

## Simple Honeypot Lab

A) For this exercise it is recommended that you work with another friend (or use tmux or screen) so that you can work on different consoles in a single connection

1. Connect (ssh) to your linux server in the virtual lab
2. Take note of your IP address
3. Write the following command at the command prompt

```
nc -vvv -l 2323 >> telnethoneypot.log
```

4. Get another friend to connect to port 2323 on your server  

```
telnet <your_friend_ip_address> 2323
```
5. Check if you are getting any connection to your honeypot
  - a. Ctrl-C to stop nc
  - b. check the contents in *telnethoneypot.log*  

```
more telnethoneypot.log
```

B) Part 2

1. Ssh to your linux server
2. Issue the following command at the shell prompt  

```
while [ 1 ]; do echo -e "220 ProFTPD 1.3.3c Server [ProFTPDx] \nFAILED FTP ATTEMPT - PORT 2121" | nc -vvv -l 2121 >> ftphoneyypot.log 2>> ftphoneyypot.log; done
```
3. Get another friend to ftp to your server  

```
ftp <your_friends_ip_address> 2121
```
4. Observe what is happening to nc and the ftphoneyypot.log

Bonus

- 1) Can we put the command in the script that we can execute at the prompt or upon boot?
- 2) Can get the scripts to run using port 23 and 21 respectively

[End of Lab]

