By William Lentini, Shamar Roberts, and Daniel Lake

1. In class we discussed the security principle of layering or defense-in-depth. How do firewalls provide this capability i.e. how do they allow one to achieve defense-in-depth? **Firewalls achieve defense-in-depth by having a layer for each type of information that could pass through a firewall. The different types of layers or "filter characteristics" are "IP address and protocol values", "application protocol", "user identity", and "network activity". Each part of information flows through the layers to have the firewall verify and make sure that the files have no malicious intent and will not harm the system.**

2. Tell me specifically what rule did your setup on step 17. What did it do, what was the service you protected? **Some rules I set up in step 17 was sudo ufw deny in from 192.168.5.6 to 193.168.5.5 port 23 this stopped the windows vm from telneting to the seedUbuntu machine. Another rule I set up took multiple parts because it had multiple addresses, I wanted to see what would happen if I tried to sudo ufw deny out one address and then all addresses, no matter what I couldn't get into the website. I wasn't sure if this was the correct way to go about it because I tried contacting you.**

3. How can firewalls allow you to implement solutions to some hypothetical intrusion attack i.e., explain how you will rely on the firewall in order to provide secure solutions to a hypothetical intrusion. **I will rely on a firewall in order to provide secure solutions to a hypothetical intrusion attacks because it has a layering system that information has to pass through to get to its destination, it has only one chokepoint that the information can go through, so the information has to go through the firewall, and the firewall is immune to penetration. These security measures ensure that no malicious information gets through the firewall and into your system.**

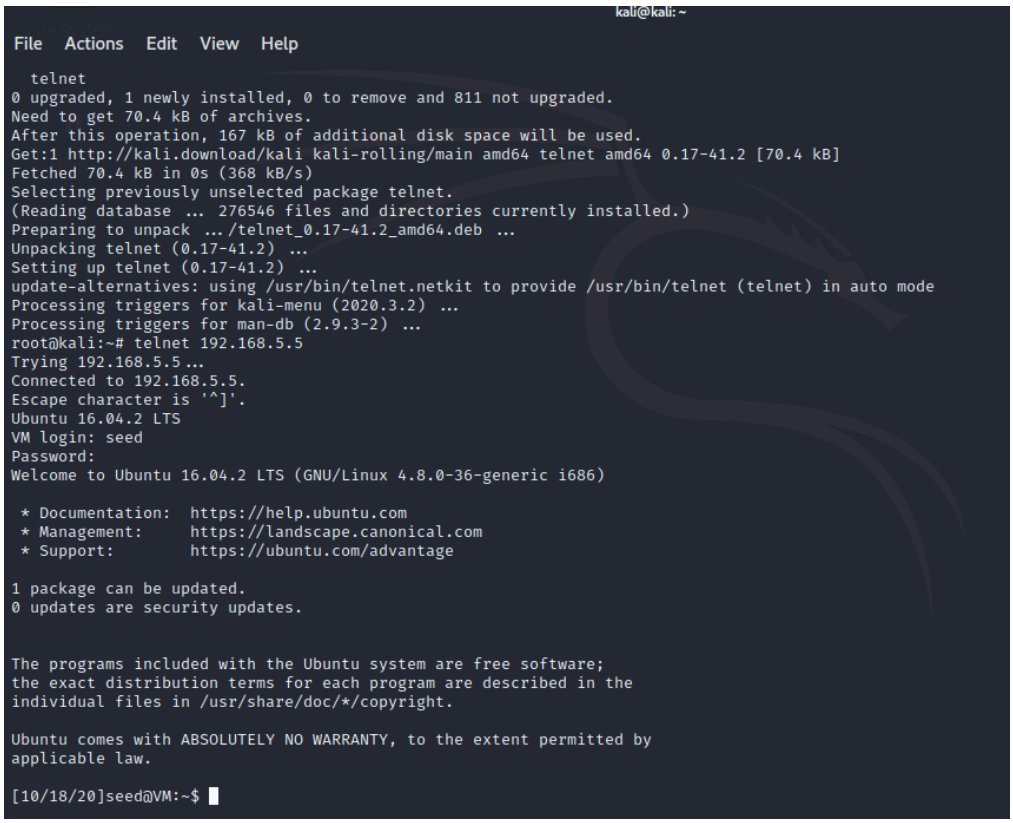
4. What did you like about this activity the most? **The thing that we most liked about this activity was the questions about the firewalls. We liked these questions because it allowed us to go back through the notes and further understand how firewalls work to protect our system.**

5. What did you dislike about this activity the most? **The thing that we most disliked about this activity was the question that stated "Tell me specifically what rule did your setup on step 17. What did it do, what was the service you protected?" The reason we disliked this question was because it was confusing and we were a bit lost as to how to get this question done.**

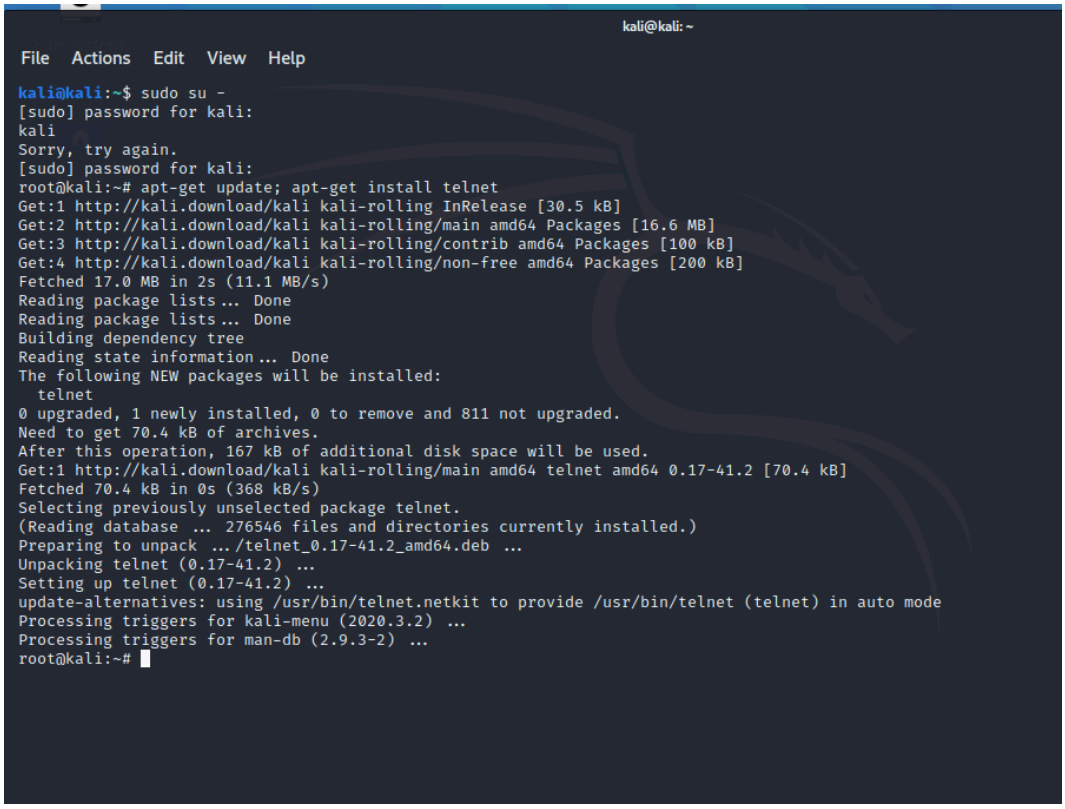
6. What change would you suggest (any at all) and for what reason? **I don't think we would change anything about the lab, it was rather straightforward and stress free besides the question which reads "Tell me specifically what rule did your setup on step 17. What did it do, what was the service you protected?" but we think that question is made to make people think so we understand the challenge there.**

Screenshots:

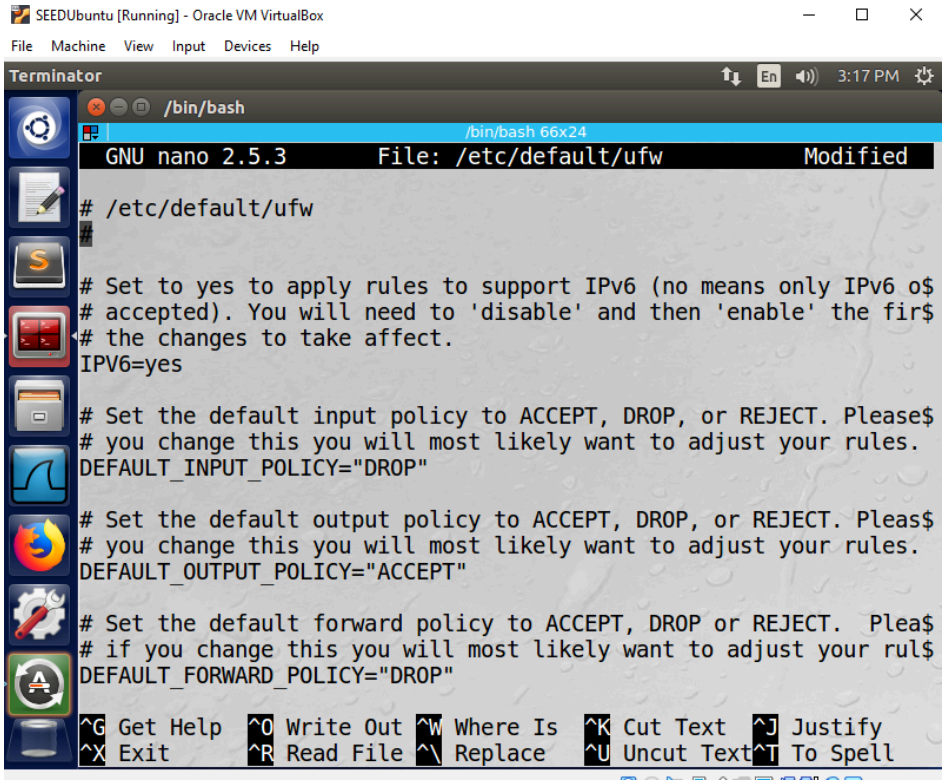
- Telnet between Seed and Kali



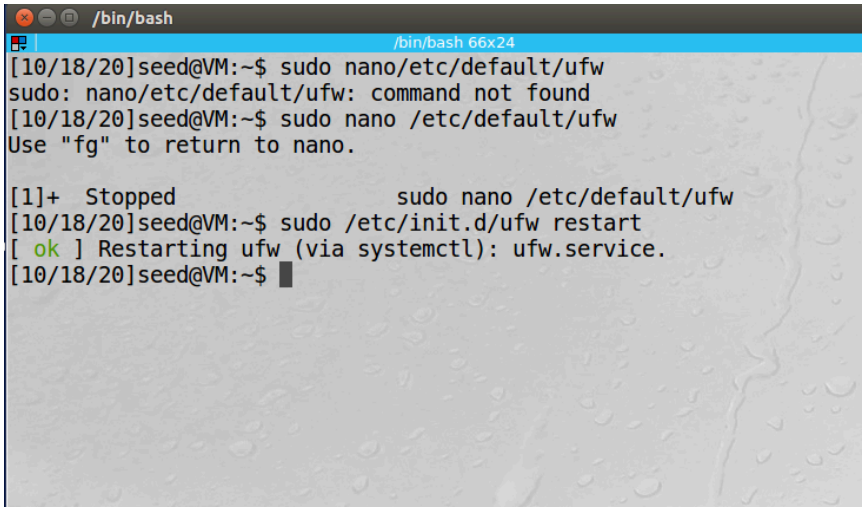
- Trying to download the telnet command on kali



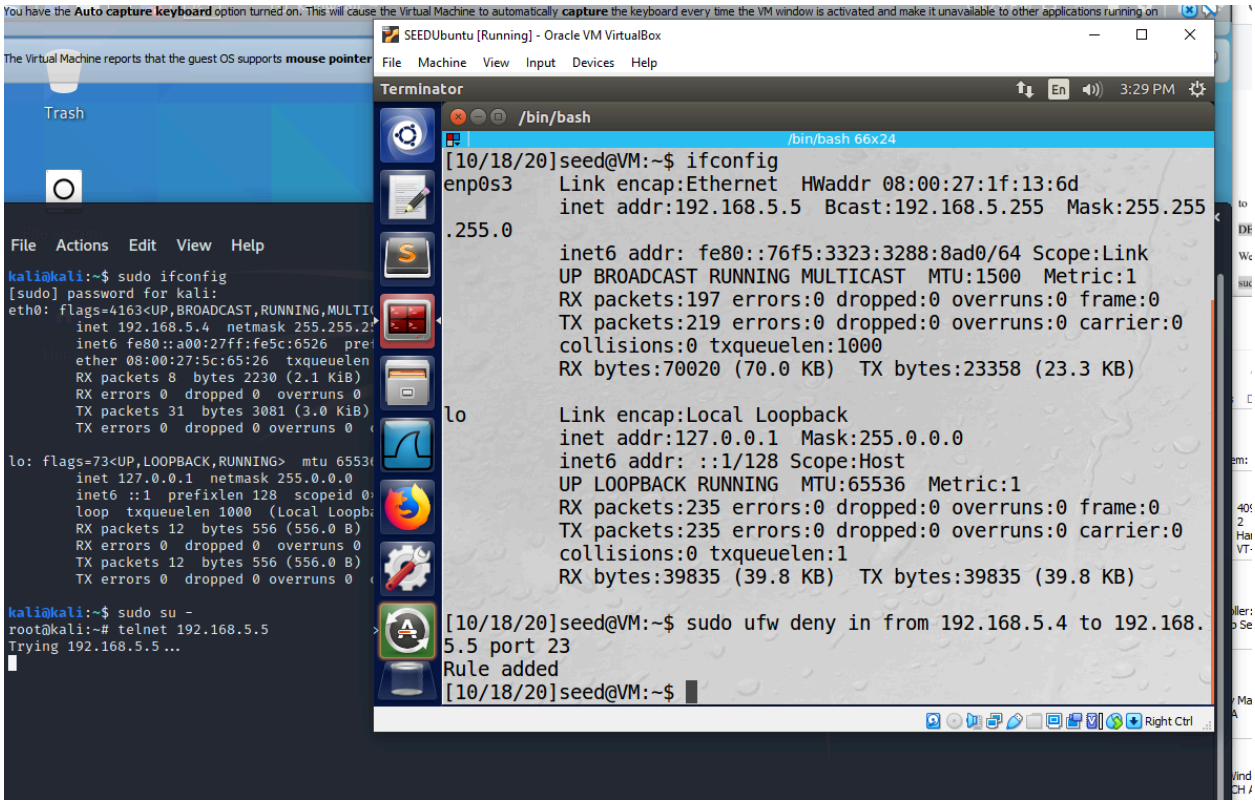
Before changing input policy to accept



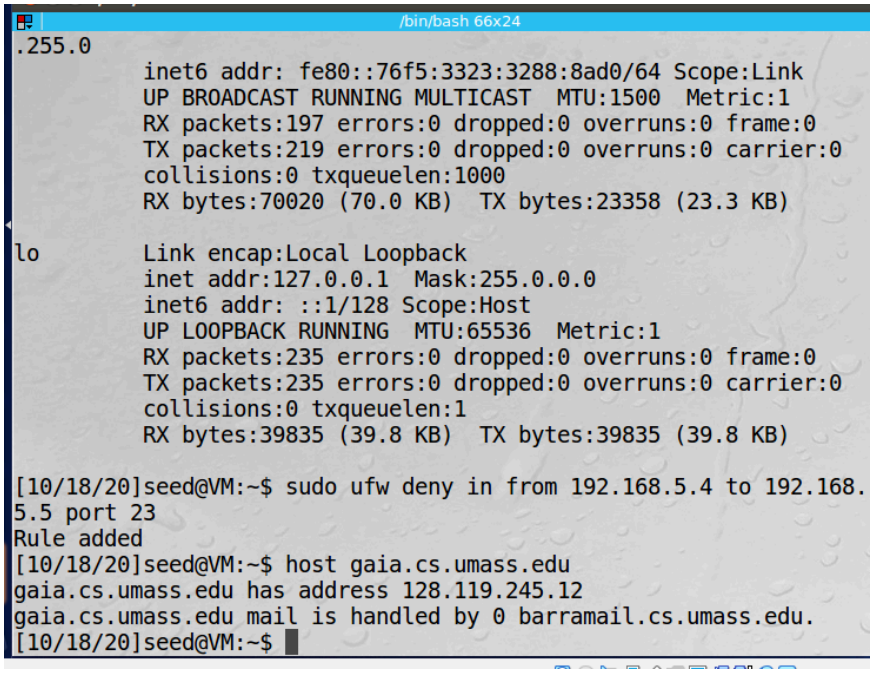
- Enable firewall



- Unable to telnet between kali and seed



- Looking for gaia address



- Unable to go to the umass website

- Deleting rules