Questions (40 points)

1. Is it generally better to use a root session when hardening a Linux machine as opposed to prefixing every command with `sudo`? Why or why not? **(5 points)**
2. How would you implement a secure password policy on Ubuntu? How does this differ from the implementation on CentOS? Include your configuration for both. **(5 points)**
3. Write up some `iptables` rules **(20 points)**
    a. Set a default deny rule on incoming connections.
    b. Allow incoming on port 22/tcp.
    c. Allow incoming mysql connections.
    d. Allow only 10.10.10.4 to access the previously listed ports.
4. What is a `netstat` command you can use to view your current connections to detect reverse shells? Think about what type of connections reverse shells will make on the victim host **(10 points)**

Troubleshooting Lab (60 points)

Use the Debian machine named "FixMe" for this lab. Fix all of the following and document your steps with text, command snippets, screenshots, and/or all 3. Show proof that the fix works.

1. FixMe's iptables command seems to be a bit funny
2. FixMe cannot hit the internet
3. Any user can switch into another user, even with the incorrect password being used
4. FixMe's SSH is not running
5. FixMe's SSH port doesn't seem to be right
6. FixMe's web server's index page is returning a 404
7. FixMe's "/test.php" is not rendering php
8. FixMe's FTP server doesn't seem to be serving the right files for the anonymous user
9. FixMe has a backdoor user
10. FixMe has a bunch of sudoers
11. FixMe has a backdoor in /opt
12. FixMe keeps generating files in the root directory