Day 1 - The search

Welcome to the River Security XMas Challenge (RSXC)! RSXC operates with the following flag format for most challenges 'RSXC{flag}'. If another flag format is used, the challenge text will mention this.

In this first challenge we have managed to forget which port we are listening on. Could you please find the port listening for traffic? We know it's in the range 30 000-31 000.

Write-Up

As the text says there is a port open in the range 30000-31000 range. The information do not tell which server, but as the rules states "Everything for the CTF will be on the domain `rsxc.no`" we will use `rsxc.no` as the server for the hidden port. We could find the port by trying all of these ports manually, or create our own tool. But there is a tool for this... NMAP!

We want to test or scan all the ports in the range and report back those that are open for the host, rsxc.no

```
$ nmap -p30000-31000 --open rsxc.no
```

Nmap will give us the result

```
PORT      STATE SERVICE
30780/tcp open  unknown
```

We now know that one port, 30780, is open... So now what?

As the port is open we could try connecting to it and we have several options to choose from

```
$ nc rsxc.no 30780
$ firefox rsxc.no:30780
```

Both methods gives us what we are looking for, the FLAG....

```
RSXC{Congrats!You_found_the_secret_port_I_was_trying_to_hide!}
```

The Flag

RSXC{Congrats!You_found_the_secret_port_I_was_trying_to_hide!}