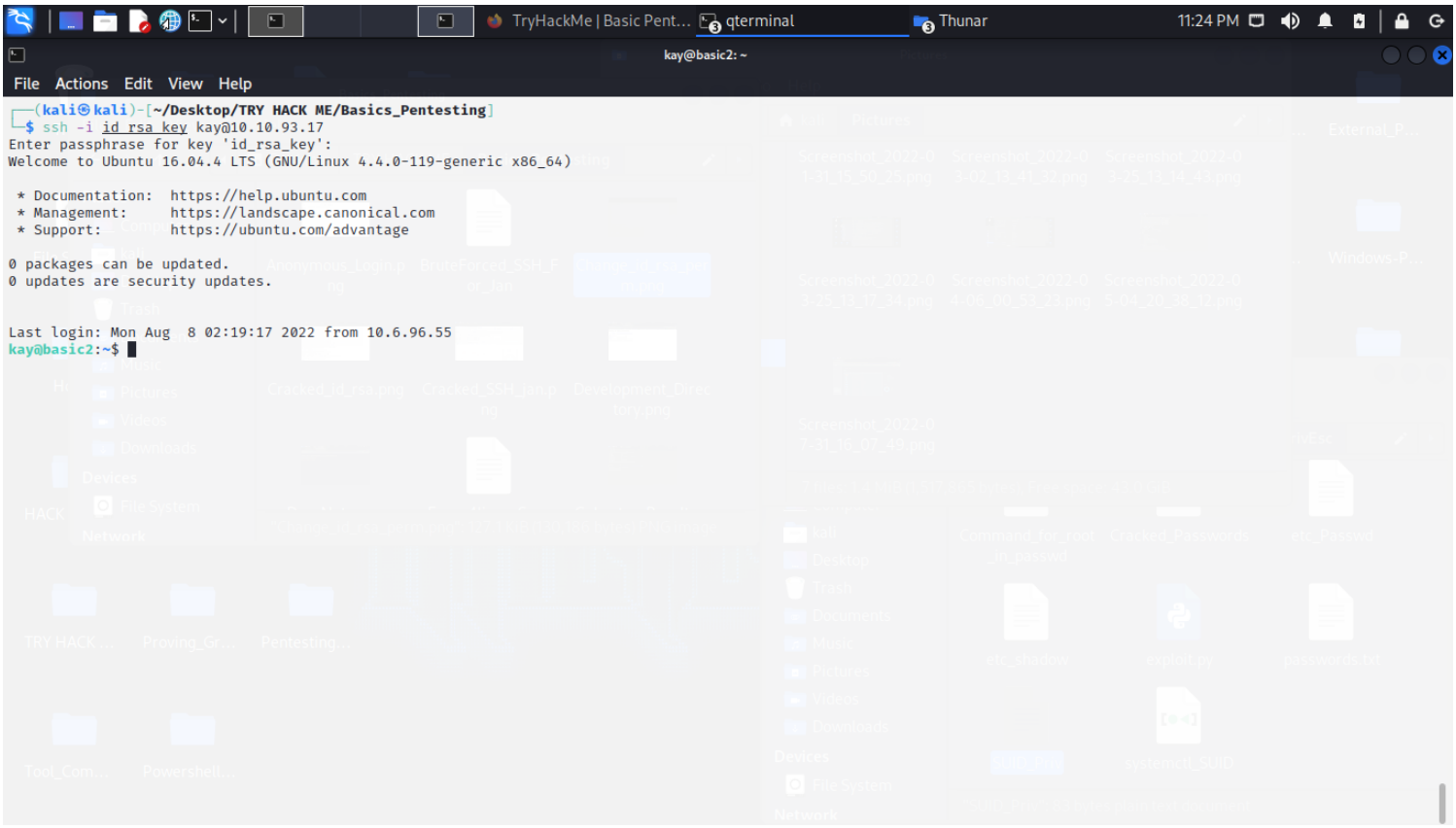
John



Notes

Use john --w=/usr/share/wordlist/rockyou.txt
this will crack the password. Lets login to ssh with kays password.

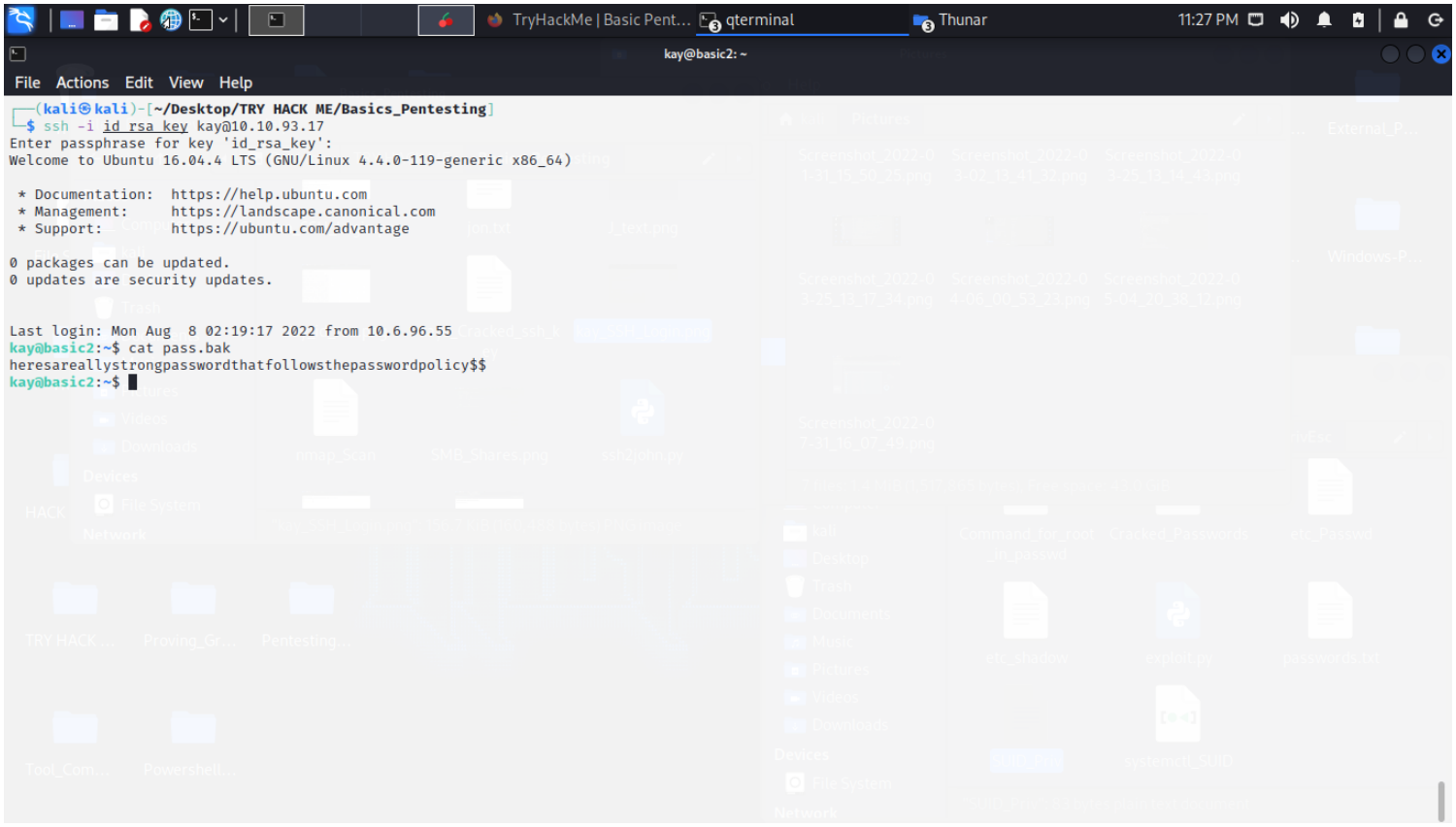
Kay_SSH_Login



Notes

Note make sure to change permissions on the id_rsa file to 644
chmod 644 id_rsa

Final_Flag



Notes

cat pass.bak to get final flag.
Thank you I hope you enjoyed.