JW4158-INFO8580-22S-Portfolio4

John White

6714518

INFO8580

Table of Contents

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:

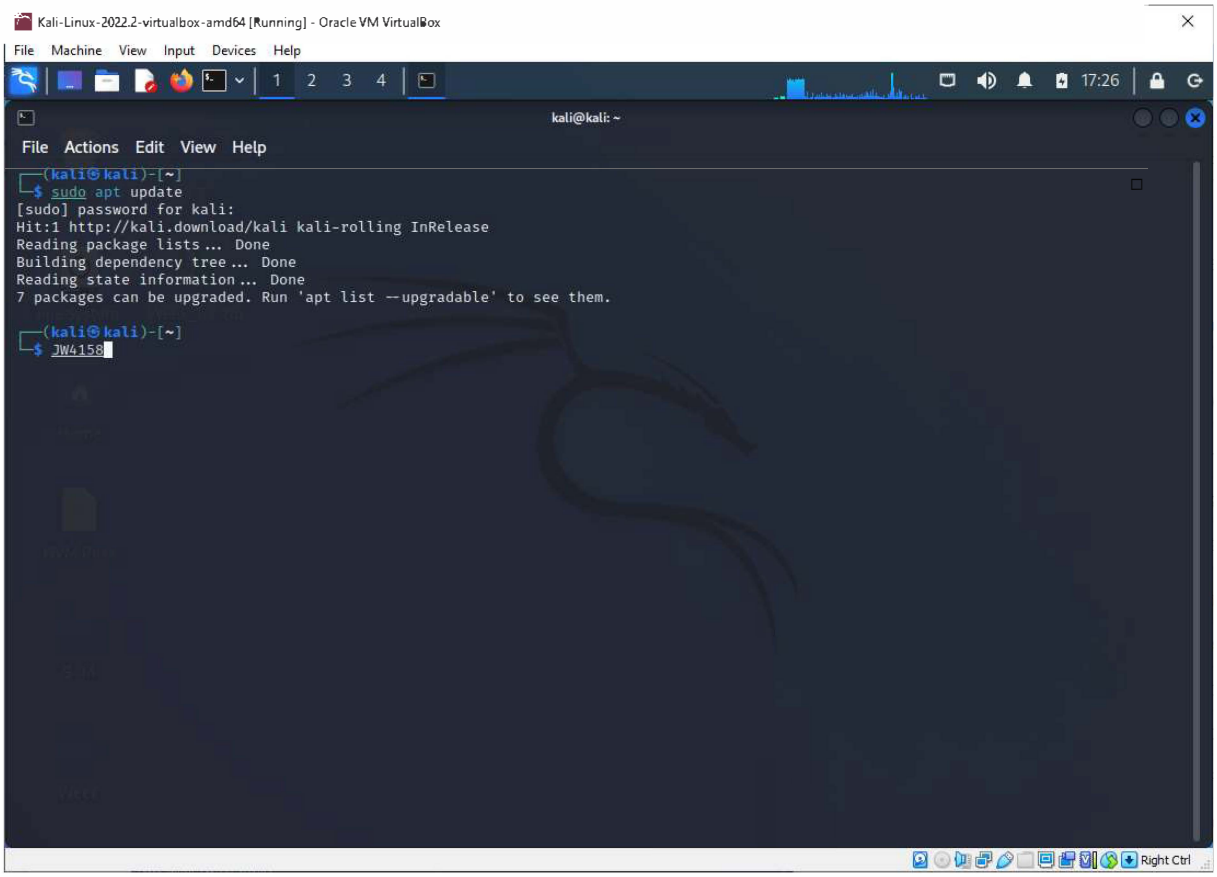

Figure 1.1 - 'Sudo apt update' completed.

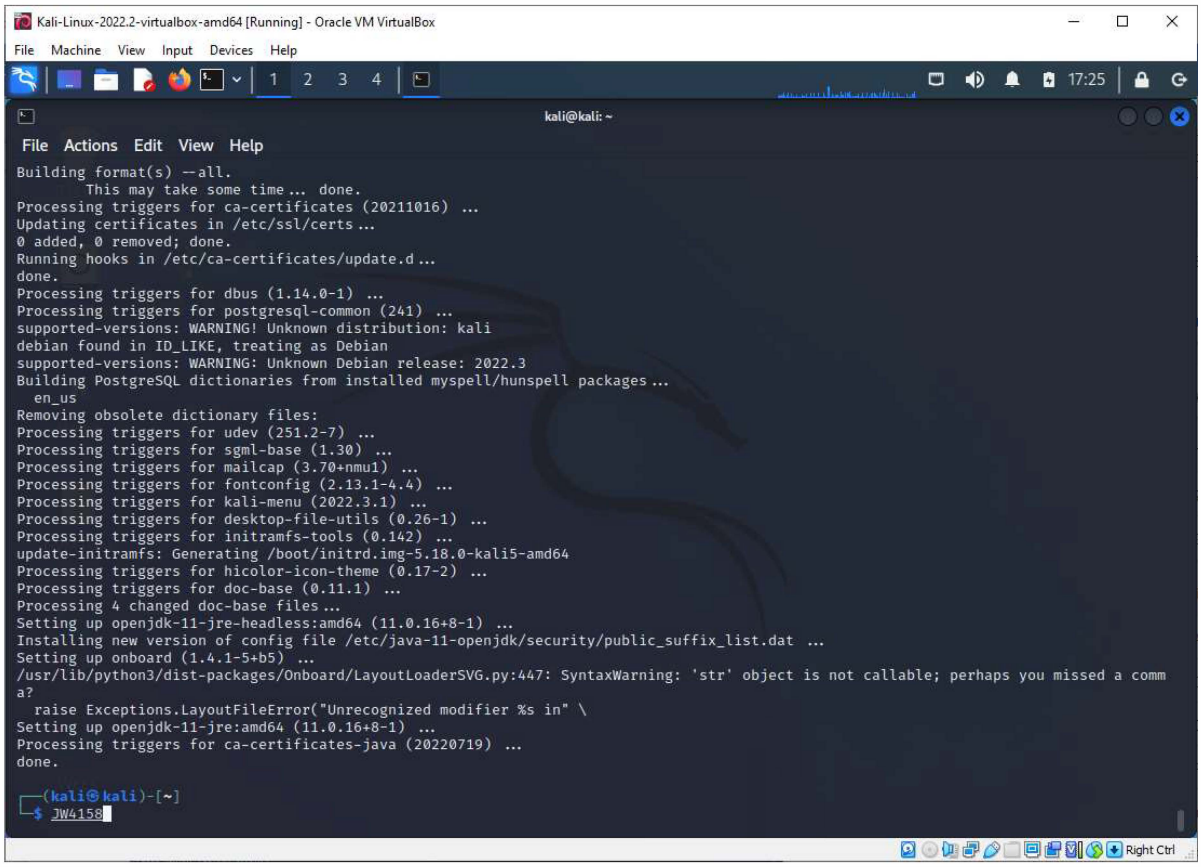

Figure 1.2 - 'Sudo apt upgrade' completed.

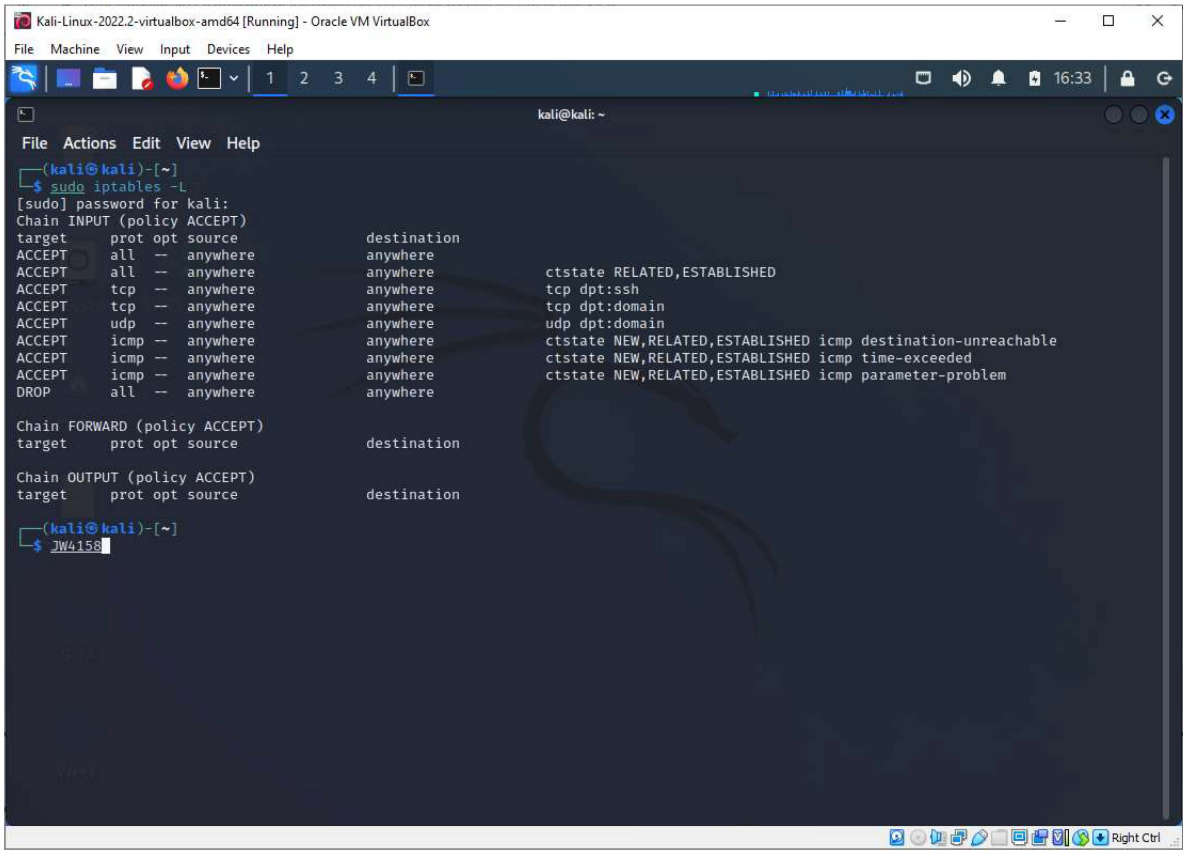

Figure 1.3 - IP Tables configuration

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)