

JW4158-INFO8580-22S-Portfolio4

John White

6714518

INFO8580

Table of Contents

Lab <8> - <Fundamental Linux Security>	3
Description	3
Preparation	3
Screenshots	4
Reflection	6
References	6

Lab <8> - <Fundamental Linux Security>Description

The purpose of this lab is to teach us how to update our Linux machines and configure iptables on them to increase our security. For this assignment, I used Kali Linux on my home laptop.

Preparation

To prepare for this lab, install a Linux VM on VSphere or your laptop.

Observations

Open the Linux terminal and enter the command 'Sudo apt update' this will update your package lists that will be used to update your software. Next, perform the command 'Sudo apt upgrade' this will use the package lists to perform the Linux updates. After updating/upgrading, we should reboot our machine. Now we need to configure our iptables. I used the following commands to configure mine.

Basic setup:

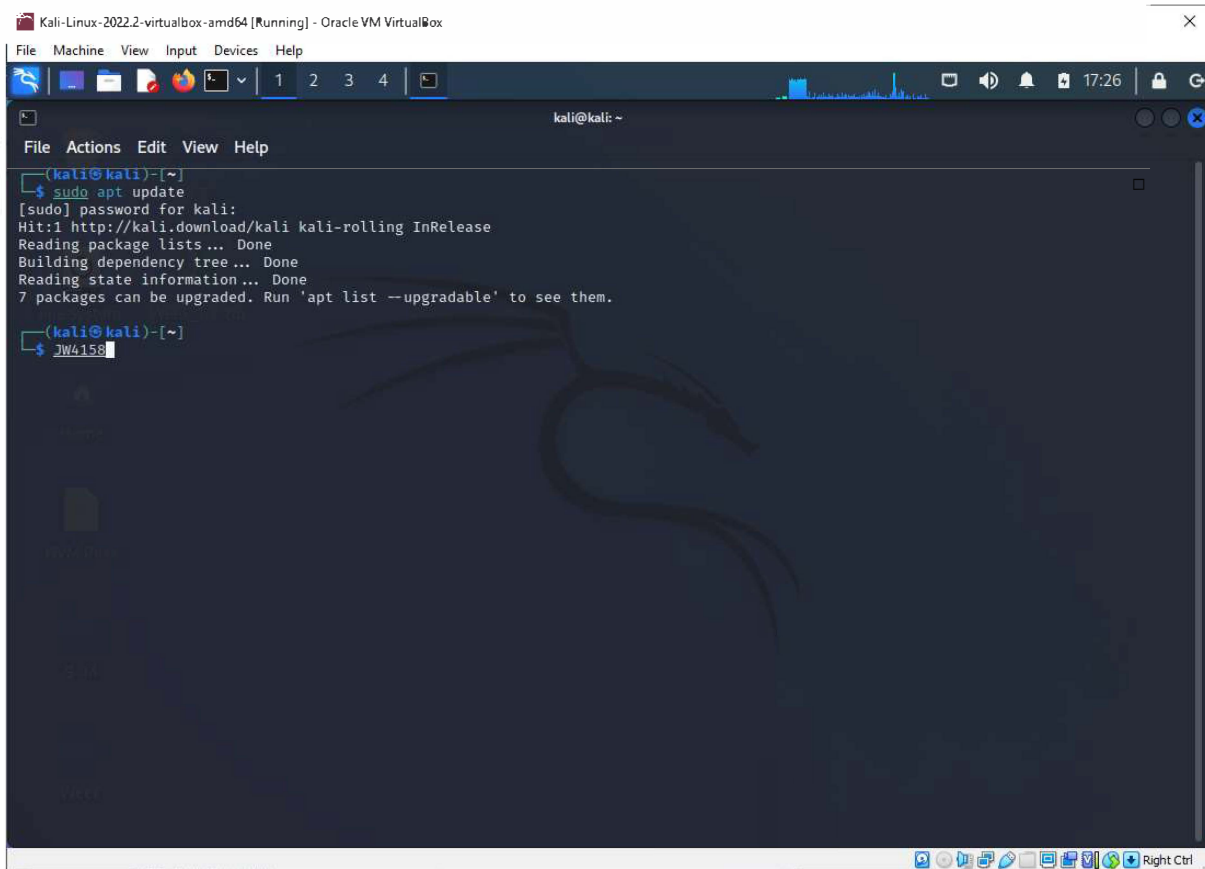
```
sudo iptables -A INPUT -m conntrack--ctstate ESTABLISHED,RELATED -j ACCEPT
sudo iptables -A INPUT -p tcp --dport ssh -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 53 -j ACCEPT
sudo iptables -A INPUT -p udp --dport 53 -j ACCEPT
sudo iptables -A INPUT -m conntrack-p icmp --icmp-type 3 --ctstate NEW,ESTABLISHED,RELATED -j ACCEPT
sudo iptables -A INPUT -m conntrack-p icmp --icmp-type 11 --ctstate NEW,ESTABLISHED,RELATED -j ACCEPT
sudo iptables -A INPUT -m conntrack-p icmp --icmp-type 12 --ctstate NEW,ESTABLISHED,RELATED -j ACCEPT
sudo iptables -A INPUT -j DROP
sudo iptables -I INPUT 1 -i lo -j ACCEPT
```

Block invalid ipv4 packets:

```
sudo iptables -t mangle -A PREROUTING -m conntrack-ctstate INVALID -j DROP
sudo iptables -t mangle -A PREROUTING -p tcp ! -syn -m conntrack--ctstate NEW -j DROP
```

Test the iptables using NULL scan and Windows scan:

```
sudo nmap -sN ip_address_of_your_VM
sudo iptables -L -v
sudo iptables -t mangle -L -v
sudo nmap -sW ip_address_of_your_VM
sudo iptables -L -v
sudo iptables -t mangle -L -v
```

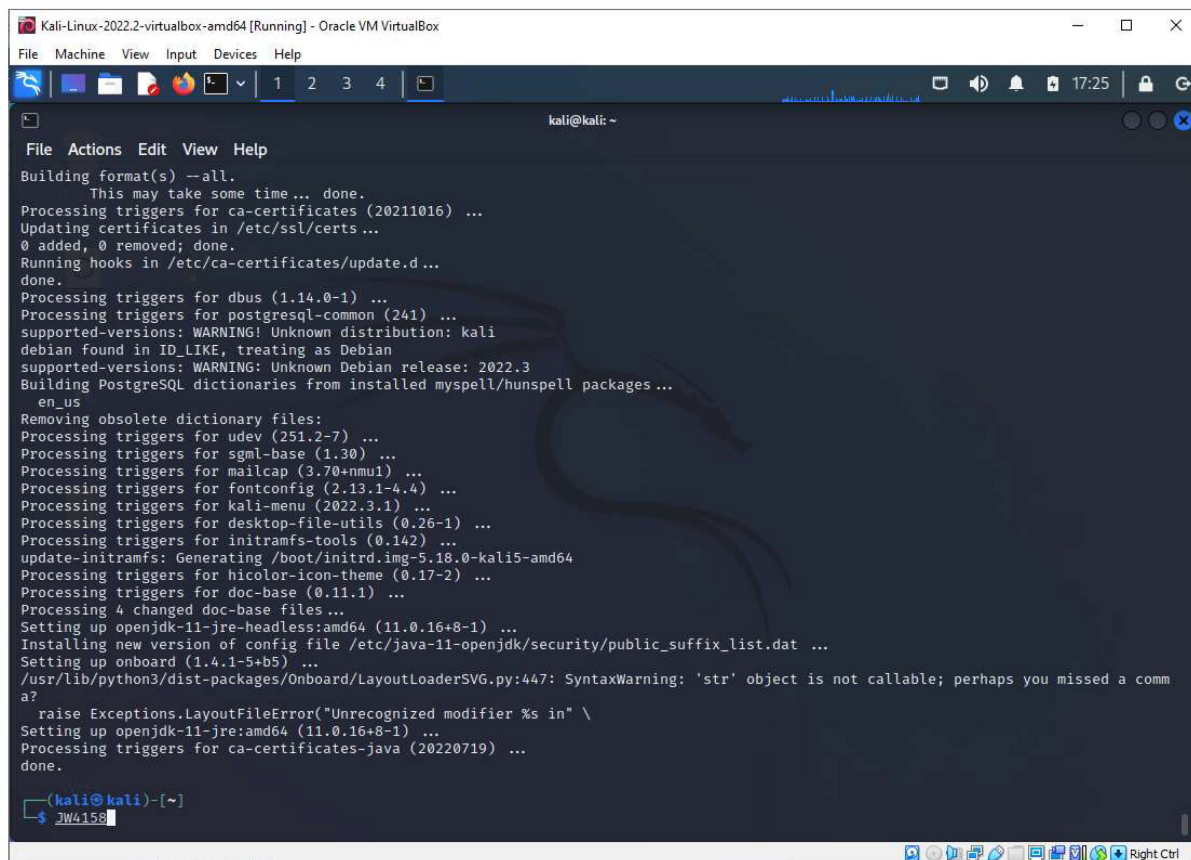
Screenshots:

The screenshot shows a Kali Linux virtual machine window titled 'Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox'. The terminal window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The prompt is '(kali@kali)-[~]'. The command 'sudo apt update' has been executed, and the output is as follows:

```
[sudo] password for kali:  
Hit:1 http://kali.download/kali kali-rolling InRelease  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
7 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

The terminal background features a large, faint dragon logo. The bottom of the window shows a taskbar with various application icons and a system tray on the right with a 'Right Ctrl' button.

Figure 1.1 - 'Sudo apt update' completed.



```
Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help
Building format(s) --all.
  This may take some time... done.
Processing triggers for ca-certificates (20211016) ...
Updating certificates in /etc/ssl/certs ...
0 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
Processing triggers for dbus (1.14.0-1) ...
Processing triggers for postgresql-common (241) ...
supported-versions: WARNING! Unknown distribution: kali
debian found in ID_LIKE, treating as Debian
supported-versions: WARNING! Unknown Debian release: 2022.3
Building PostgreSQL dictionaries from installed myspell/hunspell packages ...
en_us
Removing obsolete dictionary files:
Processing triggers for udev (251.2-7) ...
Processing triggers for sgml-base (1.30) ...
Processing triggers for mailcap (3.70+nmu1) ...
Processing triggers for fontconfig (2.13.1-4.4) ...
Processing triggers for kali-menu (2022.3.1) ...
Processing triggers for desktop-file-utils (0.26-1) ...
Processing triggers for initramfs-tools (0.142) ...
update-initramfs: Generating /boot/initrd.img-5.18.0-kali5-amd64
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for doc-base (0.11.1) ...
Processing 4 changed doc-base files...
Setting up openjdk-11-jre-headless:amd64 (11.0.16+8-1) ...
Installing new version of config file /etc/java-11-openjdk/security/public_suffix_list.dat ...
Setting up onboard (1.4.1-5+b5) ...
/usr/lib/python3/dist-packages/Onboard/LayoutLoaderSVG.py:447: SyntaxWarning: 'str' object is not callable; perhaps you missed a comma?
  raise Exceptions.LayoutFileError("Unrecognized modifier %s in" \
Setting up openjdk-11-jre:amd64 (11.0.16+8-1) ...
Processing triggers for ca-certificates-java (20220719) ...
done.
(kali@kali)-[~]
$ JW4158
```

Figure 1.2 - 'Sudo apt upgrade' completed.

```

Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help
(kali@kali)~$ sudo iptables -L
[sudo] password for kali:
Chain INPUT (policy ACCEPT)
target prot opt source destination
ACCEPT all -- anywhere anywhere ctstate RELATED,ESTABLISHED
ACCEPT all -- anywhere anywhere tcp dpt:ssh
ACCEPT tcp -- anywhere anywhere tcp dpt:domain
ACCEPT udp -- anywhere anywhere udp dpt:domain
ACCEPT icmp -- anywhere anywhere ctstate NEW,RELATED,ESTABLISHED icmp destination-unreachable
ACCEPT icmp -- anywhere anywhere ctstate NEW,RELATED,ESTABLISHED icmp time-exceeded
ACCEPT icmp -- anywhere anywhere ctstate NEW,RELATED,ESTABLISHED icmp parameter-problem
DROP all -- anywhere anywhere

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination
(kali@kali)~$ JW4158

```

Figure 1.3 - IP Tables configuration

Reflection

I did not run into any issues during this lab. After updating the PC, it is recommended to perform a reboot so that the updated software can restart. This can take some time, however, so you may not want to do it if you need to use the computer immediately. However, if you are going to be making further modifications, the computer should be restarted to avoid conflicts and errors. If you make a firewall update but do not reload it, the changes will not take effect.

References

1. eConestoga, 2022 (INFO8590_Lab_8_Fundamental_Linux_Security, retrieved from <https://conestoga.desire2learn.com/d2l/le/content/591150/viewContent/12901301/View> on August 13, 2022)
2. eConestoga, 2022 (Hands-on lab for basic iptables usage, retrieved from <https://conestoga.desire2learn.com/d2l/le/content/591150/viewContent/13050486/View> on August 13, 2022)