WEEK 7 – TASK 7.1P

Pass Task.
Release Date: 3 May, Due Date: 17 May, End Date: 24 May.

Learning Outcomes

In this task, you will learn about Snort IDS, including installation, configuration, and rule definition.

Instructions

An **answer sheet template** is available on OnTrack as a `**Resources**'. Please download the answer sheet and fill it with your answers. To upload on OnTrack, you need to convert the answer sheet template document to **PDF**. MS Word includes built-in PDF conversation capability.

All 16 questions and their sub-questions of this task must be attempted. If screenshots are required, please ensure that the text in screenshots is readable.

Remember that troubleshooting technical problem is part of learning in this field. You must patiently work through issues and solve these. Tasks are not a step-by-step guide. You need to be in the driver seat and learn concepts by doing – as you would when you start your future job (many times, even your future supervisor doesn't know the answer to problems you face). After patent troubleshooting and research, if you need help:

Help is always available in SIT182. Please go to **Discussions** and ask your questions about this task in **Task 7.1P**. All students are encouraged to participate and help peers with their questions. Helping others is a great way to learn and think about aspects you may have overlooked. You can also seek help from tutors during online and face-to-face pracs. Please do not raise your questions through Teams, OnTrack, or Email.

References In cyber security, our preferred referencing style is **IEEE** – however, you are allowed to use any Deakin approved referencing style in this unit. Please refer to unit site > Content > Referencing - Hints & Tips for more information.

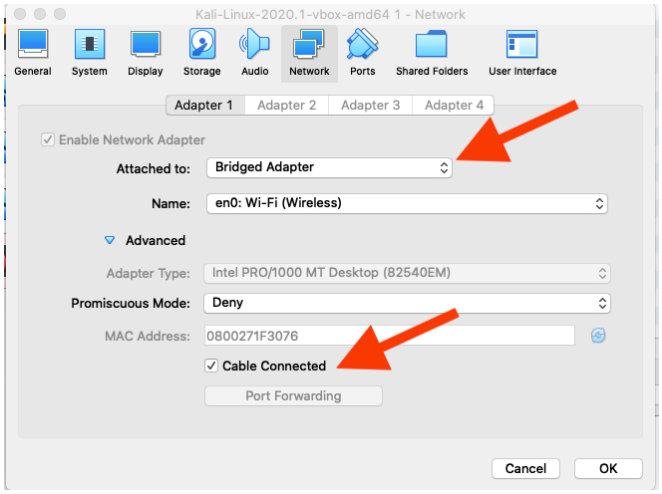
This task has 2 main sections:

- **Section A**: Install and configure Snort IDS on Kali Linux VM
- **Section B**: Learn about Snort rules

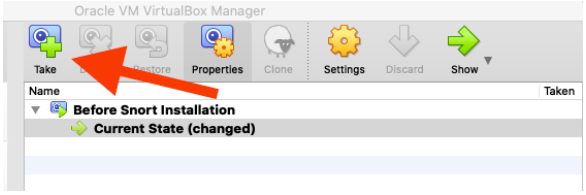
Section A:

We will install the same Kali VM that you have been using in previous weeks for this task. First, ensure that you have downloaded and imported Kali VM in VirtualBox by following the instructions available in previous task sheets.

Enable Network Access for Kali VM and Set Network Adapter to "Bridged Adapter". For this, click on Settings for Kali VM and adjust the network settings under the "Network" tab as shown in the following figure:



Before running Kali VM, take a snapshot of the VM current status. Name this snapshot as "Before Snort Installation". If you encounter any issue with Kali VM during this task, you can just restore it to the status of this snapshot.



Run Kali VM and use the same credentials your previously used for login (i.e., **kali** as username and password).

Snort IDS is not pre-installed in Kali VM. There are different ways that it can be installed and the better way of doing this is by compilation using the source file. Nonetheless, being an introductory unit, we will install Snort using the easier method, which is using a package manager.

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

In Kali VM, open up Terminal and run the following command:

```
sudo apt-get update
```

*When prompted for a password, remember that it is **kali,** and the terminal will not show the password when you type it.*

You should see outputs like the following in the Terminal confirming that APT is now updated.

```
kali@kali:~$ sudo apt-get update
[sudo] password for kali:
Get:1 https://download.docker.com/linux/debian buster InRelease [44.4 kB]
Get:2 https://download.docker.com/linux/debian buster/stable amd64 Packages [18.7 kB]
Get:3 http://kali.download/kali kali-rolling InRelease [30.5 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 Packages [17.7 MB]
Get:5 http://kali.download/kali kali-rolling/non-free amd64 Packages [199 kB]
Get:6 http://kali.download/kali kali-rolling/contrib amd64 Packages [108 kB]
Fetched 18.1 MB in 16s (1,148 kB/s)
Reading package lists... Done
```

Let's try to install software using APT. We want to install Lynx, which a text-based browser and is the oldest web browser still maintained. Lynx has some die-hard fans, including Arash (your former unit chair). You can read more about Lynx at: https://en.wikipedia.org/wiki/Lynx_(web_browser)

To install Lynx in Kali VM using APT, run the following command:

```
sudo apt-get -y install lynx
```

You will notice that APT does all the hard work for you and installs the browser and all the required dependencies. You should see outputs like the following in the Terminal confirming successful installation of Lynx:

```
kali@kali:~$ sudo apt-get install lynx
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
The following additional packages will be installed:
  libgnutls30 libhogweed6 libnettle8 lynx-common
Suggested packages:
  gnutls-bin
The following NEW packages will be installed:
  libhogweed6 libnettle8 lynx lynx-common
The following packages will be upgraded:
  libgnutls30
1 upgraded, 4 newly installed, 0 to remove and 1661 not upgraded.
Need to get 3,770 kB of archives.
After this operation, 7,012 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://kali.download/kali kali-rolling/main amd64 libnettle8 amd64 3.7.2-3 [270 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 libhogweed6 amd64 3.7.2-3 [320 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 libgnutls30 amd64 3.7.1-3 [1,338 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 lynx-common all 2.9.0dev.6-2 [1,192 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 lynx amd64 2.9.0dev.6-2 [650 kB]
Fetched 3,770 kB in 2s (1,756 kB/s)
Reading changelogs ... Done
Selecting previously unselected package libnettle8:amd64.
(Reading database ... 273847 files and directories currently installed.)
Preparing to unpack .../libnettle8_3.7.2-3_amd64.deb ...
Unpacking libnettle8:amd64 (3.7.2-3) ...
Setting up libnettle8:amd64 (3.7.2-3) ...
Selecting previously unselected package libhogweed6:amd64.
(Reading database ... 273855 files and directories currently installed.)
Preparing to unpack .../libhogweed6_3.7.2-3_amd64.deb ...
Unpacking libhogweed6:amd64 (3.7.2-3) ...
Setting up libhogweed6:amd64 (3.7.2-3) ...
(Reading database ... 273861 files and directories currently installed.)
Preparing to unpack .../libgnutls30_3.7.1-3_amd64.deb ...
Unpacking libgnutls30:amd64 (3.7.1-3) over (3.6.11.1-2) ...
Setting up libgnutls30:amd64 (3.7.1-3) ...
Selecting previously unselected package lynx-common.
(Reading database ... 273861 files and directories currently installed.)
Preparing to unpack .../lynx-common_2.9.0dev.6-2_all.deb ...
Unpacking lynx-common (2.9.0dev.6-2) ...
Selecting previously unselected package lynx.
Preparing to unpack .../lynx_2.9.0dev.6-2_amd64.deb ...
Unpacking lynx (2.9.0dev.6-2) ...
Setting up lynx-common (2.9.0dev.6-2) ...
Setting up lynx (2.9.0dev.6-2) ...
update-alternatives: using /usr/bin/lynx to provide /usr/bin/www-browser (www-browser) in auto mode
Processing triggers for mime-support (3.64) ...
Processing triggers for libc-bin (2.29-9) ...
Processing triggers for man-db (2.9.0-2) ...
Processing triggers for kali-menu (2020.1.7) ...
```

After successful installation, to run Lynx, just type lynx in Terminal. You can enjoy browsing the web in the way it all started. *(Hint: To quit lynx, press SHIFT and q.)*

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? (Hint: "sudo apt …lynx")

Now that you know the basics of APT, we can proceed with installation of Snort IDS using APT. Kali's APT repository does not include Snort IDS. We need to make a quick adjustment and use Ubuntu's APT repository that has Snort IDS.

(see next page)

NOTE: you can access a text file with the following 3 commands. Just download the text file and copy/paste the commands from the file in your Kali VM Terminal. To download the text file, you can use any of the following links:

- Dropbox: https://www.dropbox.com/s/ldyr7z2vnvzccql/commandsforAPT.txt
- Google Drive: https://drive.google.com/file/d/1o67Wd1lAZSL1rWrSWyugguiujg8yYms_/view?usp=sharing
- CloudStor: https://cloudstor.aarnet.edu.au/plus/s/cFaCJHl55CxEGwQ

First, we want to visit "/var/lib/apt/lists" and delete all the files within the directory, leaving only the partial and auxfiles directory. For this, run the following command in Terminal:

```
sudo find /var/lib/apt/lists -type f -exec rm {} \;
```

Next, we need to download Ubuntu source.list file to /etc/apt directory:

```
sudo wget
https://gist.githubusercontent.com/ishad0w/788555191c7037e249a439542c53e170/raw/3822ba49241e6fd851ca1c1cbcc4d7e87382f484/sources.list -O
/etc/apt/sources.list
```

To communicate with the Ubuntu server, we need to add their public keys. For this, run the following command in Terminal:

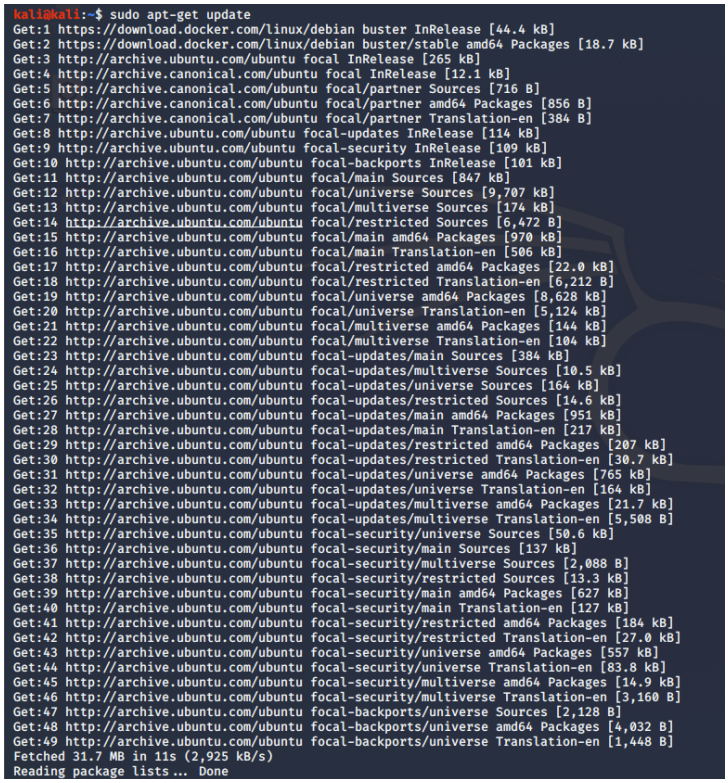
```
sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys
3B4FE6ACC0B21F32

sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys
871920D1991BC93C
```

Time to update your APT and verify if everything is OK. Run the following command in Terminal:

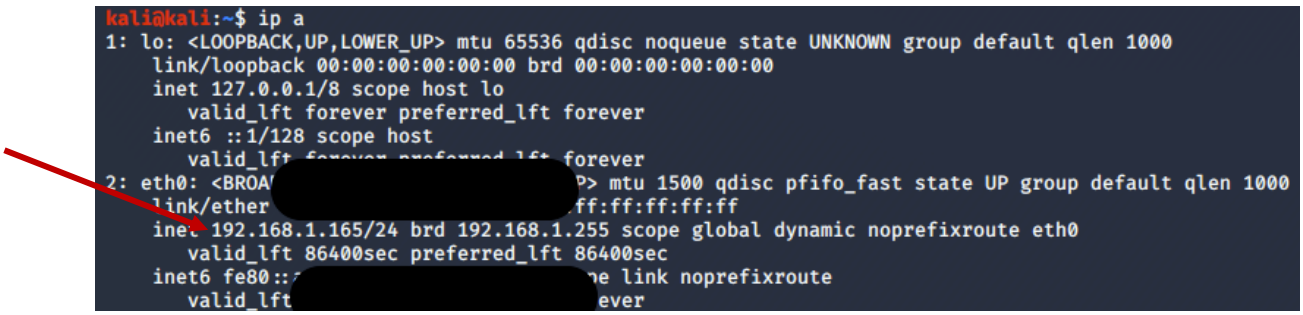
```
sudo apt-get update
```

If your changes were successfully done, you should see an output like the following in Terminal.



We are ready to install Snort IDS using APT. However, before starting the installation, you first need to make a note of your Kali VM IP. Run the following command in Terminal and make a note of your Kali VM IP.

```
ip a
```



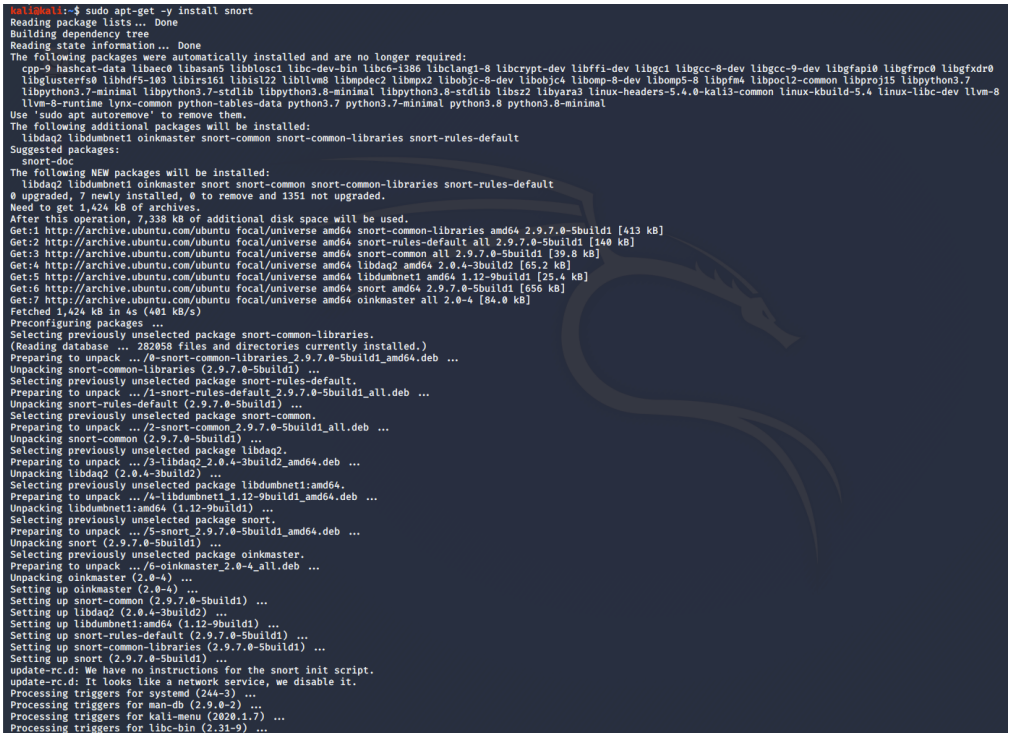
As shown in the image, my Kali VM IP is 192.168.1.165 – please note that yours will be different.

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.

Let's proceed with Snort IDS installation. Run the following command in Terminal of Kali VM:

```
sudo apt-get -y install snort
```

You will be prompted with a page (it's in blue colour) during the installation. Just press return/enter in your keyboard and let the installation proceed. Your output in Terminal should be similar to the following at the end of the installation:



You have now managed to install Snort IDS successfully.

Before running Snort, spend some time browsing through the Snort website and the available documentation: https://www.snort.org. Specifically, you may find the information available at https://www.snort.org/documents#OfficialDocumentation helpful.

The following section is extracted from [1], a comprehensive book on learning Snort and electronically available through the Deakin Library.

Overview of Snort[1]

Snort is a freeware IDS developed by Martin Roesch and Brian Caswell. It's a lightweight, network-based IDS that can be set up on a Linux or Windows host. While the core program uses a Command Line Interface (CLI), graphical user interfaces (GUIs) can also be used. Snort operates as a network sniffer and logs activity that matches predefined signatures. Signatures can be designed for a wide range of traffic, including Internet Protocol (IP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

Snort consists of two basic parts:

- Header Where the rules "actions" are identified
- Options Where the rules "alert messages" are identified

Overview of Snort rules[2]

Snort matches the captured packets with a set of rules that the administrator provides. The rules reside in simple ASCII text files and can be modified as needed. It is possible to comment out existing rules to eliminate false positive matches. It is also possible to craft a new rule to spot a new intrusion or a network activity of interest to the administrator of the Snort system. For instance, imagine that you want to be alerted when the user with the userid "ImaTerrorist" logs in to the Post Office Protocol (POP) server to check his or her mail. A Snort rule could be inserted into the pop3.rules file in the /etc/snort/rules directory on the Snort machine:

```
#--------------
# POP3 RULES
#--------------

alert tcp $HOME_NET any -> $HOME_NET 110 (msg:"Bad Guy Mail Check";\
flow:to_server,established; content:"USER ImaTerrorist"; nocase;)
```

[1] Extracted from Chapter 1 of [1].
[2] Extracted from Chapter 5 of [1] with amendments in text.

Upon encountering a packet that meets those criteria, the content is examined to see if user "ImaTerrorist" is logging in. If the rule matches, an alert is generated.

In Section 2 of this task, you will learn more Snort Rules. For the time being, let's try to run Snort using a basic rule.

Configuring "Snort.conf"

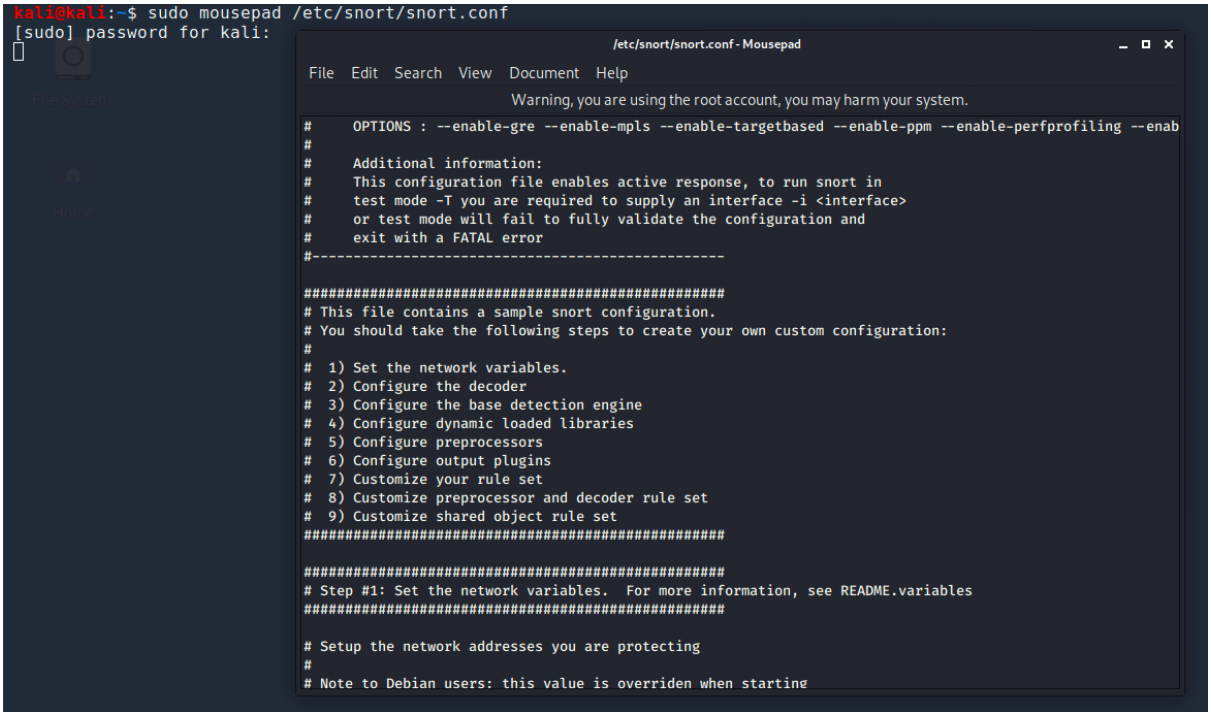
The snort.conf file controls everything about what Snort watches, how it defends itself from attack, what rules it uses to find malicious traffic, and even how it watches for potentially dangerous traffic that isn't defined by a signature.

Snort configuration file is available at /etc/snort/snort.conf. To access this file using Kali's built-in editor run the following command in Terminal:

```
sudo mousepad /etc/snort/snort.conf
```

Hint: when prompted for password after running commands with escalated privilege, use ***kali****.*

You should be shown the snort.conf file similar to the following screenshot:

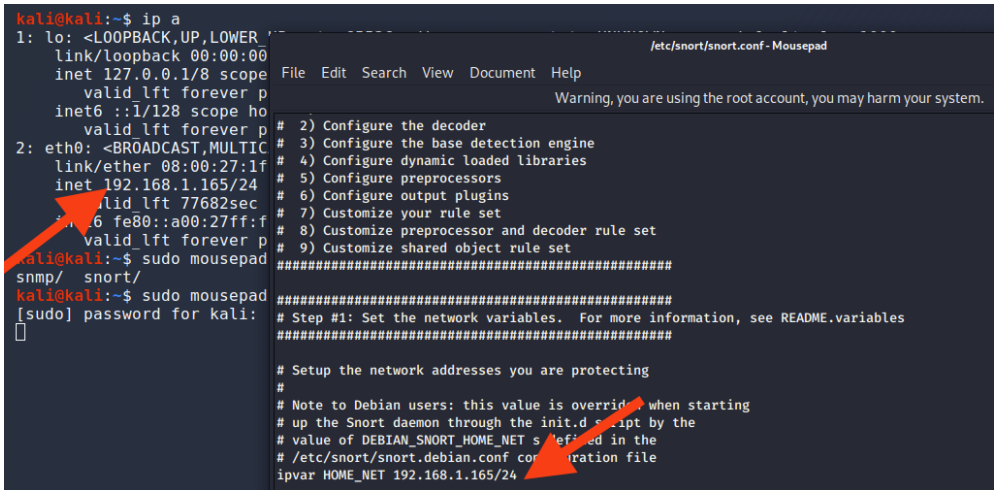


You will notice that the Snort.conf file has 9 sections. In this task, we will need to make the following 3 changes to Snort.conf before being able to test Snort in this case.

1. Setting a value for HOME_NET (in Step 1 of Snort.config file)
2. Disabling all existing rules (in Step 7 of Snort.config file)
3. Adding a custom rule (in Step 7 of Snort.config file)

Setting a value for HOME_NET (in Step 1 of Snort.config file)

Scroll to Step 1 in Snort.config file. Replace "any" with the value for IP that you retrieved in Q3. For instance, in the following screenshot, I have changed "any" to IP value 192.168.1.165/24, which is the IP for my Kali VM. Save the file after adding the IP (File > Save or CTRL+S)



Disabling all existing rules (in Step 7 of Snort.config file)

Scroll to Section 7 of Snort.conf file and comment **all** the rules by adding "#" at the start of each line stating with "include".

For instance, "include $RULE_PATH/app-detect.rules" needs to be updated to "#include $RULE_PATH/app-detect.rules". You will need to ensure that all rules are commented in Section 7 (up to start of Section 8). After you have commented all the rules in Section 7, save the file and exit.

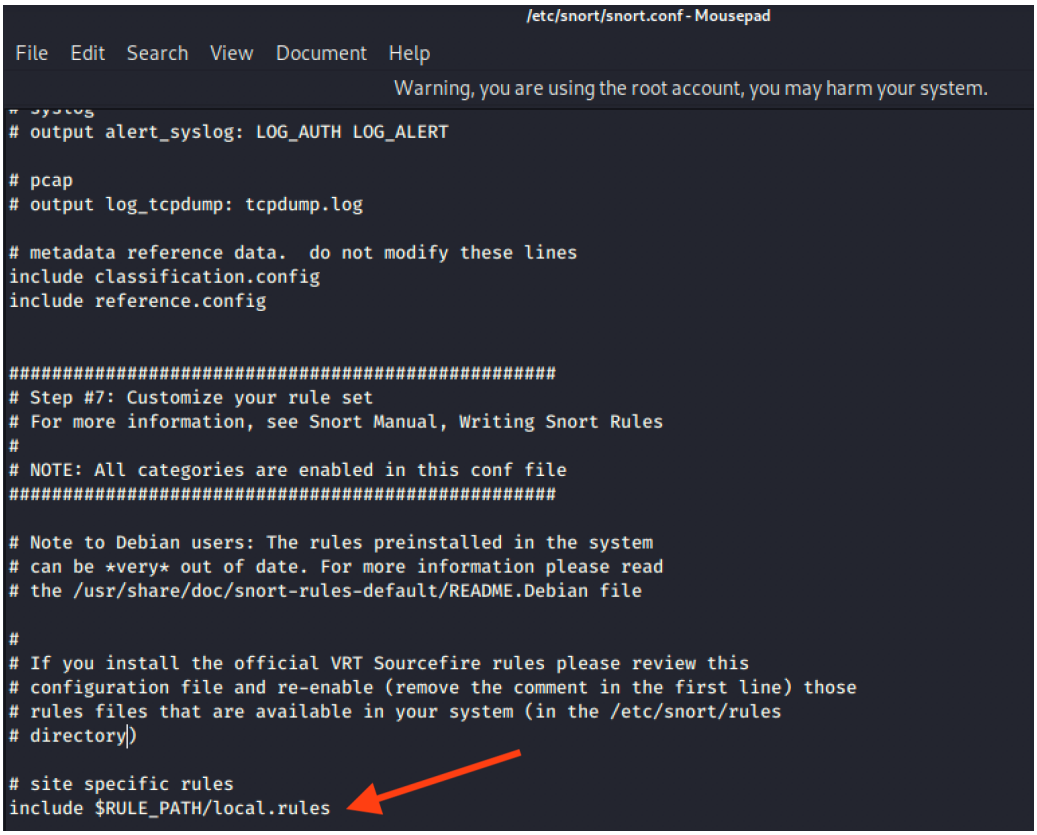
```
#include $RULE_PATH/attack-responses.rules
#include $RULE_PATH/backdoor.rules
#include $RULE_PATH/bad-traffic.rules
#include $RULE_PATH/blacklist.rules
#include $RULE_PATH/botnet-cnc.rules
#include $RULE_PATH/browser-chrome.rules
#include $RULE_PATH/browser-firefox.rules
#include $RULE_PATH/browser-ie.rules
#include $RULE_PATH/browser-other.rules
#include $RULE_PATH/browser-plugins.rules
#include $RULE_PATH/browser-webkit.rules
#include $RULE_PATH/chat.rules
#include $RULE_PATH/content-replace.rules
#include $RULE_PATH/ddos.rules
#include $RULE_PATH/dns.rules
#include $RULE_PATH/dos.rules
#include $RULE_PATH/experimental.rules
#include $RULE_PATH/exploit-kit.rules
#include $RULE_PATH/exploit.rules
#include $RULE_PATH/file-executable.rules
#include $RULE_PATH/file-flash.rules
#include $RULE_PATH/file-identify.rules
```

Adding a custom rule (in Step 7 of Snort.config file)

Re-open the Snort.config file by running the following command in Terminal:

```
sudo mousepad /etc/snort/snort.conf
```

Scroll to Step 7 and locate "include $RULE_PATH/local.rules" and uncomment it by removing # (see the following screenshot). This will allow defining custom rules in "local.rules" file.



Save the file after change and close it.

Now, we need to open "local.rules" and our custom rule to see Snort IDS in action. For this, run the following command in Terminal:

```
sudo mousepad /etc/snort/rules/local.rules
```

The file is currently empty. We will now add the following basic rule to it. This rule triggers an alert whenever a TCP connected is detected.

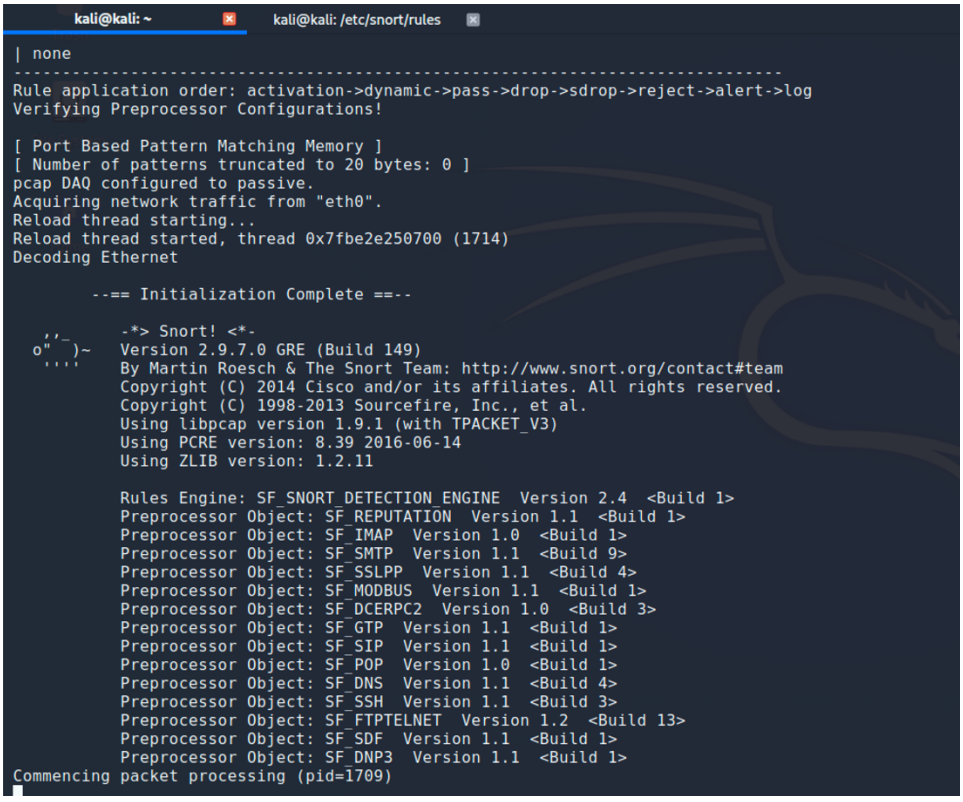
```
alert tcp any any -> any any (msg:"TCP Connection
Detected!"; sid:100006927; rev:1;)
```

Save the file after adding the rule and close it. You will know more about Snort IDS rules after completing the next part of this task.

Start Snort IDS by running the following command in Terminal:

```
sudo snort -d -l /var/log/snort/ -A console -c
/etc/snort/snort.conf
```

You should get a confirmation that Snort is up and running similar to the following screenshot:



Leave the Terminal with Snort running. Run "Web Browser" in Kali VM and access Google.com.

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.

Section B:

In this section, you will need to answer questions that require understanding Snort rules. To understand Snort rules and answer the questions, you need to refer to Snort's official documentation and user manual and study Snort rule basics on your own:

- Snort Documentation: https://www.snort.org/documents#OfficialDocumentation
- Snort User Manual: http://manual-snort-org.s3-website-us-east-1.amazonaws.com

You can also find a range of online resources that may help you further for this. [1] is a textbook that is accessible through Deakin library. The following may also be useful resources:

- https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2016/pdf/DevNet-1693.pdf
- https://paginas.fe.up.pt/~mgi98020/pgr/writing_snort_rules.htm

After your research and exploration, you may still have some doubts about Snort rules. You can seek help from tutors in practicals (online or on-campus) with your specific questions about Snort rules.

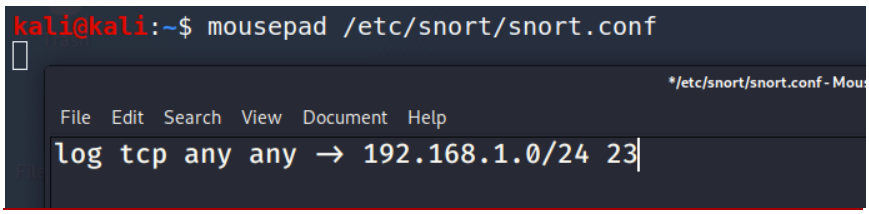
Please note that the final exam will include questions similar to questions in Section B of this document.

(see next page)

Q5: Consider the following Snort rule:

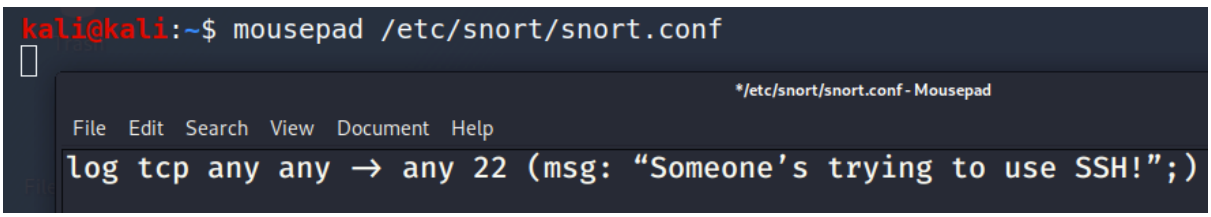
A. What protocol is this rule applied to?
B. What traffic is monitored? *(include source, destination, ports, and directions)*
C. What is the rule action?
D. What does **msg: "IP Packet detected"** do in this rule?
E. What is the meaning of **sid:1000002** in this rule?
F. What is the meaning of **rev:0** in this rule?

Q6: Consider the following Snort rule:



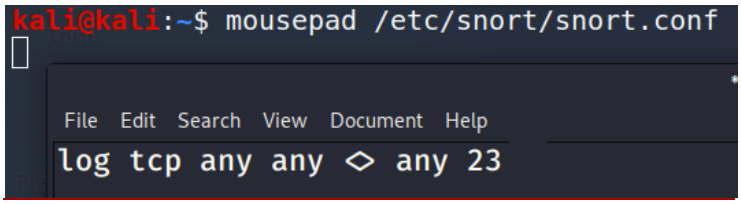
A. What protocol is this rule applied to?
B. What traffic is monitored? *(include source, destination, ports, and directions)*
C. What is the rule action?
D. Does this rule have a rule option argument?

Q7: Consider the following Snort rule:



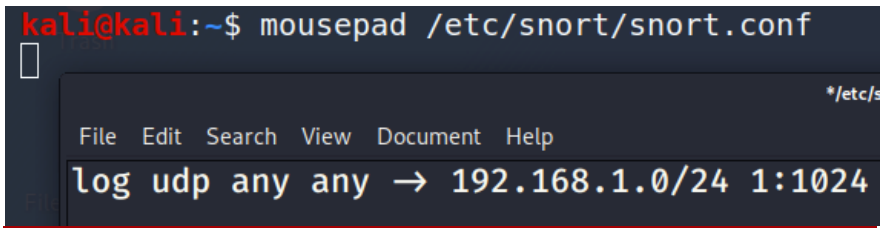
A. What protocol is this rule applied to?
B. What traffic is monitored? *(include source, destination, ports, and directions)*
C. What is the rule action?

Q8: Consider the following Snort rule:



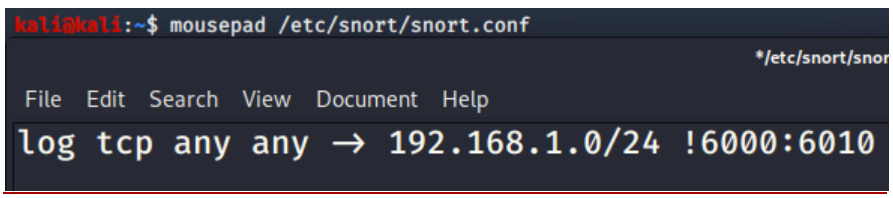
A. What protocol is this rule applied to?
B. What traffic is monitored? *(include source, destination, ports, and directions)*
C. What is the rule action?

Q9: Consider the following Snort rule:



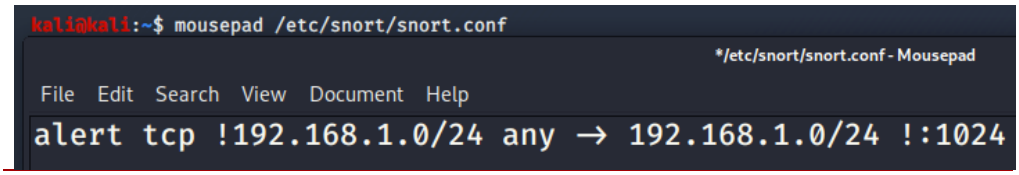
A. What protocol is this rule applied to?
B. What traffic is monitored? *(include source, destination, ports, and directions)*
C. What is the rule action?

Q10: Consider the following Snort rule:



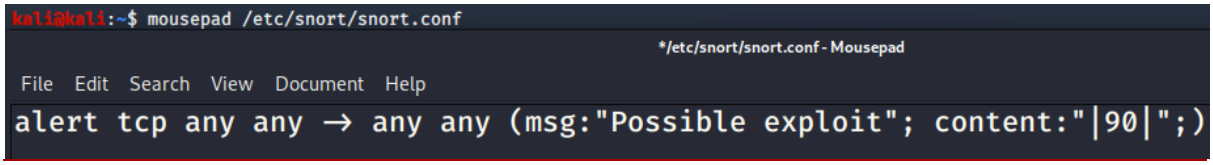
A. What protocol is this rule applied to?
B. What traffic is monitored? *(include source, destination, ports, and directions)*
C. What is the rule action?
D. What is the meaning of "!6000:6010" in this rule?

Q11: Consider the following Snort rule:



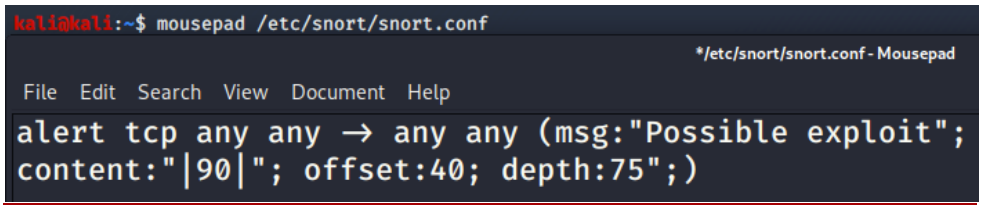
A. What protocol is this rule applied to?
B. What traffic is monitored? *(include source, destination, ports, and directions)*
C. What is the rule action?
D. What is the meaning of "**!192.168.1.0/24**" in this rule?

Q12: Consider the following Snort rule:



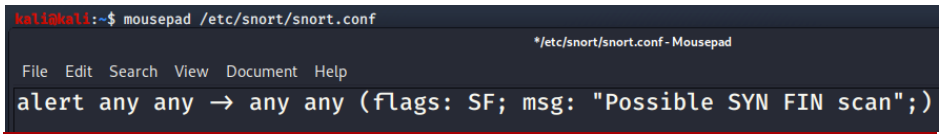
A. What protocol is this rule applied to?
B. What traffic is monitored? *(include source, destination, ports, and directions)*
C. What is the rule action?
D. What is the meaning of **content:"|90|"** in this rule?

Q13: Consider the following Snort rule:



A. What protocol is this rule applied to?
B. What traffic is monitored? *(include source, destination, ports, and directions)*
C. What is the rule action?
D. What is the meaning of "**offset:40**" in this rule?
E. What is the meaning of "**depth:75**" in this rule?

Q14: Consider the following Snort rule:



A. What protocol is this rule applied to?
B. What traffic is monitored? *(include source, destination, ports, and directions)*
C. What is the rule action?
D. What is the meaning of "**flags: SF**" in this rule?

Q15: Consider the following Snort rule:

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

Q16: Next week is the final week of tasks in SIT182. It's a good time to reflect on your journey thus far in SIT182. Think about all the different tasks you have completed and all the hands-on skills you have learned. Similar to other pass-tasks, this question is just a reflection point. How did this task complement the theoretical concepts covered about IDS and IPS? How did you learn about Snort rules to complete questions in Section B of this task?

References:

[1]: Michael Gregg, Stephen Watkins, George Mays, Chris Ries, Ronald M. Bandes & Brandon Franklin 2006, Hack the Stack : Using Snort and Ethereal to Master The 8 Layers of An Insecure Network, Syngress, Rockland, MA, viewed 30 April 2021, https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=174832&authtype=sso&custid=deakin&site=eds-live&scope=site