# CYB 310 Module Five Lab Worksheet

Complete this worksheet by replacing the bracketed phrases in the Response column with the relevant information.

| **Lab: Closing Ports and Unnecessary Services** | |
| --- | --- |
| **Prompt** | **Response** |
| In the lab section, "Connecting to the Open Ports and Services Using Telnet and FTP," **Step 13,** complete the steps, type your name after the command prompt, and take a screenshot of the output. |  |
| In the lab section, "Closing Unnecessary Ports and Services," **Step 26,** type your name after the command prompt and take a screenshot of the output of the scan of port 80 (www) on the Windows machine after closing HTTP services. |  |
| Closing unwanted ports and communication mediums is essential to network hardening. Why is this essential and how does it help with network defense? | Open and unnecessary ports can lead to unanticipated and unnecessary exploitation. While we can’t close every single port, certain ports have no reason to be open. For example, there is no reason for telnet to be open. By closing it, we completely eliminate exploitation in that avenue. |
| Using an adversarial mindset, how can you test to make sure only needed ports are open? What tools would you use? | Personally, I would use zenmap to check for open ports. While nmap does the same exact thing, zenmap has a nice GUI and can help simplify the process. For example, and obsolete ports such as telnet should be closed immediately. I can then look at my organizations mission and see which other ports can be closed. For example, HTTP/HTTPS can be closed if you’re not hosting a webserver. |