PSP0201

Week 2

Writeup

Group Name: ikun no 1

Members

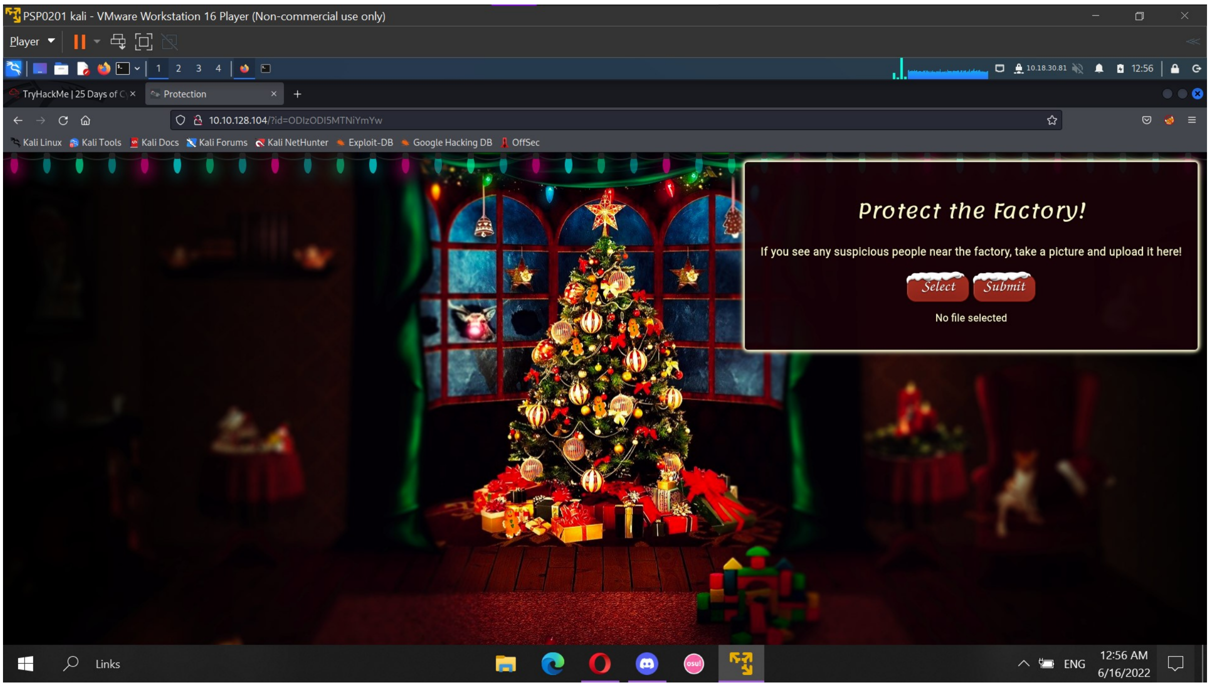
ID	Name	Role
1211102058	Chu Liang Chern	Leader
1211101401	Chong Jii Hong	Member
1211103206	Ng Kai Keat	Member
1211103095	Siddiq Ferhad Bin Khairil Anual	Member

DAY 2: Web Exploitation The Elf Strike Back!

Tool used: kali Linux, Firefox

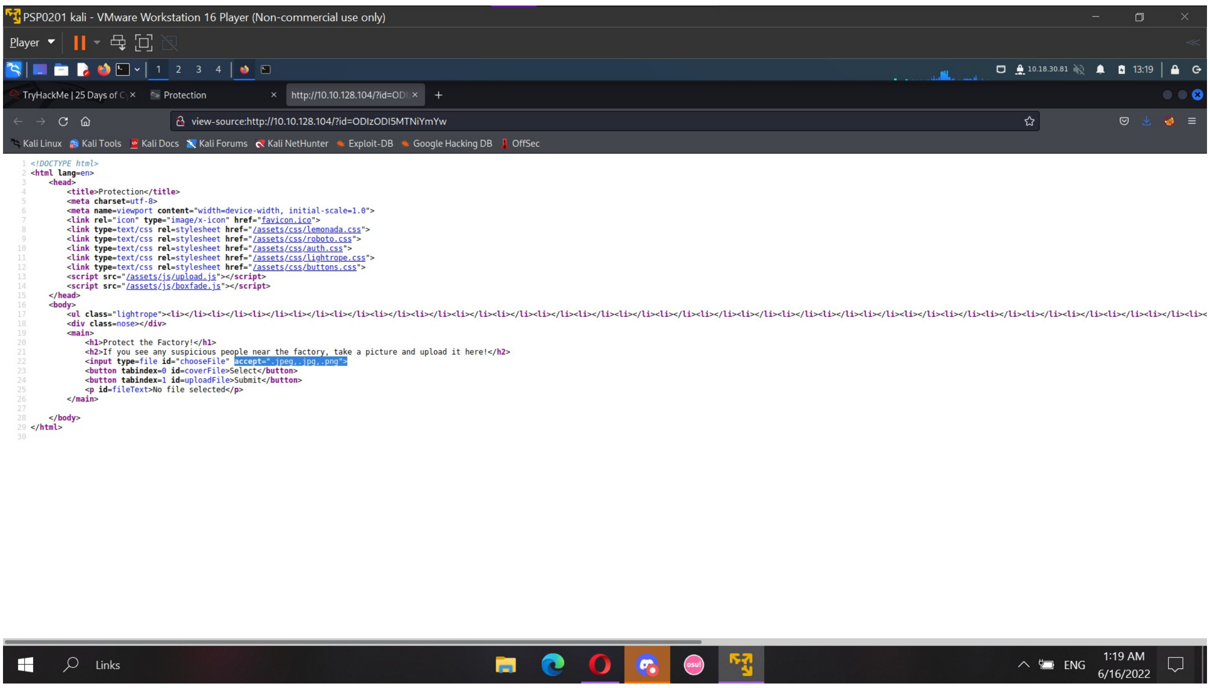
Solution/Walkthrough:

Q1



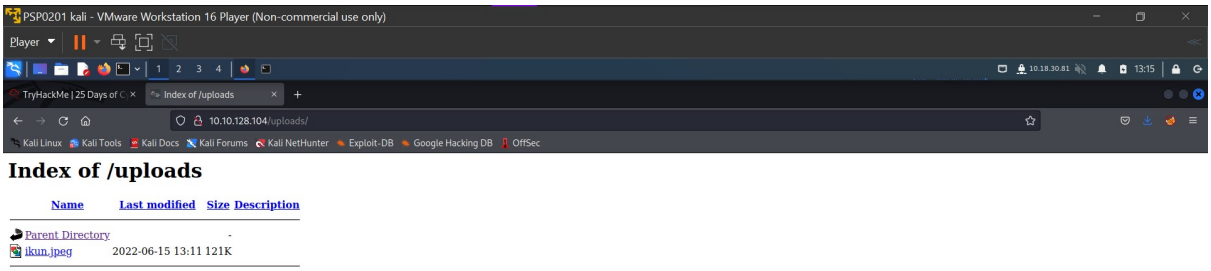
Add the id given in THM behind the ip address with the format ?id=<id given>

Q2



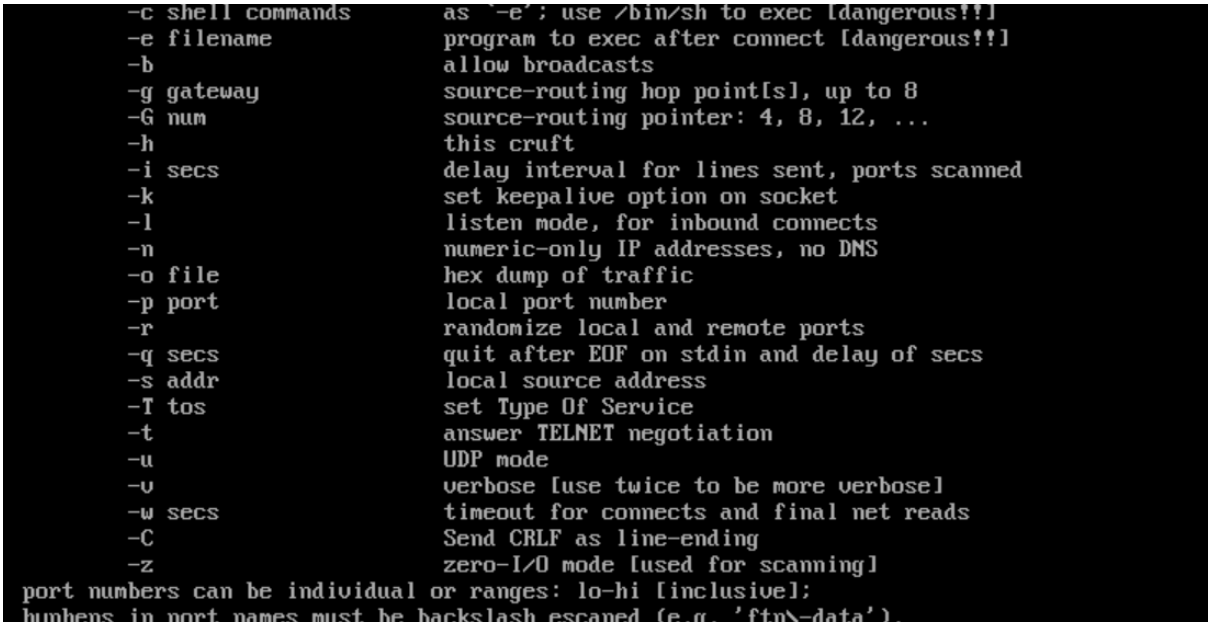
Right click on the page and choose the page source button. From the input type line, we can know that the site only accepts jpeg, jpg and png files only, which is the image file format.

Q3



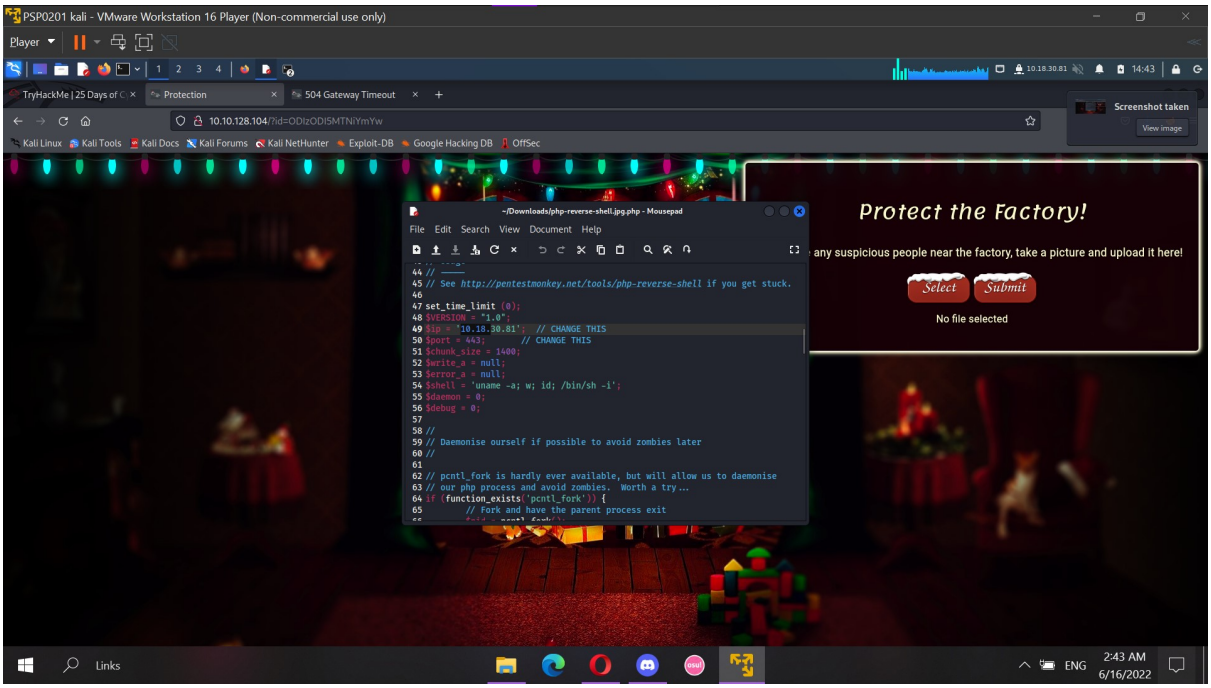
The directory can be found with a tool such as Gobuster, or by checking each of the common directories from the dossier. In this case, I am using the second method and the directory is bypassed with the subdirectory of /uploads/

Q4

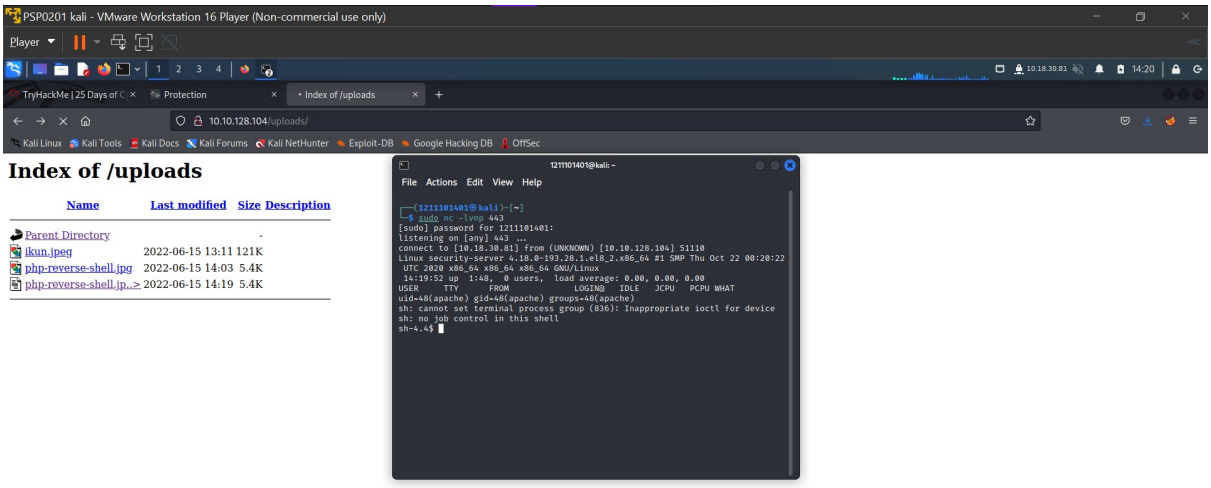


Run nc -h in the terminal and all the commands available in the netcat will be shown.

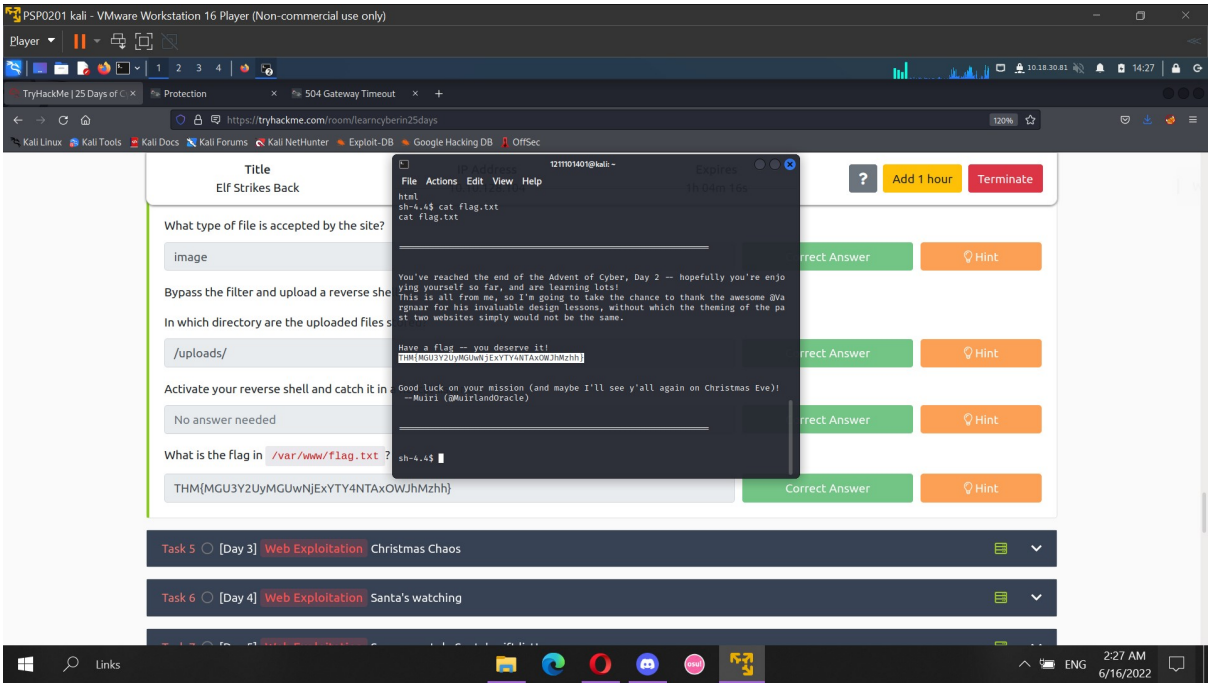
Q5



Download reverse shell. Edit the ip address into our own ip and the port to a common port such as 443 as this kind of port usually is not filtered by the firewalls. Save the file and change the file name into <php-reverse-shell.jpg.php>.



Upload the file to the site and start listening by typing in the command sudo nc -lvnp 443 in the terminal. Wait until the listener receives the shell successfully.



After finishing the task, the flag will appear. Catch the flag.