Quiz 2

Student name: Evan Smith

1(20): what is the firewall, what are the types of the firewall according to filtering directions.

What type is the default ufw according to it's filtering direction(without setting up anything)? Can ufw be both direction? How? if you'd like to use ufw to block traffic, what is the first thing to do in VM(assume it is already enabled)? What is the reason?

A firewall is a filter that looks at incoming and outgoing traffic through a node and blocks or limits that traffic using some rules. The types of firewalls by filter direction are ingress and egress filtering. By default, ufw is an inbound firewall that blocks all incoming traffic. You can use ufw in both directions by adding specific filter rules to the set. If ufw is already enabled on the VM, you would just need to add a rule to block the traffic that you are trying to prevent using sudo ufw deny from xx.xx.xx.xx.

2(20): How many types of firewall do we have according to it functions?

Three: Packet Filters, Stateful, and Application/Proxy

3(20): Where does firewall run: Kernel or user space?

It runs in the kernel.

4(40): What is the module are you using to write firewall in this lab, is it in the user space or kernel space? how does it work? (not in code detail, in names detail, such as what do you call those connections function? where does this module run and how does it achieve it's purpose etc)

We are using the Loadable Kernel Module and NetFilter for the lab. It runs in the kernel, which is required to filter packets, but it is written in the user space. LKM is used to inject the written code into the kernel using hooks that Linux has in place for this purpose. We then can run Netfilter rules in the kernel by adding them via the terminal. As packets come into the machine, they will trigger the Netfilter hooks at certain points in their processing. The ruleset we can make will now be checked at these points in the process, allowing us to filter traffic as desired.