Knock knock knocking on shuttles door

1> Let me in

We found a web server at 10.6.0.2... you may need the wordlist attached to this challenge.

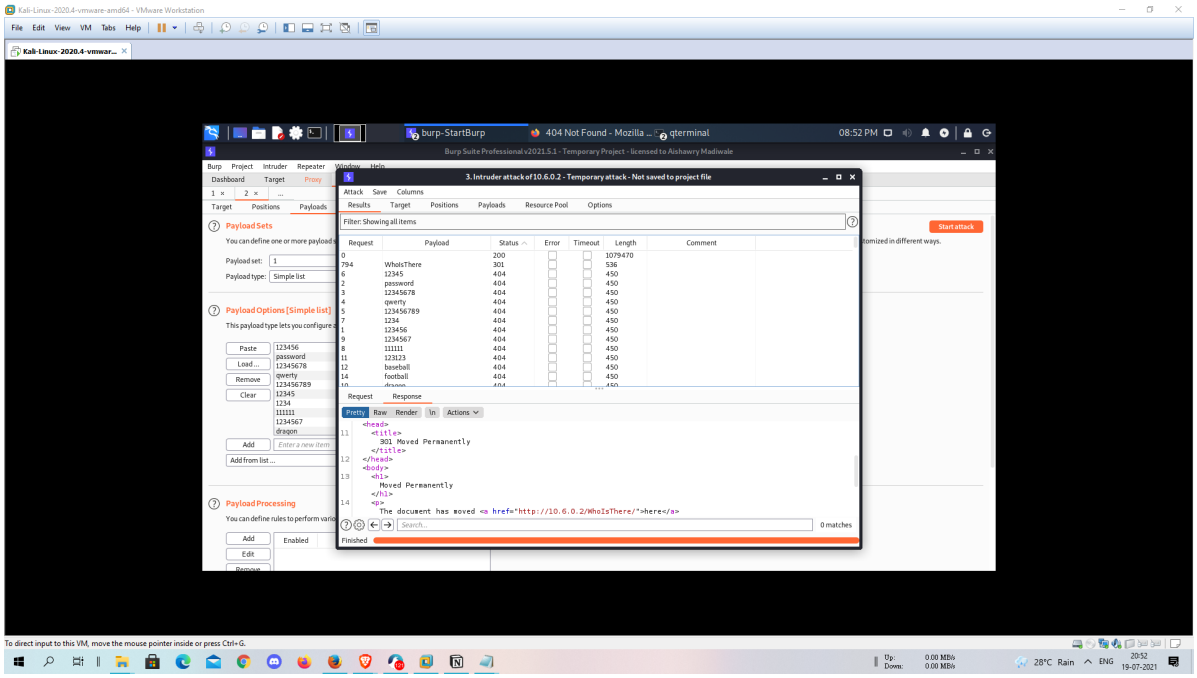
which doors should I knock? Note: enter them comma (,) separated in the ordered you found them example ctf{num1,num2,num3,num4}

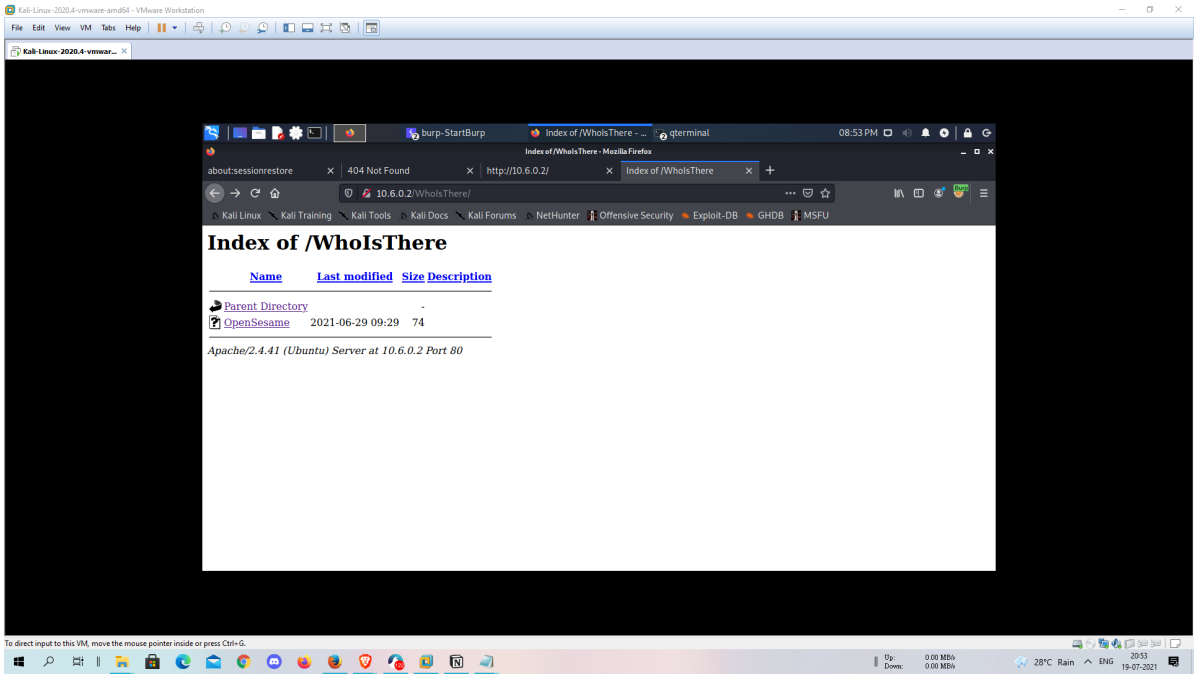
Points [75 points]

- The challenge has also provided us with a wordlist as they have suggested I tried the wordlist on the ip address was able to findout an endpoint WhoIsThere which

returns 301 status.

```
https://developer.mozilla.org/en-US/docs/Web/HTTP/Status/301
```

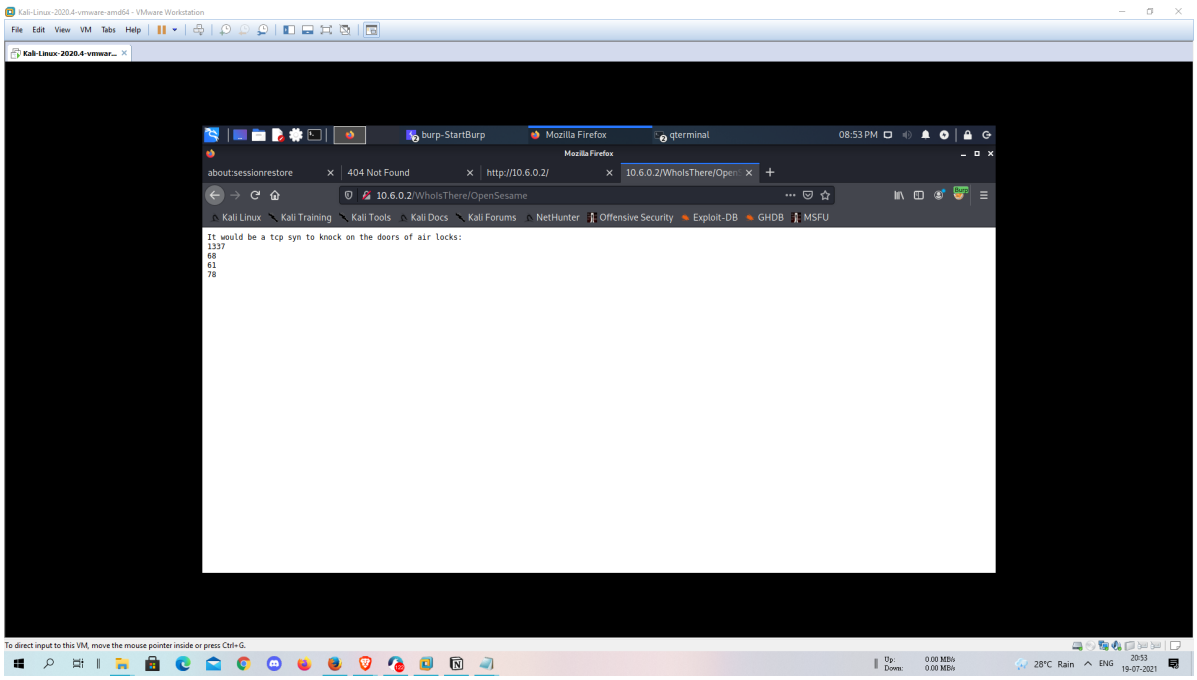




- On visiting the webpage it had an index directory and when visited the first OpenSesame directory, it told us that we have to perform TCP syn knock on the ports in the given order. After some research found out that this can be done by knock tool and the command to do is
- Knock 10.0.6.2 1337 68 61 78 && nmap 10.0.6.2

This command gave me that we have a 2021 port open and which we will use in the second part, since the ports worked as knocking on them opens 2021 port which was closed earlier, this might be the correct order so the order is correct and this is the first flag

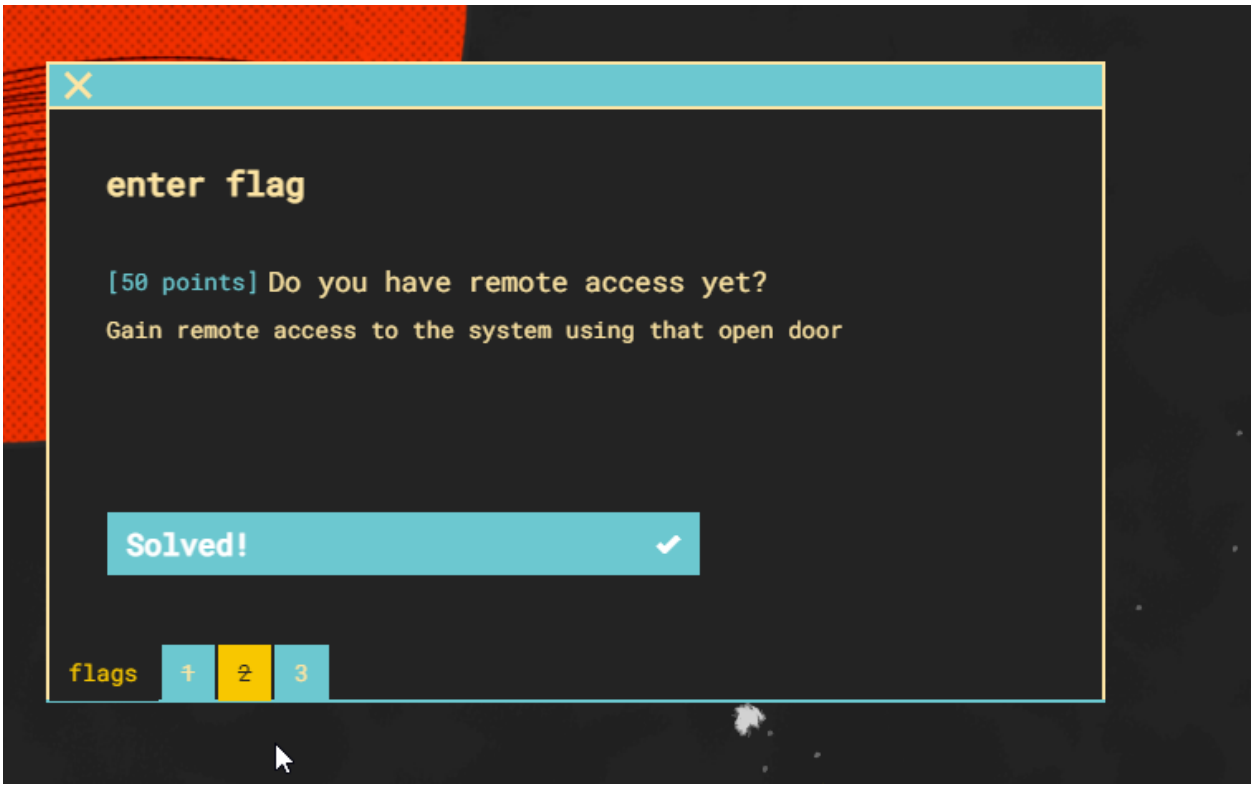
- Flag :- ctf{1337,68,61,78}



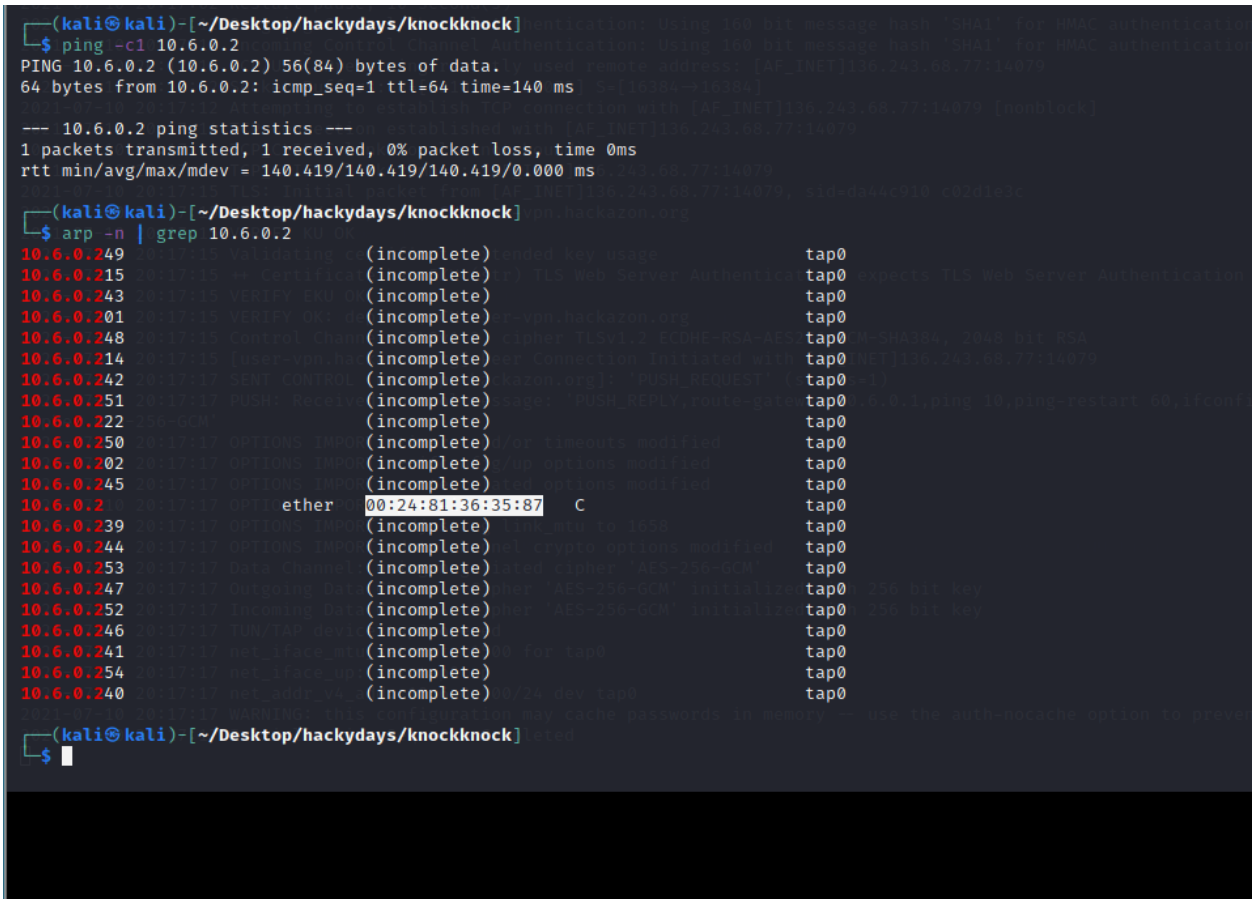
2> Do you have remote access yet?

Gain remote access to the system using that open door

Point [50 points]



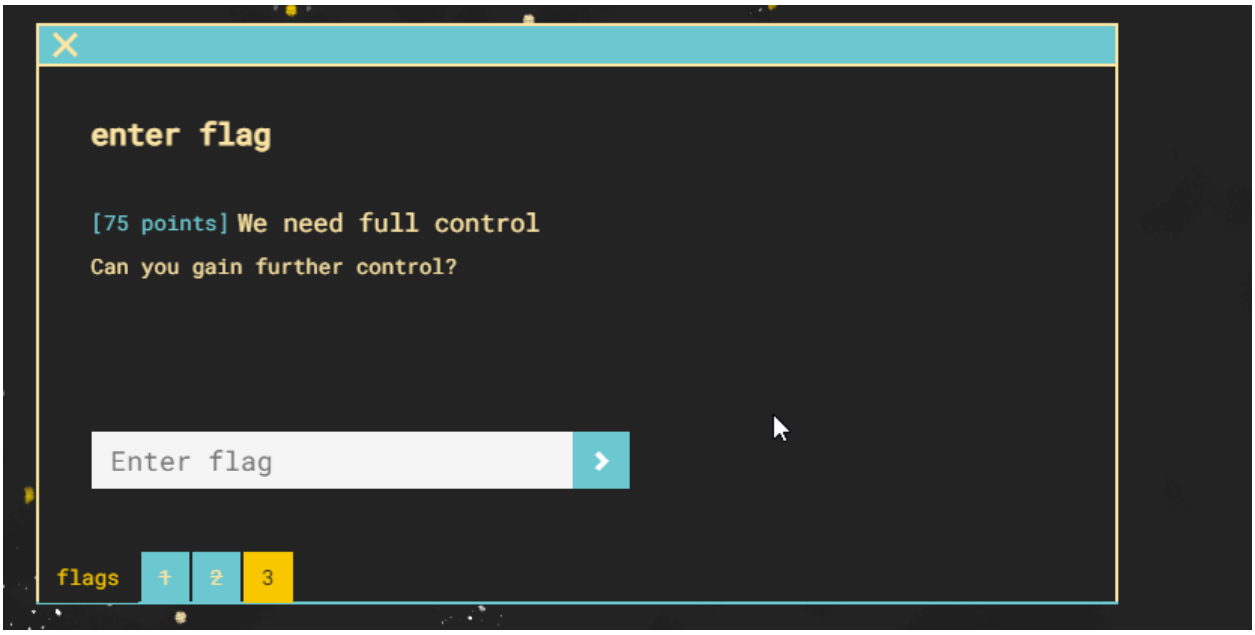
- In this challenge, we have to remotely connect to the machine using the 2021 port that we have found out in previous challenge telnet to the machine ip and port no get's me shell access to the machine and the flag.txt on the desktop which has the flag for the second challenge
- Flag:- ctf{we_have_lift_off}



3> We need full control

Can you gain further control?

Point [75 points]



mac address - 00:24:81:36:35:87

```
https://cd6629.gitbook.io/ctfwriteups/linux-privesc/knockknock
```

```
https://d00mfist.gitbooks.io/ctf/content/port_knocking.html
```

```
https://www.exploit-db.com/exploits/49754
```