Task 7.1P

Name of Student

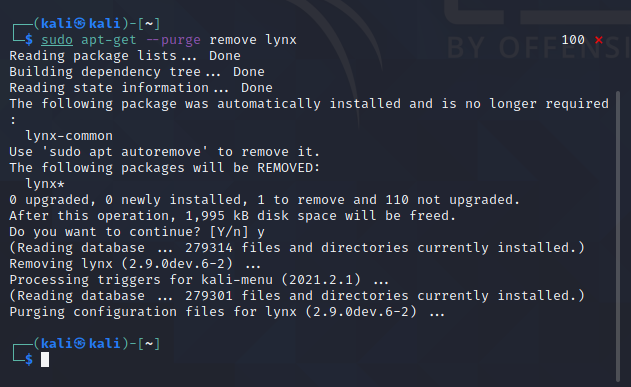
Institutional Affiliation

Q1: What is the APT package manager, and how is it useful?

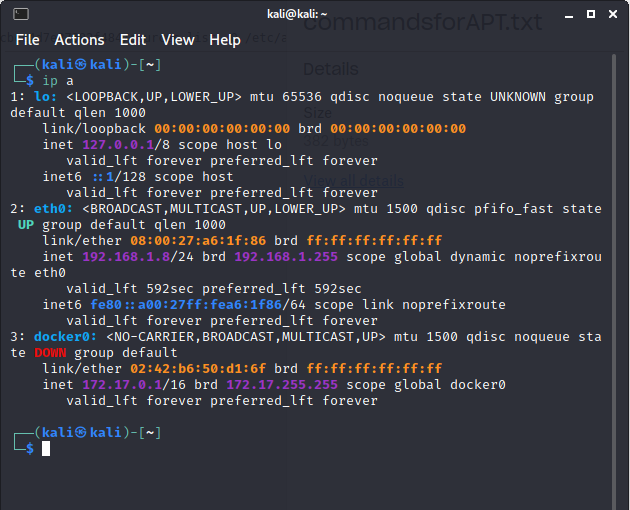
The apt command is a powerful command-line tool, which works with Linux’s Advanced Packaging Tool (APT) performing such functions as installation of new software packages, upgrade of existing software packages, updating of the package list index, and even upgrading the entire system.

Q2: Having used Lynx, you now want to remove it from your Kali VM. You want to use APT for the uninstallation. What is the full command you need to use for this?

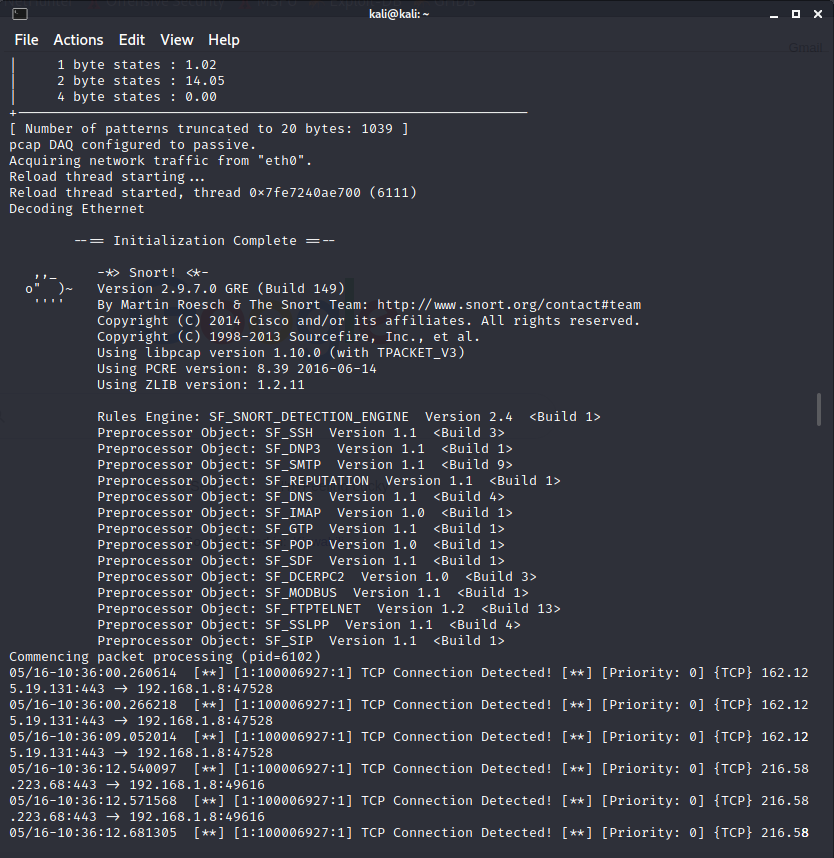
sudo apt-get --purge remove lynx



Q3: What is the IP address for your Kali VM? Include a screenshot of the output you get after running the `ip a’ command in Terminal.



Q4: Include a screenshot of the Terminal with Snort running showing alert messages with “TCP Connection Detected” confirming that Snort has detected TCP traffic after you accessed Google.com in the Web Browser of Kali VM.



Q5: Consider the following Snort rule:

A. What protocol is this rule applied to?

TCP protocol

B. What traffic is monitored? (include source, destination, ports, and directions)

Source: any

Destination: any

Source Port: any

Destination Port: any

Direction: left to right

C. What is the rule action?

alert

D. What does msg: “IP Packet detected” do in this rule?

It is displayed when tcp connection is detected.

E. What is the meaning of sid:1000002 in this rule?

The sid keyword is used to uniquely identify Snort rules

F. What is the meaning of rev:0 in this rule?

The rev keyword is used to uniquely identify revisions of Snort rules. Revisions, along with Snort rule id’s, allow signatures and descriptions to be refined and replaced with updated information. This option should be used with the sid keyword.

Q6: Consider the following Snort rule:

A. What protocol is this rule applied to?

TCP

B. What traffic is monitored? (include source, destination, ports, and directions)

Source: any

Destination: 192.168.1.0/24

Source Port: any

Destination Port: 23

Direction: left to right

C. What is the rule action?

log

D. Does this rule have a rule option argument?

No.

Q7: Consider the following Snort rule:

A. What protocol is this rule applied to?

TCP

B. What traffic is monitored? (include source, destination, ports, and directions)

Source: any

Destination: any

Source Port: any

Destination Port: 22

Direction: left to right

C. What is the rule action?

log

Q8: Consider the following Snort rule:

A. What protocol is this rule applied to?

TCP

B. What traffic is monitored? (include source, destination, ports, and directions)

Source: any

Destination: any

Source Port: any

Destination Port: 23

Direction: bidirectional

C. What is the rule action?

log

Q9: Consider the following Snort rule:

A. What protocol is this rule applied to?

UDP

B. What traffic is monitored? (include source, destination, ports, and directions)

Source: any

Destination: 192.168.1.0/24

Source Port: any

Destination Port: from 1 to 1024

Direction: left to right

C. What is the rule action?

log

Q10: Consider the following Snort rule:

A. What protocol is this rule applied to?

TCP

B. What traffic is monitored? (include source, destination, ports, and directions)

Source: any

Destination: 192.168.1.0/24

Source Port: any

Destination Port: all except from 6000 to 6010

Direction: left to right

C. What is the rule action?

log

D. What is the meaning of “!6000:6010” in this rule?

Not from 6000 to 6010. This means it should not scan those ports.

Q11: Consider the following Snort rule:

A. What protocol is this rule applied to?

TCP

B. What traffic is monitored? (include source, destination, ports, and directions)

Source: not 192.168.1.0/24

Destination: 192.168.1.0/24

Source Port: any

Destination Port: from 1025 onwards

Direction: left to right

C. What is the rule action?

alert

D. What is the meaning of “!192.168.1.0/24” in this rule?

Not from address 192.168.1.0/24.

Q12: Consider the following Snort rule:

A. What protocol is this rule applied to?

TCP

B. What traffic is monitored? (include source, destination, ports, and directions)

Source: any

Destination: any

Source Port: any

Destination Port: any

Direction: left to right

C. What is the rule action?

alert

D. What is the meaning of content:”|90|” in this rule?

It allows the user to set rules that search for specific content in the packet payload. In this case, it searches for 90.

Q13: Consider the following Snort rule:

A. What protocol is this rule applied to?

TCP

B. What traffic is monitored? (include source, destination, ports, and directions)

Source: any

Destination: any

Source Port: any

Destination Port: any

Direction: left to right

C. What is the rule action?

alert

D. What is the meaning of “offset:40” in this rule?

The offset keyword allows the rule writer to specify where to start searching for a pattern within a packet.

E. What is the meaning of “depth:75” in this rule?

A depth of 75 would tell Snort to only look for the specified pattern within the first 75 bytes of the payload

Q14: Consider the following Snort rule:

A. What protocol is this rule applied to?

All protocols

B. What traffic is monitored? (include source, destination, ports, and directions)

Source: any

Destination: any

Source Port: any

Destination Port: any

Direction: left to right

C. What is the rule action?

alert

D. What is the meaning of “flags: SF” in this rule?

The flags keyword is used to find out which flag bits are set inside the TCP header of a packet.

Q15: Consider the following Snort rule:

A. Explain this rule in your own words covering all the different parameters specified as part of it.

$HOME NET is a variable that sets the networks you want to secure, and the external, untrusted networks you are communicating with are $EXTERNAL NET. These variables are used for specifying a packet source and destination conditions in nearly all rules. The snort rule also has options functions in which a message is displayed if any TCP connection that meets the rules are displayed.

Q16: Reflection

Snort is an intrusion and monitoring device free and open-source network. It uses rules to detect suspicious activities on a network and combines the signature, protocol, and anomaly approaches. It is capable of performing real-time traffic analysis and packet logging on IP networks. The more I used Snort, the better I got at understanding the snort rules. The system could be very handy in handling traffic and analyzing specific packets such as UDP or TCP.