


Space Pirate: Entrypoint

Event	Cyber Apocalypse 2022
Tags	pwn
Author	 Jun Peng Tan

Challenge Description



Challenge Walkthrough

In this challenge, we need to start a docker and it will provide us an IP address and port number to connect. To run it, use the netcat command.

```
$ nc [ipaddr] [port]
```

Then it will show us the authentication system and two option for us to choose.

```
(arfuu@kali) - [~]  
$ nc 157.245.33.77 31915  
  
Authentication System  
  
1. Scan card 🇲🇪  
2. Insert password 🔑
```

Move on to the zip file given, it provided 2 files and 1 directory for us. Lets output the flag.txt and it out the fake flag.

```
(arfuu@kali) - [~/Downloads/htb(CyberApocalypse2022)/Pwn/challenge]  
$ ls  
flag.txt  glibc  sp_entrypoint  
(arfuu@kali) - [~/Downloads/htb(CyberApocalypse2022)/Pwn/challenge]  
$ cat flag.txt  
HTB{f4k3_fl4g_4_t35t1ng}
```

Then, use strings command to crosscheck all the strings contains in the sp_entrypoint file. We can see there is a "sus" strings after the "Insert password:" function.

```
$ strings sp_entrypoint
```

```

%s[+] Door opened, you can proceed with the passphrase:
cat flag*
[*] Insert password:
0nlyTh30r1g1n4lCr3wM3mb3r5C4nP455
[1;5;31m
%s[-] Invalid password! Intruder detected!
1. Scan card [red] you can proceed with the passphrase:
2. Insert password
[!] Scanning card.. Something is wrong!
Insert card's serial number: 0P455
Your card is:
%s[-] Invalid option! Intruder detected!
%s[-] Invalid ID! Intruder detected!
;*3$"

```

Insert the strings as the password and we got the flag ! In this case, we need to also include the "" in the strings and this issues had caused our teams for 2 hours to solve it. 😊

```
"0nlyTh30r1g1n4lCr3wM3mb3r5C4nP455"
```

Flag

That's the flag !

```
HTB{th3_g4t35_4r3_0p3n!}
```

```
(arfuu@kali) - [~]  
$ nc 157.245.33.77 31915
```

Authentication System



```
1. Scan card 🇪🇸  
2. Insert password 🔑  
> 2  
[*] Insert password: "0nlyTh30r1g1n4lCr3wM3mb3r5C4nP455"  
  
[+] Door opened, you can proceed with the passphrase: HTB{th3_g4t35_4r3_0p3n!}
```