

Connecting to the CTF Server

14-735

Step 1 Install Firefox:

Download Firefox from: <https://www.mozilla.org/firefox>

Below directions based on: <https://www.digitalocean.com/community/tutorials/how-to-route-web-traffic-securely-without-a-vpn-using-a-socks-tunnel>

Step 2 — Setting Up the Tunnel

Open a terminal program on your computer. On Mac OS X, this is Terminal in Applications > Utilities.

Set up the tunnel with this command:

- `ssh -D 8123 -C -q -N ctfssocks@ctf.martincarlisle.com`

Explanation of arguments

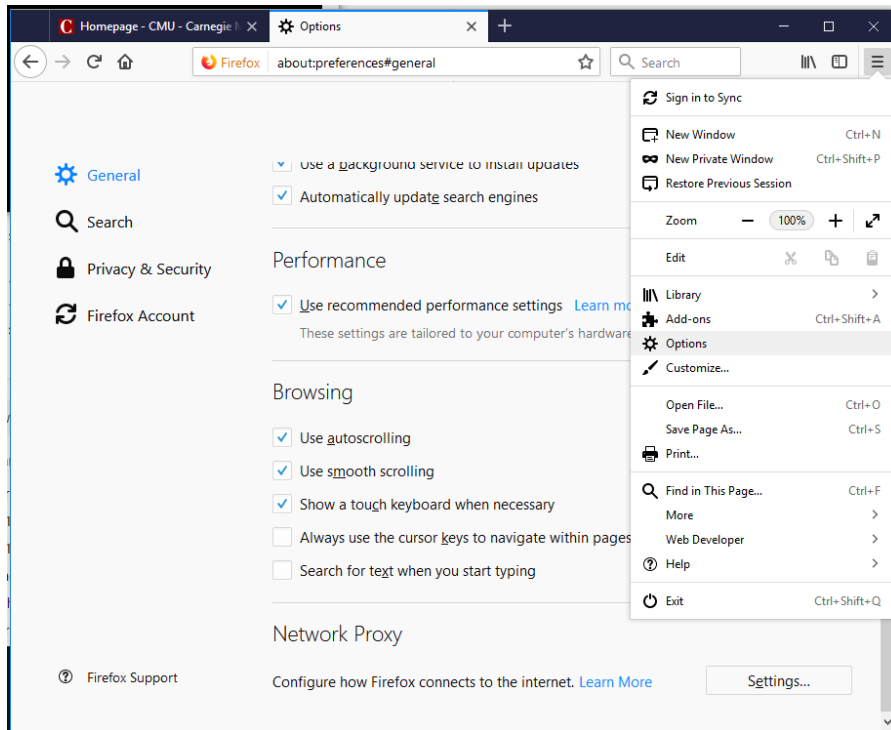
- `-D`: Tells SSH that we want a SOCKS tunnel on the specified port number (you can choose a number between 1025-65536)
- `-C`: Compresses the data before sending it
- `-q`: Uses quiet mode
- `-N`: Tells SSH that no command will be sent once the tunnel is up

Once you enter the command, you'll be asked for the password: XXXX! (include the !)

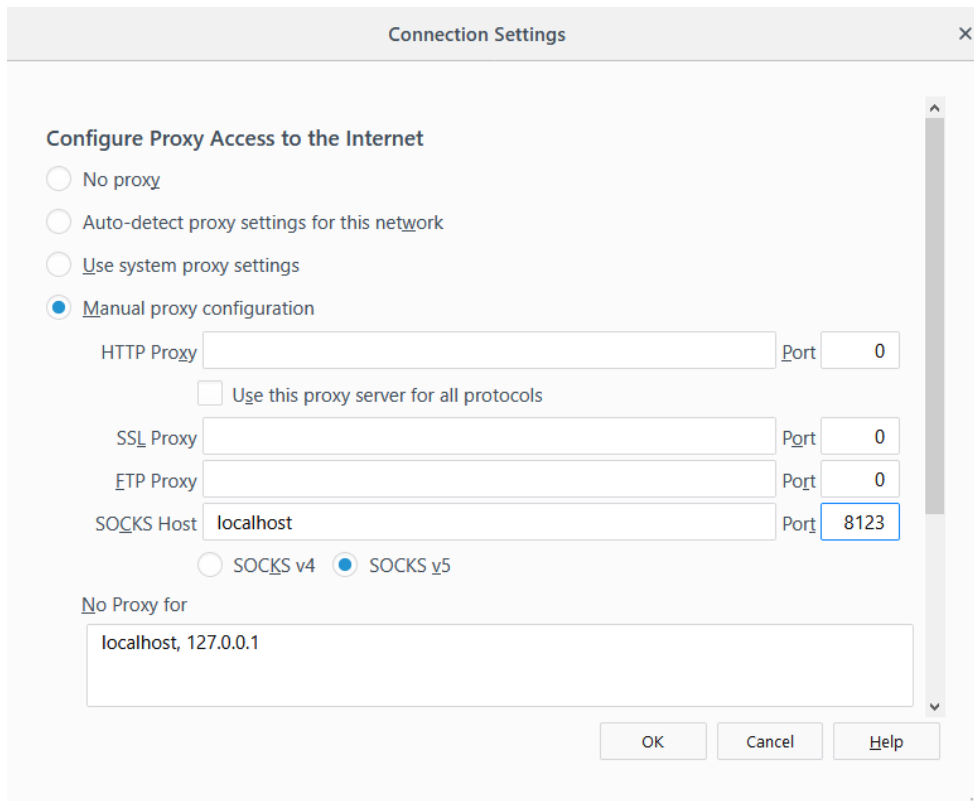
Then, it will look like the terminal has locked up-- that's normal. Just leave that window open. Hit Ctrl-C to exit when you are finished, or just close this window.

Step 3 — Connect to the CTF Server

In Firefox, select Options from the menu, then scroll down to Network Proxy and push the Settings button:



Configure the manual proxy with SOCKS Host localhost and port 8123 and push OK



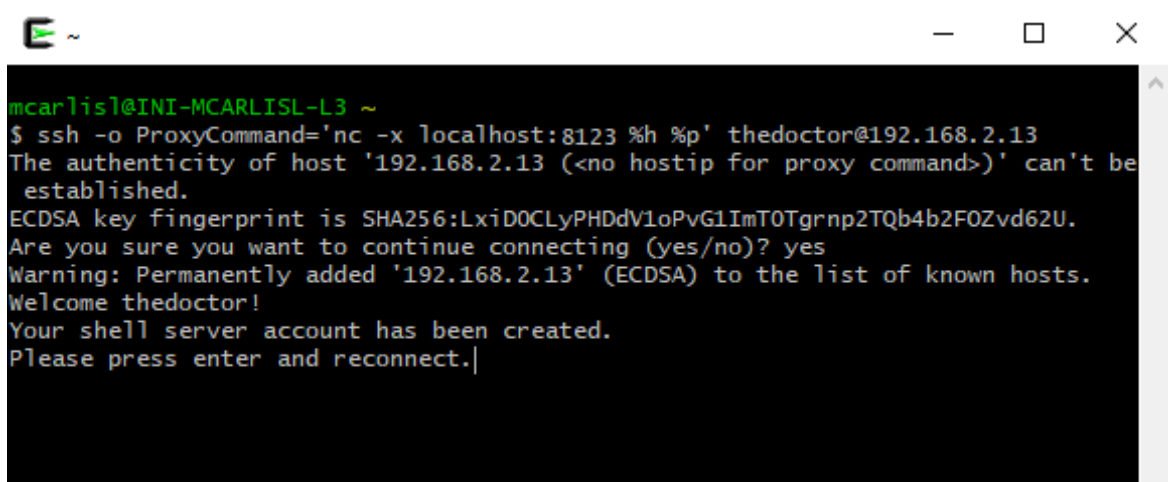
Point the browser to <http://192.168.2.82/> and register an account. **NOTE: your username and score will be public. For privacy, you should select a username that is not personally identifiable.**

Step 4 — Login to the CTF Server shell

Use this command in a second terminal to connect to the shell (replace “thedoctor” with the username you selected).

```
ssh -o ProxyCommand='nc -x localhost:8123 %h %p' thedoctor@192.168.2.83
```

Note the first time, you’ll see the below message. Just push enter and use the Up arrow to repeat the ssh command above

A terminal window with a black background and green text. The prompt is 'mcarlisl@INI-MCARLISL-L3 ~'. The user enters the command '\$ ssh -o ProxyCommand='nc -x localhost:8123 %h %p' thedoctor@192.168.2.13'. The terminal output shows a warning about the authenticity of the host, the ECDSA key fingerprint, and a confirmation to add the host to the known hosts list. It then says 'Welcome thedoctor!' and 'Your shell server account has been created. Please press enter and reconnect.'

```
mcarlisl@INI-MCARLISL-L3 ~  
$ ssh -o ProxyCommand='nc -x localhost:8123 %h %p' thedoctor@192.168.2.13  
The authenticity of host '192.168.2.13 (<no hostip for proxy command>)' can't be  
established.  
ECDSA key fingerprint is SHA256:Lxid0CLyPHDdV1oPvG1ImT0Tgrnp2TQb4b2F0Zvd62U.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '192.168.2.13' (ECDSA) to the list of known hosts.  
Welcome thedoctor!  
Your shell server account has been created.  
Please press enter and reconnect.
```

Re-connecting to the CTF Server (quick guide)

This is an abbreviated version without the steps (installing software & setting up an account) that you only need to do the first time.

1. In a terminal, run:

```
ssh -D 8123 -C -q -N ctfssocks@ctf.martincarlisle.com
```

Password: XXXX!

The terminal will appear to hang; just leave it open until you are done with the CTF server.

2. Re-enable the Firefox proxy, if you turned it off last time. It should remember your settings; you just have to change “No proxy” to “Manual proxy configuration”.

3. In Firefox, go to <http://192.168.2.82/>

4. In a new terminal, run:

```
ssh -o ProxyCommand='nc -x localhost:8123 %h %p' your_username@192.168.2.83
```

This terminal is where you will run commands for your exploits.

When you're done, change the Firefox proxy settings back to “No Proxy” if you plan to use Firefox for normal web browsing. You can also close out of both terminals.