Lab 12 – The Joys of Netcat

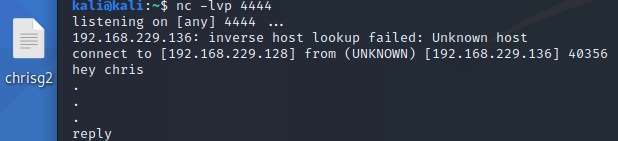
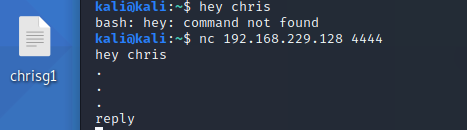
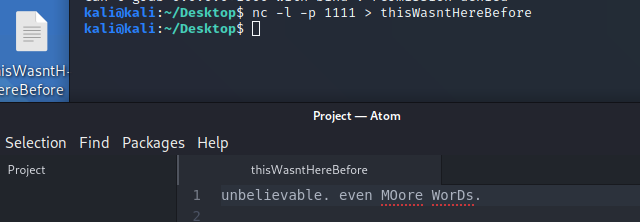
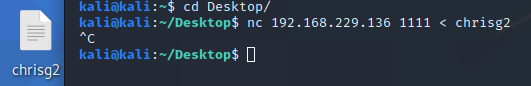
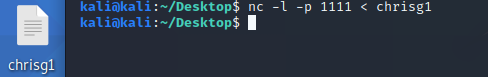
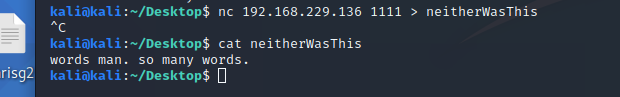
We are going to build on our Netcat skills with some exercises to flex our muscles. It is up to **you** to determine the environment that you do this work in. If you like, you can use Kali 2017 and Kali 2020-3 in the IA Lab lab 11 environment. If you have a home set up, you can copy one Kali, and the two could communicate. Any setup you can envisage is acceptable; you can even do Linux to Windows, although you will need to do additional research to make that work for you. **If in doubt, simply use the Lab 11 environment.**

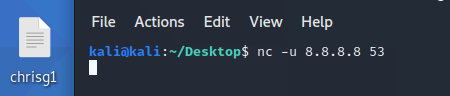
For task, you must complete the requested action and supply a screenshot. **If it is in a Linux environment, your name should be visible in the background.** For a Windows environment, I still need to see your name in an open text file or similar in the background.

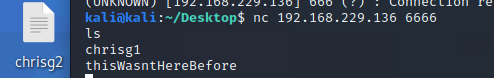
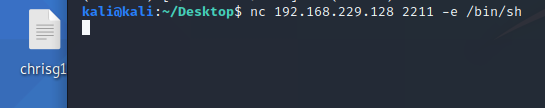
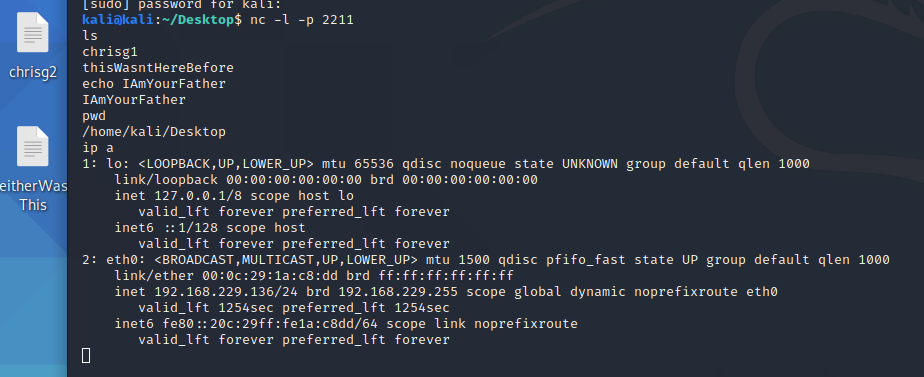
Make sure to number your response; no numbering, no grade. If screenshots are unreadable due to being a too tiny to read, no points are given. Please crop screenshots appropriately. I only need to see what I am asking for – not the entire desktop.

Provide screenshot(s) for each question, along with supporting text, to demonstrate you have satisfied each question. Most can be answer by 1-3 cropped screenshots.

The following questions have some suggested ways to implement this. You may vary from this, as need be! These are merely suggestions.

1. Create a netcat listener and a client. Have them “chat” between each other, passing messages.
2. Push a file with Netcat
3. Pull a file with Netcat
4. 
5. Use Netcat to interact with an open port of your choice



1. Use Netcat as a **passive** backdoor --Bind a service to a port and execute once it connects.
2. Use Netcat as a **active** backdoor
3. **Extra Credit (4 points).** 
   * Relay traffic with Netcat. Relay traffic over four different machines. Provide sufficient screenshots and/or video to demonstrate success.

**I don’t have the disk space to clone kali 2 more times, so I’m going to just run a relay back and forth through both machines for 4 links … hopefully that’s fine**

**Deliverables**

* These MUST be contained all in one PDF or DOC/DOCX.
* Crop screenshots appropriately; points are taken off if this is not done.