

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

```
kali@kali: ~  
File Actions Edit View Help  
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 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) ...  
Processing triggers for man-db (2.9.3-2) ...  
root@kali:~# telnet 192.168.5.5  
Trying 192.168.5.5...  
Connected to 192.168.5.5.  
Escape character is '^]'.  
Ubuntu 16.04.2 LTS  
VM login: seed  
Password:  
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  
  
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

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali:~$ sudo su -  
[sudo] password for kali:  
kali  
Sorry, try again.  
[sudo] password for kali:  
root@kali:~# apt-get update; apt-get install telnet  
Get:1 http://kali.download/kali kali-rolling InRelease [30.5 kB]  
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [16.6 MB]  
Get:3 http://kali.download/kali kali-rolling/contrib amd64 Packages [100 kB]  
Get:4 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 package lists... Done  
Building dependency tree  
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 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) ...  
Processing triggers for man-db (2.9.3-2) ...  
root@kali:~#
```

Before changing input policy to accept

SEEDUbuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminator

```
/bin/bash  
GNU nano 2.5.3 File: /etc/default/ufw Modified  
# /etc/default/ufw  
#  
# Set to yes to apply rules to support IPv6 (no means only IPv6 o$  
# accepted). You will need to 'disable' and then 'enable' the fir$  
# the changes to take affect.  
IPV6=yes  
# Set the default input policy to ACCEPT, DROP, or REJECT. Please$  
# you change this you will most likely want to adjust your rules.  
DEFAULT_INPUT_POLICY="DROP"  
# Set the default output policy to ACCEPT, DROP, or REJECT. Pleas$  
# you change this you will most likely want to adjust your rules.  
DEFAULT_OUTPUT_POLICY="ACCEPT"  
# Set the default forward policy to ACCEPT, DROP or REJECT. Pleas$  
# if you change this you will most likely want to adjust your rul$  
DEFAULT_FORWARD_POLICY="DROP"  
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify  
^X Exit ^R Read File ^N Replace ^U Uncut Text ^T To Spell
```

- Enable firewall

```

/bin/bash
[10/18/20]seed@VM:~$ sudo nano /etc/default/ufw
sudo: nano /etc/default/ufw: command not found
[10/18/20]seed@VM:~$ sudo nano /etc/default/ufw
Use "fg" to return to nano.

[1]+  Stopped                  sudo nano /etc/default/ufw
[10/18/20]seed@VM:~$ sudo /etc/init.d/ufw restart
[ ok ] Restarting ufw (via systemctl): ufw.service.
[10/18/20]seed@VM:~$

```

- Unable to telnet between kali and seed

```

You have the Auto capture keyboard option turned on. This will cause the Virtual Machine to automatically capture the keyboard every time the VM window is activated and make it unavailable to other applications running on
The Virtual Machine reports that the guest OS supports mouse pointer

Trash

File Actions Edit View Help
kali@kali:~$ sudo ifconfig
[sudo] password for kali:
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.5.4 netmask 255.255.255.255
    inet6 fe80::a00:27ff:fe5c:6526 prefixlen 64 scopeid 0x0
    ether 08:00:27:5c:65:26 txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 2230 (2.1 KiB)
    RX errors 0 dropped 0 overruns 0
    TX packets 31 bytes 3081 (3.0 KiB)
    TX errors 0 dropped 0 overruns 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x0
    loop txqueuelen 1000 (Local Loopback)
    RX packets 12 bytes 556 (556.0 B)
    RX errors 0 dropped 0 overruns 0
    TX packets 12 bytes 556 (556.0 B)
    TX errors 0 dropped 0 overruns 0

kali@kali:~$ sudo su -
root@kali:~# telnet 192.168.5.5
Trying 192.168.5.5 ...

SEEDUbuntu [Running] - Oracle VM VirtualBox
Terminator
/bin/bash
[10/18/20]seed@VM:~$ ifconfig
enp0s3: Link encap:Ethernet HWaddr 08:00:27:1f:13:6d
    inet addr:192.168.5.5 Bcast:192.168.5.255 Mask:255.255.255.0
    inet6 addr: fe80::76f5:3323:3288:8ad0/64 Scope:Link
    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
    RX packets:197 errors:0 dropped:0 overruns:0 frame:0
    TX packets:219 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:70020 (70.0 KB) TX bytes:23358 (23.3 KB)

lo: Link encap:Local Loopback
    inet addr:127.0.0.1 Mask:255.0.0.0
    inet6 addr: ::1/128 Scope:Host
    UP LOOPBACK RUNNING MTU:65536 Metric:1
    RX packets:235 errors:0 dropped:0 overruns:0 frame:0
    TX packets:235 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1
    RX bytes:39835 (39.8 KB) TX bytes:39835 (39.8 KB)

[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:~$

```

- Looking for gaia address

```

/bin/bash 66x24
.255.0
    inet6 addr: fe80::76f5:3323:3288:8ad0/64 Scope:Link
    UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
    RX packets:197 errors:0 dropped:0 overruns:0 frame:0
    TX packets:219 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:70020 (70.0 KB)  TX bytes:23358 (23.3 KB)

lo
    Link encap:Local Loopback
    inet addr:127.0.0.1  Mask:255.0.0.0
    inet6 addr: ::1/128 Scope:Host
    UP LOOPBACK RUNNING  MTU:65536  Metric:1
    RX packets:235 errors:0 dropped:0 overruns:0 frame:0
    TX packets:235 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1
    RX bytes:39835 (39.8 KB)  TX bytes:39835 (39.8 KB)

[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:~$

```

- Unable to go to the umass website



- Deleting rules

```
/bin/bash
/bin/bash 66x24
[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

      To                        Action      From
      --                        -
[ 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:~$
```