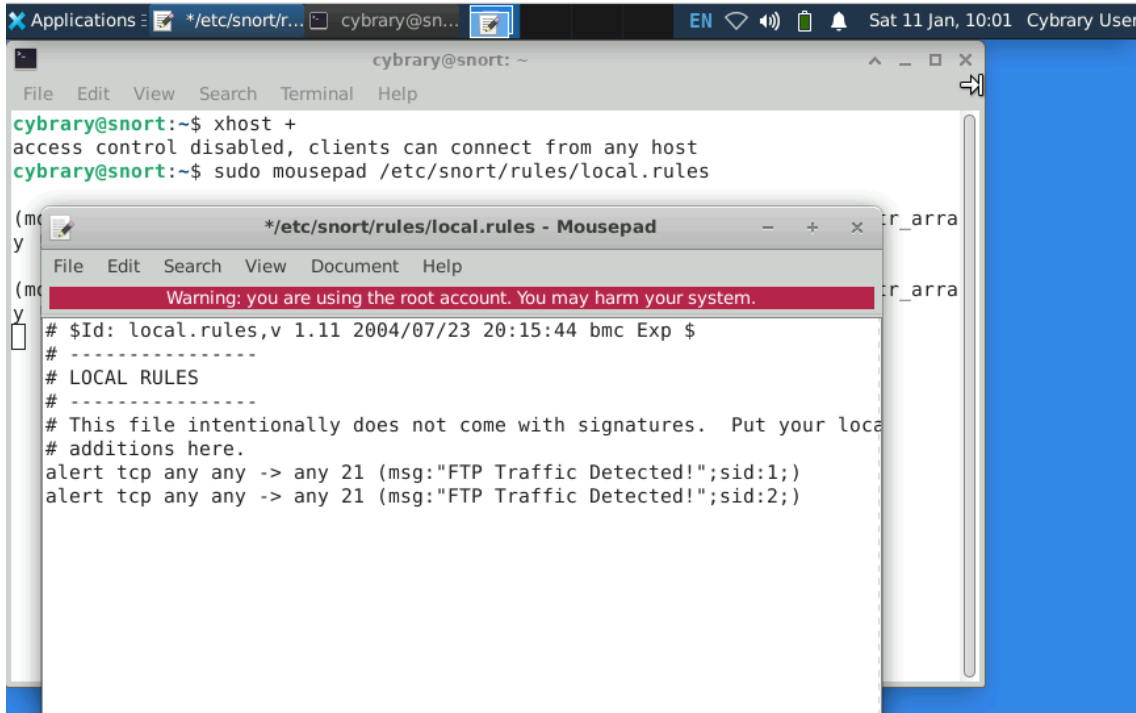


CodeAlpha Task 2

Step 2: Writing Snort Rules. In this step, custom rules are defined in the 'local.rules' file.

These rules are configured to detect FTP traffic on port 21 and log the events.



The screenshot shows a Linux desktop environment. In the background, a terminal window titled 'cybrary@snort: ~' displays the following commands and output:

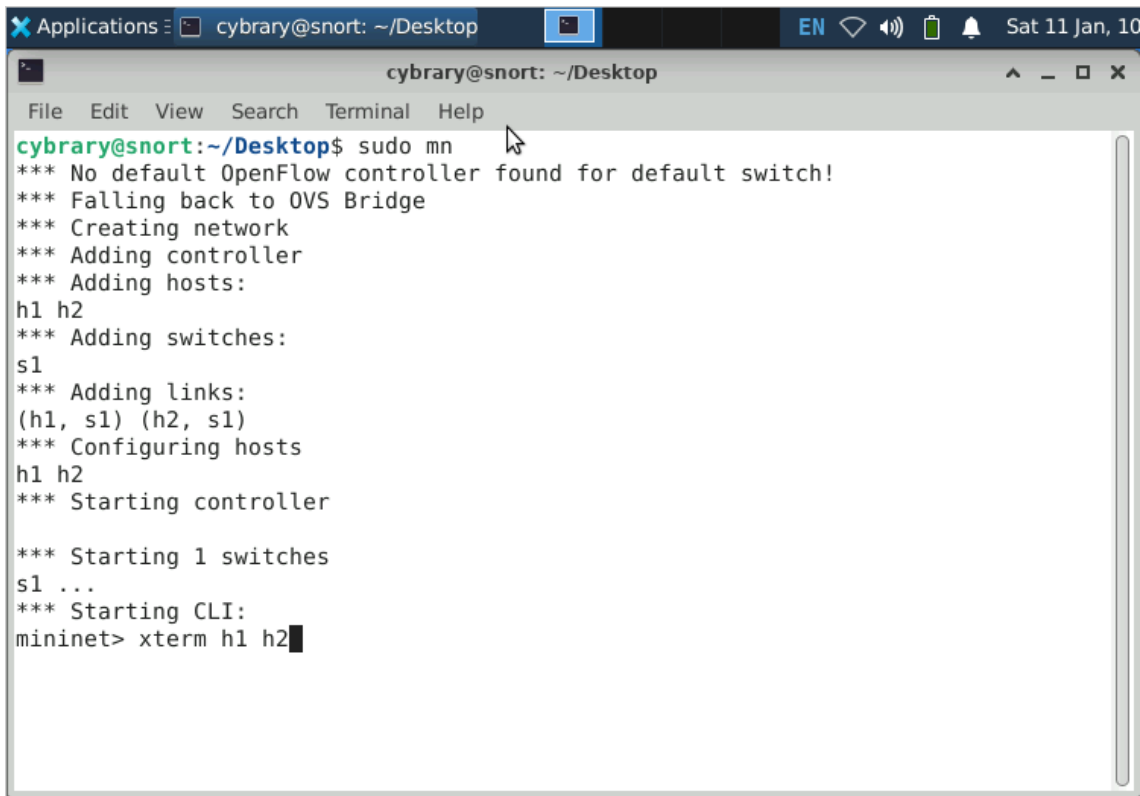
```
cybrary@snort:~$ xhost +
access control disabled, clients can connect from any host
cybrary@snort:~$ sudo mousepad /etc/snort/rules/local.rules
```

In the foreground, a 'Mousepad' window titled '*etc/snort/rules/local.rules - Mousepad' is open. It shows the content of the 'local.rules' file, which includes a warning banner and two custom rules for detecting FTP traffic on port 21:

```
Warning: you are using the root account. You may harm your system.

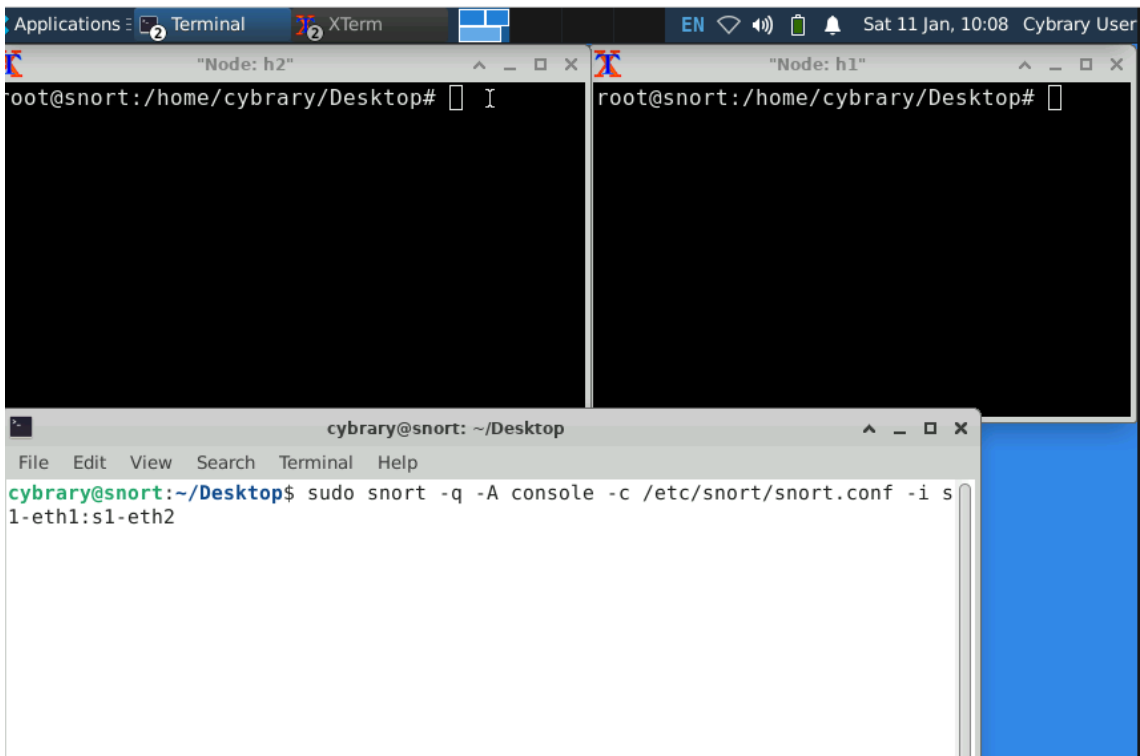
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# -----
# LOCAL RULES
# -----
# This file intentionally does not come with signatures. Put your local
# additions here.
alert tcp any any -> any 21 (msg:"FTP Traffic Detected!";sid:1;)
alert tcp any any -> any 21 (msg:"FTP Traffic Detected!";sid:2;)
```

Step 1: Setting up Mininet. This step shows the creation of a virtual network using the Mininet CLI. Hosts (h1, h2) and a switch (s1) are added to establish the testing environment.



```
cybrary@snort: ~/Desktop
File Edit View Search Terminal Help
cybrary@snort:~/Desktop$ sudo mn
*** No default OpenFlow controller found for default switch!
*** Falling back to OVS Bridge
*** Creating network
*** Adding controller
*** Adding hosts:
h1 h2
*** Adding switches:
s1
*** Adding links:
(h1, s1) (h2, s1)
*** Configuring hosts
h1 h2
*** Starting controller
*** Starting 1 switches
s1 ...
*** Starting CLI:
mininet> xterm h1 h2
```

Step 3: Starting Snort. Snort is launched in IDS mode using the appropriate configuration file. It monitors traffic on the specified network interface for rule violations.



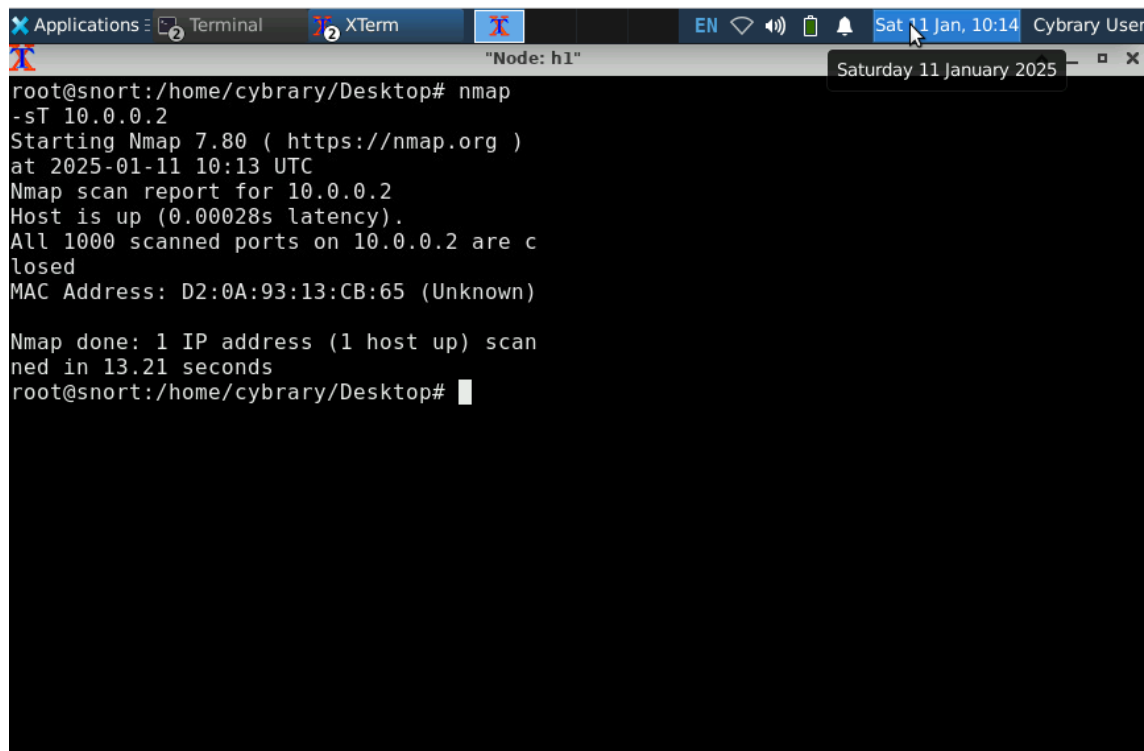
```
Applications: 2 Terminal 2 XTerm
Sat 11 Jan, 10:08 Cybrary User

"Node: h2"
root@snort:/home/cybrary/Desktop# I

"Node: h1"
root@snort:/home/cybrary/Desktop#

cybrary@snort: ~/Desktop
File Edit View Search Terminal Help
cybrary@snort:~/Desktop$ sudo snort -q -A console -c /etc/snort/snort.conf -i s1-eth1-s1-eth2
```

Step 4: Conducting an Nmap Scan. An Nmap scan is performed on the target host (10.0.0.2). This generates network traffic that will trigger Snort rules if matched.



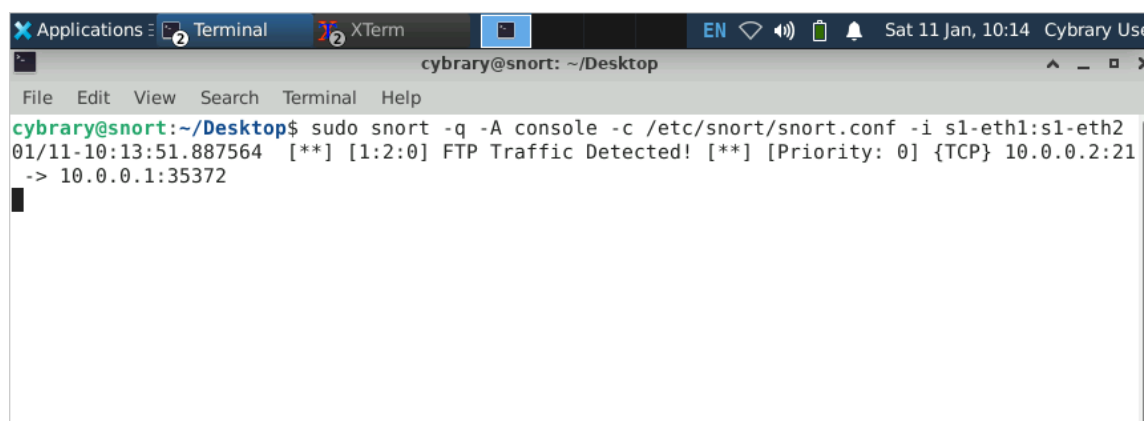
A terminal window titled "Node: h1" showing the output of an Nmap scan. The user is root@snort:/home/cybrary/Desktop. The command 'nmap -sT 10.0.0.2' is executed. The output shows that the host is up with a latency of 0.00028s and that all 1000 scanned ports are closed. The MAC address is D2:0A:93:13:CB:65 (Unknown). The scan took 13.21 seconds.

```
root@snort:/home/cybrary/Desktop# nmap
-sT 10.0.0.2
Starting Nmap 7.80 ( https://nmap.org )
at 2025-01-11 10:13 UTC
Nmap scan report for 10.0.0.2
Host is up (0.00028s latency).
All 1000 scanned ports on 10.0.0.2 are closed
MAC Address: D2:0A:93:13:CB:65 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 13.21 seconds
root@snort:/home/cybrary/Desktop#
```

Step 5: Detecting FTP Traffic. Snort successfully detects FTP traffic as defined in the rules.

The alert is displayed in the console, confirming that the setup is working correctly.



A terminal window titled "cybrary@snort: ~/Desktop" showing the output of a Snort command. The user is cybrary@snort. The command 'sudo snort -q -A console -c /etc/snort/snort.conf -i s1-eth1:s1-eth2' is executed. The output shows an alert for FTP traffic detected from 10.0.0.2 to 10.0.0.1:35372.

```
cybrary@snort:~/Desktop$ sudo snort -q -A console -c /etc/snort/snort.conf -i s1-eth1:s1-eth2
01/11-10:13:51.887564  [**] [1:2:0] FTP Traffic Detected! [**] [Priority: 0] {TCP} 10.0.0.2:21
-> 10.0.0.1:35372
```