

Day 1 - A Christmas Crisis

Scenario

"The Best Festival Company's brand new OpenVPN server has been hacked. This is a crisis!

The attacker has damaged various aspects of the company infrastructure -- including using the Christmas Control Centre to shut off the assembly line!

It's only 24 days until Christmas, and that line has to be operational or there won't be any presents! You have to hack your way back into Santa's account (blast that hacker changing the password!) and getting the assembly line up and running again, or Christmas will be ruined!"

After giving you the assignment, McSkidy hands you the following dossier of important information for the task. Before reading it, you **press the big green "Deploy" button to start the Control Centre, as well as the **"Start AttackBox" button at the top of the page** **

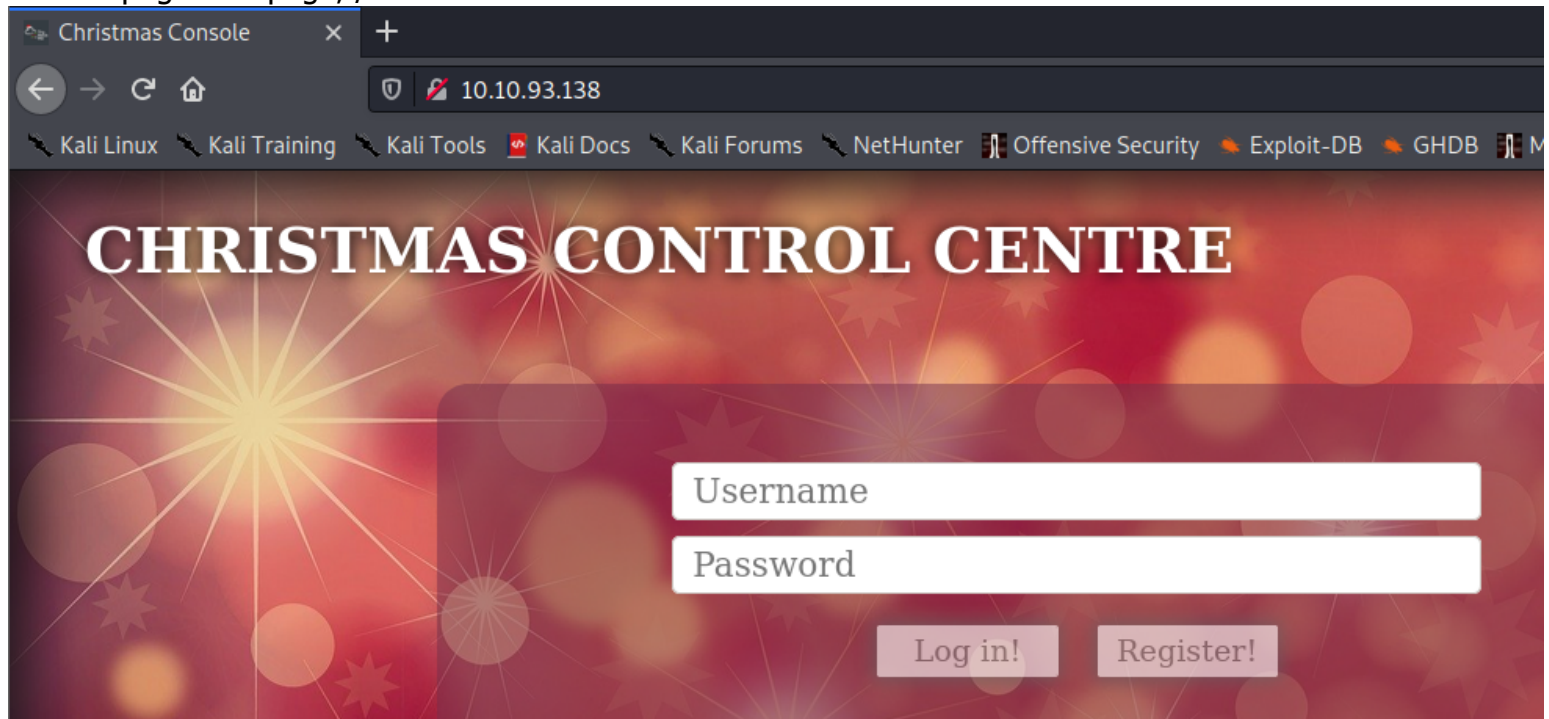
[Watch JohnHammonds video on solving this task!](#)

Dossier compiled by [@MuirlandOracle](#)

*Having read the lengthy dossier, you get ready to hack your way back into Santa's Christmas Control Centre! You **enter the IP address at the top of the screen into your browser search bar** and press enter to load the page.*

Note: Remember that machines can take up to five minutes to boot up fully!

the webpage root page, /



Christmas Console x +

← → ↻ 🏠 10.10.93.138

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB M

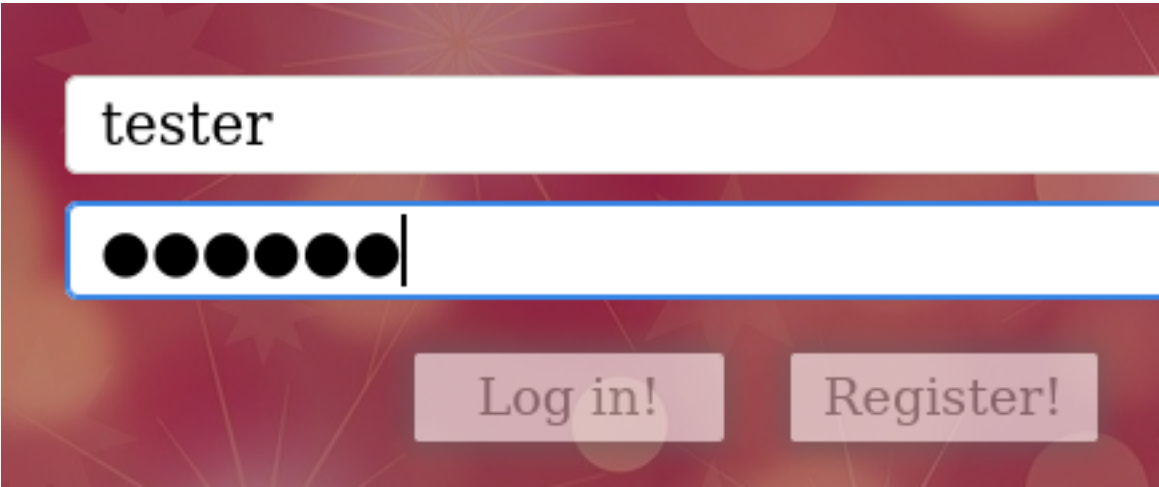
CHRISTMAS CONTROL CENTRE

Username

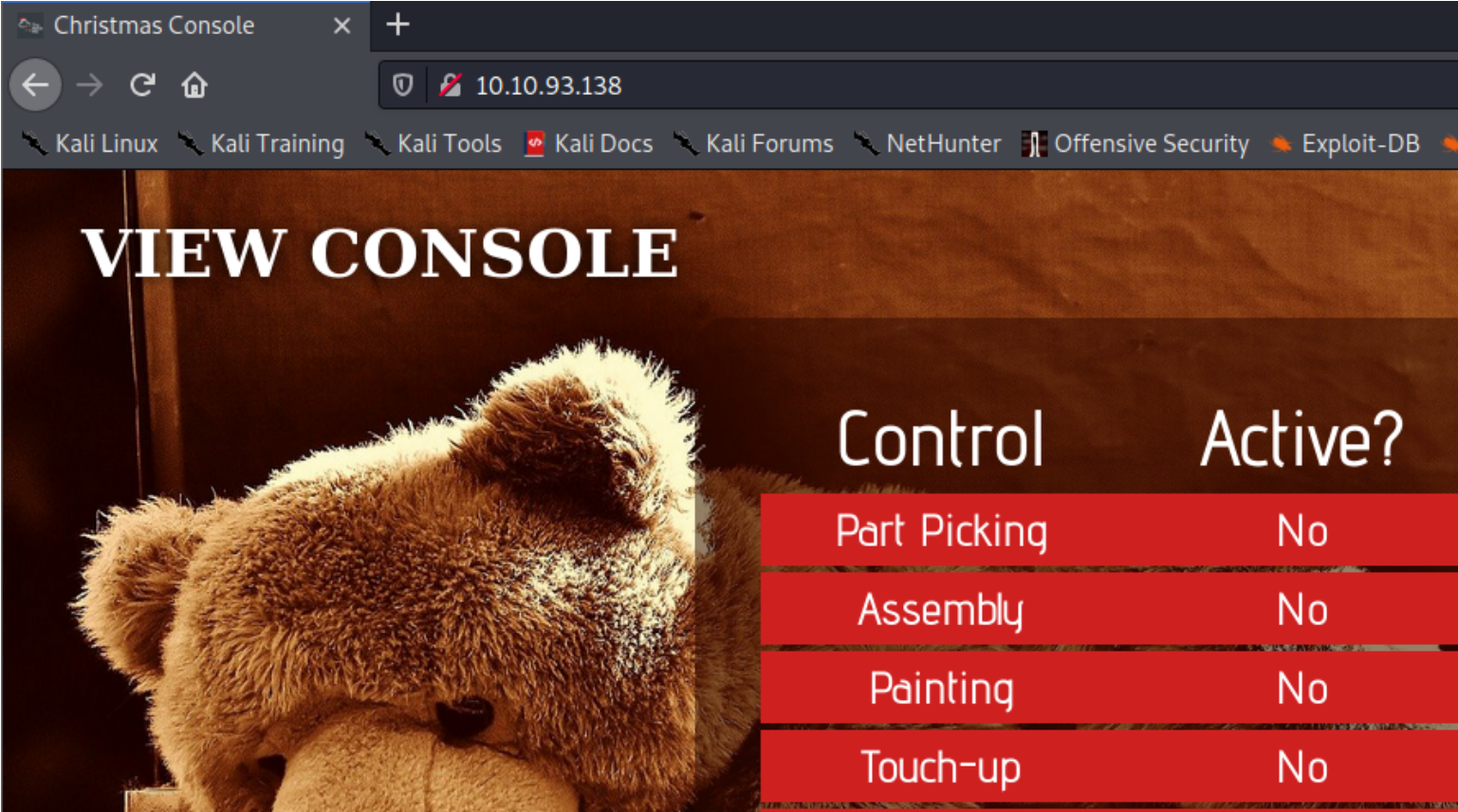
Password

Log in! Register!

register an account for christmas control centre



login into the account that created



check the cookies & found auth cookie
//the cookie seems to be encoded into hex code

Name	Value	Domain	Path	Expires / Max-Age	Size
auth	7b22636f6d70616e79223a2254686520...	10.10.139.32	/	Session	124

Question: What is the name of the cookie used for authentication?
-auth

Question: In what format is the value of this cookie encoded?
-hexadecimal

use hex to ascii converter & voila we found it seems like json format

//company and username key field
//the username is the tester user that we logon just now

```
7b22636f6d70616e79223a22546865204265737420466573746976616c2  
0436f6d70616e79222c2022757365726e616d65223a2274657374657222  
7d
```

Character encoding

ASCII

↻ Convert

✕ Reset

↑↓ Swap

```
{"company":"The Best Festival Company",  
"username":"tester"}
```

Question: Having decoded the cookie, what format is the data stored in?
-json

now let's change the username to 'santa' & convert it to hexadecimal

```
{"company":"The Best Festival Company", "username":"santa"}
```

Character encoding

ASCII

Output delimiter string (optional)

None

Convert

Reset

Swap

```
7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2273616e7461227d
```

Question: What is the value of Santa's cookie? (answer accept uppercase 'S' hex but the cookies only works for 's' hex to access santa's account)

-7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2273616e7461227d

-7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2273616e7461227d

let's change the auth cookie value to santa's cookie

Name	Value	Domain
auth	7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c20...	10.1...

refresh the page & we're in santa's account

CONTROL CONSOLE



re-activate all the controls that the threat actor disabled & we got our flag!

