- 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

```
kali@kali: ~
  File Actions Edit View Help
   telnet
O upgraded, 1 newly installed, 0 to remove and 811 not upgraded.

Need to get 70.4 kB of archives.

After this operation, 167 kB of additional disk space will be used.

Get:1 http://kali.download/kali kali-rolling/main amd64 telnet amd64 0.17-41.2 [70.4 kB]
Get:1 http://kali.download/kali kali-rolling/main amd64 telnet amd64 0.17-41.2 [70.4 kB]
Fetched 70.4 kB in 0s (368 kB/s)
Selecting previously unselected package telnet.
(Reading database ... 276546 files and directories currently installed.)
Preparing to unpack ... /telnet_0.17-41.2_amd64.deb ...
Unpacking telnet (0.17-41.2) ...
Setting up telnet (0.17-41.2) ...
update-alternatives: using /usr/bin/telnet.netkit to provide /usr/bin/telnet (telnet) in auto mode
Processing triggers for kali-menu (2020.3.2) ...
Proctakali:-# telnet 192.168.5.5
 root@kali:~# telnet 192.168.5.5
root@kati.~#
Trying 192.168.5.5...
Connected to 192.168.5.5.
Connected to 192.168.5.5.
Escape character is
Ubuntu 16.04.2 LTS
VM login: seed
 Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)
  * Documentation: https://help.ubuntu.com

* Management: https://landscape.canonical.com

* Support: https://ubuntu.com/advantage
  * Support:
 1 package can be updated.
0 updates are security updates.
The programs included with the Ubuntu system are free software;
  the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.  \\
 [10/18/20]seed@VM:~$
```

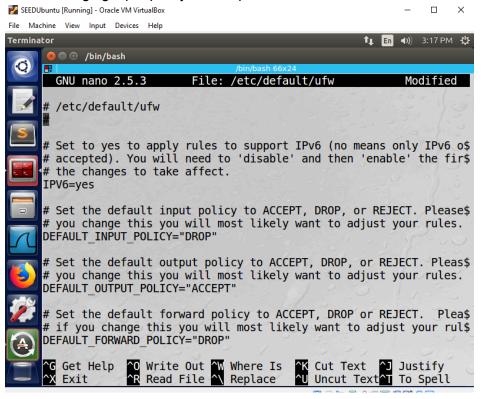
Trying to download the telnet command on kali

```
File Actions Edit View Help

kalimkalir-$ sudo su -
[sudo] password for kali:
kali

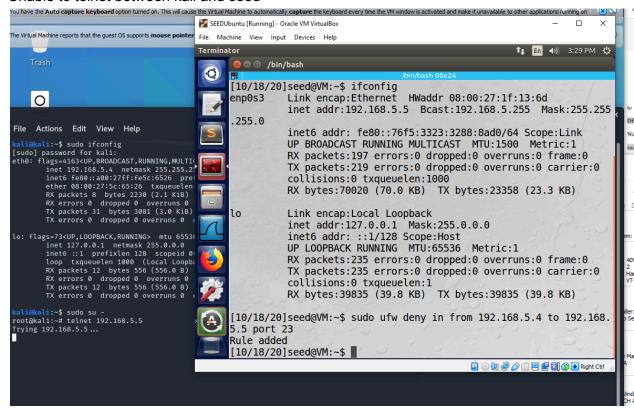
Sorry, try again.
[sudo] password for kali:
rootākalir-# apt-get update; apt-get install telnet
Get:1 http://kali.download/kali kali-rolling/nain amd64 Packages [16.6 MB]
Get:2 http://kali.download/kali kali-rolling/nain amd64 Packages [100 kB]
Get:3 http://kali.download/kali kali-rolling/non-free amd64 Packages [200 kB]
Fetched 17.0 MB in 2s (11.1 MB/s)
Reading package lists ... Done
Reading state information ... Done
The following NEW packages will be installed:
telnet
0 upgraded, 1 newly installed, 0 to remove and 811 not upgraded.
Need to get 70.4 kB of archives.
After this operation, 167 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 telnet amd64 0.17-41.2 [70.4 kB]
Fetched 70.4 kB in 0s (368 kB/s)
Selecting previously unselected package telnet.
(Reading database ... 276546 files and directories currently installed.)
Preparing to unnack ... /telnet.0.17-41.2 ...
Unnacking telnet (0.17-41.2) ...
Unnacking telnet (0.17-41.2) ...
Undate-alternatives: using /usr/bin/telnet.netkit to provide /usr/bin/telnet (telnet) in auto mode
Processing triggers for kali-menu (2020.3.2) ...
rootākali:-#
```

Before changing input policy to accept

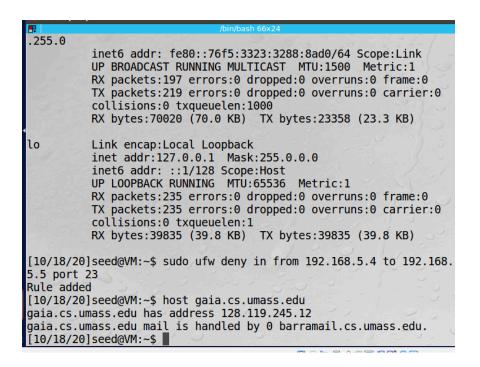


Enable firewall

Unable to telnet between kali and seed



Looking for gaia address



Unable to go to the umass website



Deleting rules

```
[10/18/20]seed@VM:~$ sudo ufw deny in from 192.168.5.4 to 192.168.
5.5 port 23
Rule added [10/18/20]seed@VM:~$ host gaia.cs.umass.edu
gaia.cs.umass.edu has address 128.119.245.12
gaia.cs.umass.edu mail is handled by 0 barramail.cs.umass.edu.
[10/18/20]seed@VM:~$ sudo ufw deny out to 128.119.245.12
Rule added
[10/18/20] seed@VM:~$ sudo ufw status numbered
Status: active
                                 Action
                                              From
     To
[ 1] 192.168.5.5 23
                                 DENY IN
                                              192.168.5.4
[ 2] 128.119.245.12
                                 DENY OUT
                                              Anywhere
     (out)
[10/18/20]seed@VM:~$ sudo ufw delete 1
Deleting:
deny from 192.168.5.4 to 192.168.5.5 port 23
Proceed with operation (y|n)? y
Rule deleted
[10/18/20]seed@VM:~$
```