OS PROJECT:

NETWORK TRAFFIC ANALYZER

My Journey in Network Monitoring and GUI Development

JOHN NWEKE

Introduction

Objective:

- Develop a network traffic analyzer using **Scapy** and **tcpdump**.
- Implement a **GUI** using **Tkinter** for better usability.

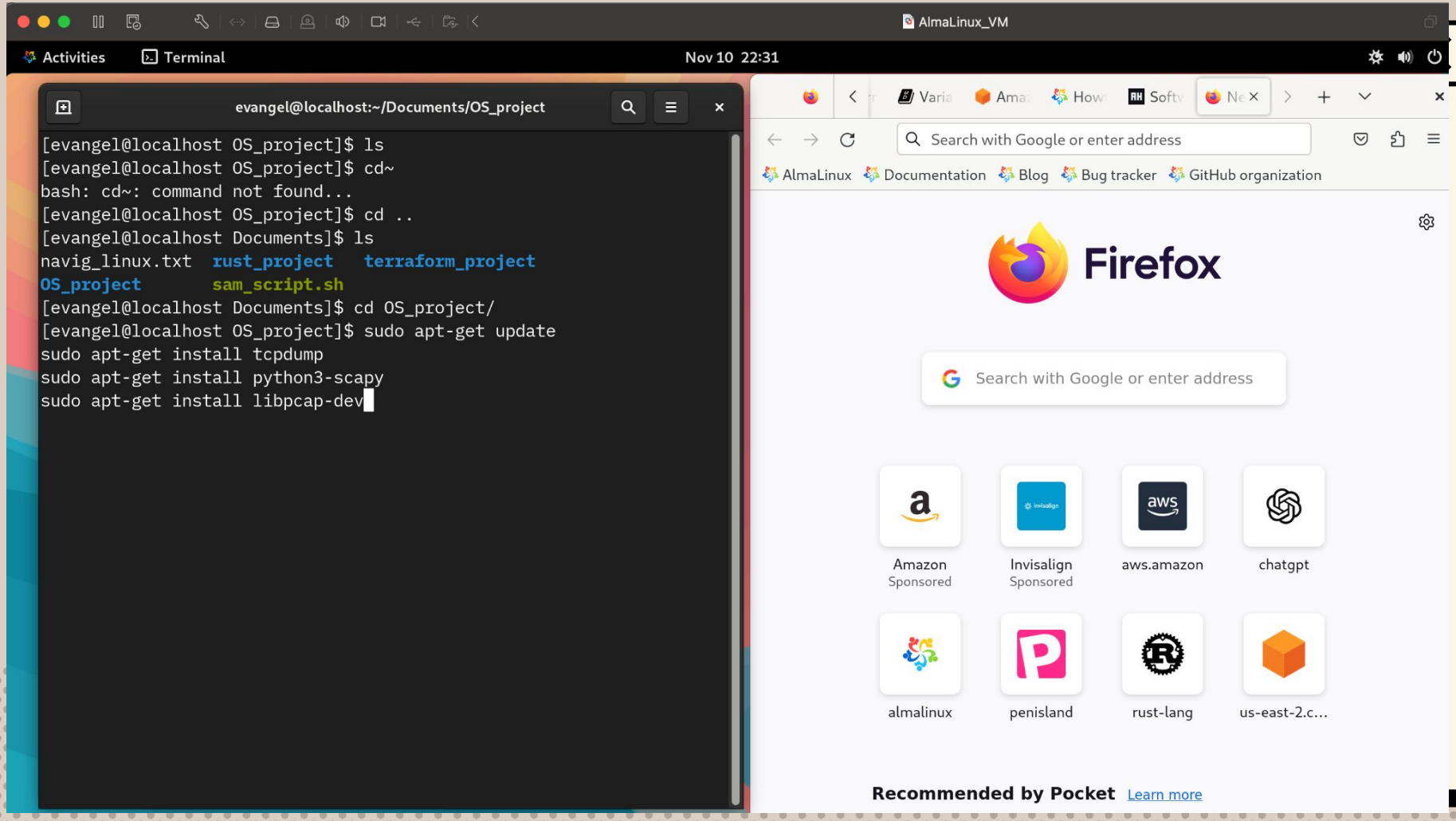
Key Components:

- Linux environment (AlmaLinux 9 - fork of RHEL/CentOS)
- Python-based packet analysis

Initial Setup

What I did:

- Installed required packages using `dnf`
- Faced errors due to missing network connectivity.


AlmaLinux_VM
Activities
Terminal
Nov 10 22:31
evangel@localhost:~/Documents/OS_project
[evangel@localhost OS_project]$ ls
[evangel@localhost OS_project]$ cd~
bash: cd~: command not found...
[evangel@localhost OS_project]$ cd ..
[evangel@localhost Documents]$ ls
navig_linux.txt rust_project terraform_project
OS_project sam_script.sh
[evangel@localhost Documents]$ cd OS_project/
[evangel@localhost OS_project]$ sudo apt-get update
sudo apt-get install tcpdump
sudo apt-get install python3-scapy
sudo apt-get install libpcap-dev
Search with Google or enter address
AlmaLinux
Documentation
Blog
Bug tracker
GitHub organization
Firefox
Search with Google or enter address
Amazon
Sponsored
Invisalign
Sponsored
aws.amazon
chatgpt
almalinux
penisland
rust-lang
us-east-2.c...
Recommended by Pocket
Learn more

Network Challenges

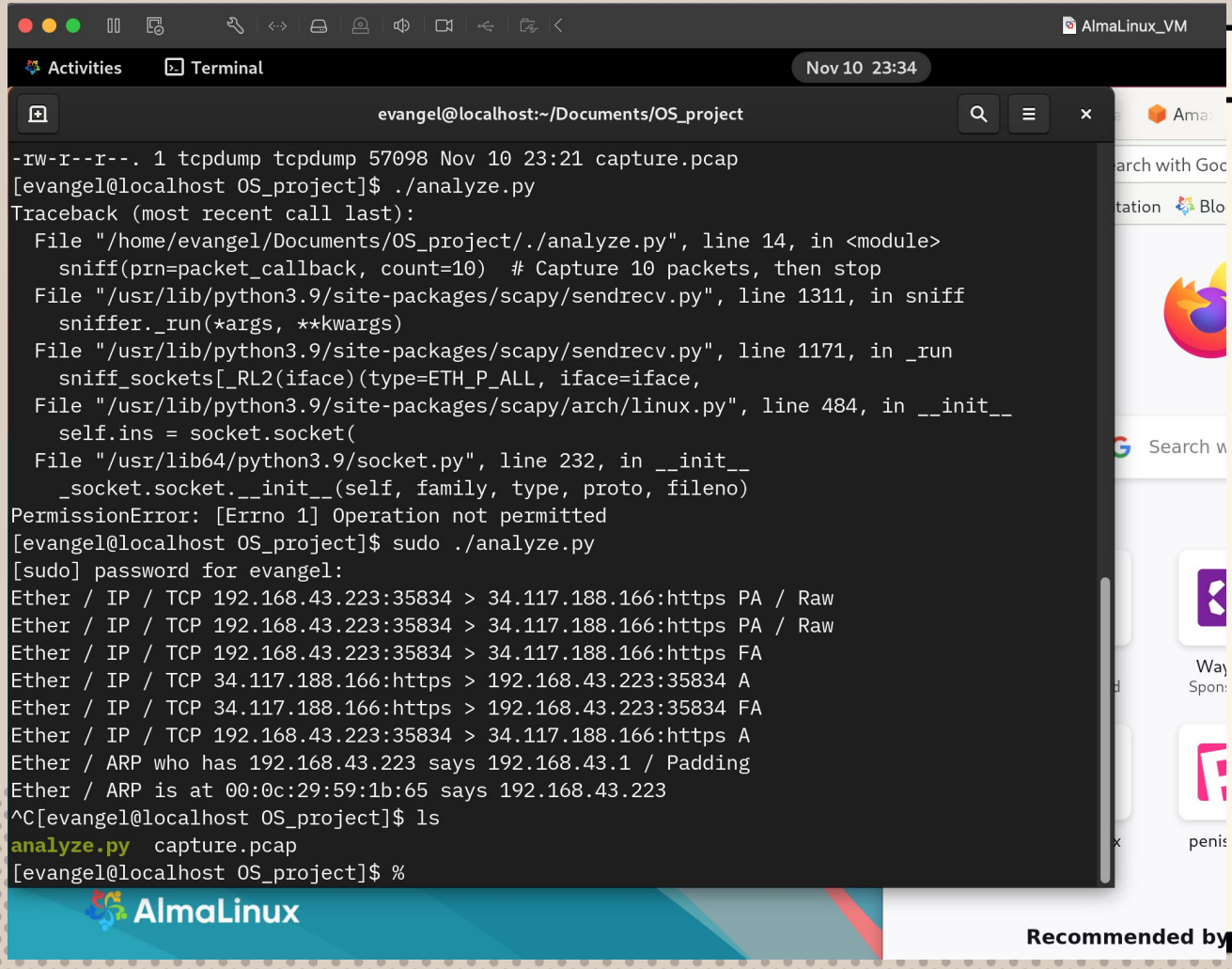
What I did:

- Error while downloading metadata for AlmaLinux repositories.
- Debugged using ping to check internet connectivity:

```
ping -c 4 8.8.8.8
```

Solution:

- Switched from Towson Wi-Fi to mobile hotspot.
- Configured VM to use a bridged network adapter.


AlmaLinux_VM
Activities
Terminal
Nov 10 23:34
evangel@localhost:~/Documents/OS_project
-rw-r--r--. 1 tcpdump tcpdump 57098 Nov 10 23:21 capture.pcap
[evangel@localhost OS_project]$ ./analyze.py
Traceback (most recent call last):
File "/home/evangel/Documents/OS_project/./analyze.py", line 14, in <module>
sniff(prn=packet_callback, count=10) # Capture 10 packets, then stop
File "/usr/lib/python3.9/site-packages/scapy/sendrecv.py", line 1311, in sniff
sniffer._run(*args, **kwargs)
File "/usr/lib/python3.9/site-packages/scapy/sendrecv.py", line 1171, in _run
sniff_sockets[_RL2(iface)(type=ETH_P_ALL, iface=iface,
File "/usr/lib/python3.9/site-packages/scapy/arch/linux.py", line 484, in __init__
self.ins = socket.socket(
File "/usr/lib64/python3.9/socket.py", line 232, in __init__
_socket.socket.__init__(self, family, type, proto, fileno)
PermissionError: [Errno 1] Operation not permitted
[evangel@localhost OS_project]$ sudo ./analyze.py
[sudo] password for evangel:
Ether / IP / TCP 192.168.43.223:35834 > 34.117.188.166:https PA / Raw
Ether / IP / TCP 192.168.43.223:35834 > 34.117.188.166:https PA / Raw
Ether / IP / TCP 192.168.43.223:35834 > 34.117.188.166:https FA
Ether / IP / TCP 34.117.188.166:https > 192.168.43.223:35834 A
Ether / IP / TCP 34.117.188.166:https > 192.168.43.223:35834 FA
Ether / IP / TCP 192.168.43.223:35834 > 34.117.188.166:https A
Ether / ARP who has 192.168.43.223 says 192.168.43.1 / Padding
Ether / ARP is at 00:0c:29:59:1b:65 says 192.168.43.223
^C[evangel@localhost OS_project]$ ls
analyze.py capture.pcap
[evangel@localhost OS_project]$ %
AlmaLinux
Recommended by

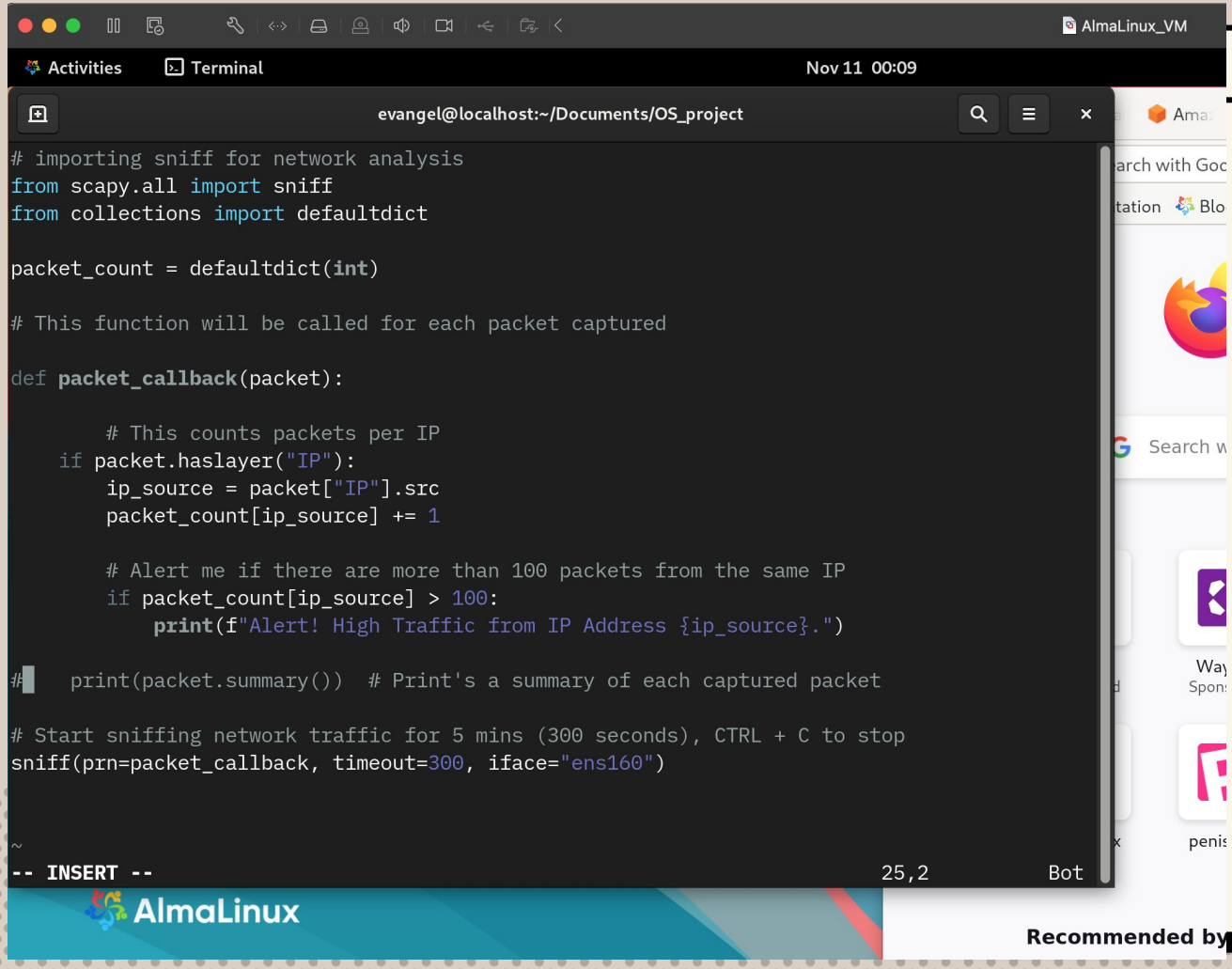
Dependency Challenges

Challenge:

- libpcap wasn’t available by default.
- Pcap file is where raw, low-level network data is stored (Pcap = Packet Capture)

Solution:

- Enabled crb (CodeReady Builder/PowerTools) repository:
  `sudo dnf config-manager --set-enabled crb`
- Successfully installed libpcap.


AlmaLinux_VM
Activities
Terminal
Nov 11 00:09
evangel@localhost:~/Documents/OS_project
# importing sniff for network analysis
from scapy.all import sniff
from collections import defaultdict
packet_count = defaultdict(int)
# This function will be called for each packet captured
def packet_callback(packet):
# This counts packets per IP
if packet.haslayer("IP"):
ip_source = packet["IP"].src
packet_count[ip_source] += 1
# Alert me if there are more than 100 packets from the same IP
if packet_count[ip_source] > 100:
print(f"Alert! High Traffic from IP Address {ip_source}.")
# print(packet.summary()) # Print's a summary of each captured packet
# Start sniffing network traffic for 5 mins (300 seconds), CTRL + C to stop
sniff(prn=packet_callback, timeout=300, iface="ens160")
~
-- INSERT --
25,2
Bot
AlmaLinux
Recommended by

Analyzing Traffic

Using tcpdump:

- Captured network traffic and saved it to a pcap file

```
sudo tcpdump -i any -w capture.pcap
```

Packet Analysis with Scapy:

- Developed a Python script to analyze packets and log suspicious IP activity.

Interface Config

Identified Network Interfaces:

Used `ip link show` to find active interfaces:

`Loopback: lo`

`Ethernet: ens160`

Optimization:

Specified `ens160` for monitoring.

Automated script execution with `shebang` and `chmod +x:`

```
[evangel@localhost OS_project]$ cd ..
[evangel@localhost Documents]$ ls
navig_linux.txt  OS_project  rust_project  sam_script.sh  terraform_project
[evangel@localhost Documents]$ mkdir "OS_project_2"
[evangel@localhost Documents]$ ls
navig_linux.txt  OS_project  OS_project_2  rust_project  sam_script.sh  terraform_proj
[evangel@localhost Documents]$ cd OS_project_2/
[evangel@localhost OS_project_2]$ ls
[evangel@localhost OS_project_2]$ touch network_analyzer.py
[evangel@localhost OS_project_2]$ vim network_analyzer.py
[evangel@localhost OS_project_2]$ ls
network_analyzer.py
[evangel@localhost OS_project_2]$ chmod +x network_analyzer.py
[evangel@localhost OS_project_2]$ ls -tharl
total 4.0K
drwxr-xr-x. 6 evangel evangel  133 Dec  3 16:11 ..
-rwxr-xr-x. 1 evangel evangel 2.3K Dec  3 16:15 network_analyzer.py
drwxr-xr-x. 2 evangel evangel   33 Dec  3 16:15 .
[evangel@localhost OS_project_2]$ %
```

Adding a GUI

Professor's Feedback:

Requested GUI for user-friendly alerts, but AlmaLinux doesn't natively support GUIs.

Solution:

Had to Install GUI dependencies and integrate Tkinter.

```
Dependencies resolved.
================================================================================
 Package                    Architecture        Version                 Repository              Size
================================================================================
Installing:
 python3-tkinter            x86_64              3.9.19-8.el9_5.1        appstream              309 k
Upgrading:
 python-unversioned-command noarch              3.9.19-8.el9_5.1        appstream              9.0 k
 python3                    x86_64              3.9.19-8.el9_5.1        baseos                  26 k
 python3-libs               x86_64              3.9.19-8.el9_5.1        baseos                 7.5 M
Installing dependencies:
 tk                         x86_64              1:8.6.10-9.el9          appstream              1.6 M

Transaction Summary
================================================================================
Install  2 Packages
Upgrade  3 Packages

Total download size: 9.4 M
Is this ok [y/N]: y
Downloading Packages:
(1/5): python-unversioned-command-3.9.19-8.el9_5.1.noarch.rpm  159 kB/s | 9.0 kB     00:00
(2/5): python3-3.9.19-8.el9_5.1.x86_64.rpm                     294 kB/s |  26 kB     00:00
(3/5): python3-tkinter-3.9.19-8.el9_5.1.x86_64.rpm             886 kB/s | 309 kB     00:00
(4/5): tk-8.6.10-9.el9.x86_64.rpm                              1.5 MB/s | 1.6 MB     00:01
(5/5): python3-libs-3.9.19-8.el9_5.1.x86_64.rpm                3.0 MB/s | 7.5 MB     00:02
--------------------------------------------------------------------------------
```

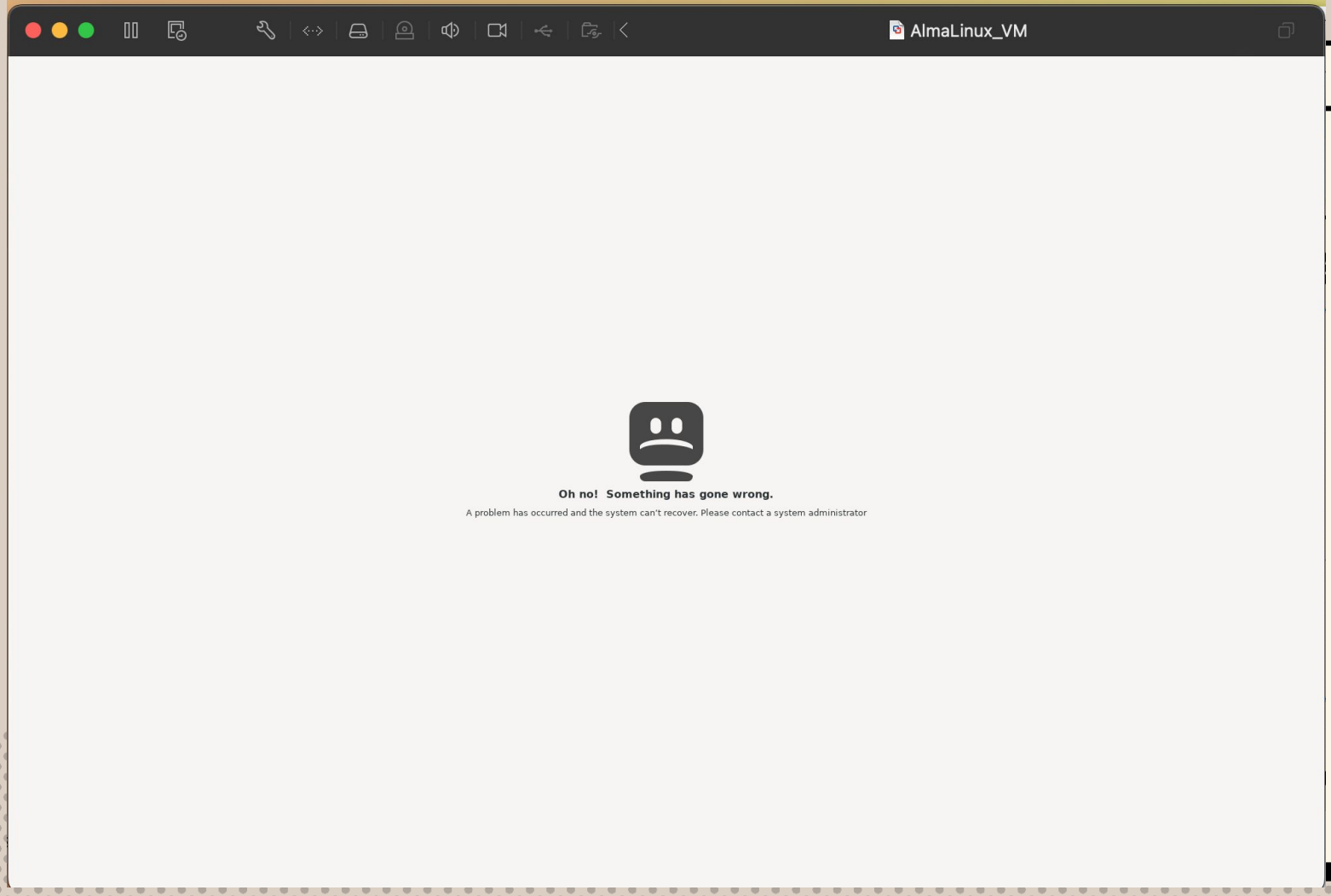
```
Traceback (most recent call last):
  File "/home/evangel/Documents/OS_project_2/./network_analyzer.py", line 65, in <module>
    root = tk.Tk()
  File "/usr/lib64/python3.9/tkinter/__init__.py", line 2270, in __init__
    self.tk = _tkinter.create(screenName, baseName, className, interactive, wantobjects, useTk, sync, use)
_tkinter.TclError: no display name and no $DISPLAY environment variable
[evangel@localhost OS_project_2]$ sudo dnf groupinstall "Server with GUI"
Last metadata expiration check: 0:05:11 ago on Tue 03 Dec 2024 04:19:02 PM EST.
Dependencies resolved.
```

Package	Architecture	Version	Repository	Size
Upgrading:				
NetworkManager	x86_64	1:1.48.10-2.el9_5.alma.1	baseos	2.3 M
NetworkManager-adsl	x86_64	1:1.48.10-2.el9_5.alma.1	baseos	34 k
NetworkManager-bluetooth	x86_64	1:1.48.10-2.el9_5.alma.1	baseos	61 k
NetworkManager-config-server	noarch	1:1.48.10-2.el9_5.alma.1	baseos	20 k
NetworkManager-libnm	x86_64	1:1.48.10-2.el9_5.alma.1	baseos	1.8 M
NetworkManager-team	x86_64	1:1.48.10-2.el9_5.alma.1	baseos	40 k
NetworkManager-tui	x86_64	1:1.48.10-2.el9_5.alma.1	baseos	247 k
NetworkManager-wifi	x86_64	1:1.48.10-2.el9_5.alma.1	baseos	82 k
NetworkManager-wwan	x86_64	1:1.48.10-2.el9_5.alma.1	baseos	68 k
almalinux-gpg-keys	x86_64	9.5-1.el9	baseos	9.5 k
almalinux-release	x86_64	9.5-1.el9	baseos	20 k
almalinux-repos	x86_64	9.5-1.el9	baseos	9.6 k
alsa-lib	x86_64	1.2.12-1.el9	appstream	504 k
alsa-ucm	noarch	1.2.12-1.el9	appstream	150 k

Virtual Machine Crashed

Virtual Machine Crashed after installing GUI dependencies on AlmaLinux

Didn’t cuss tho


AlmaLinux_VM
Oh no! Something has gone wrong.
A problem has occurred and the system can't recover. Please contact a system administrator

Pivot to Use MacOS

Like any good Carnie says: “The Show must Go on.”

Final Solution

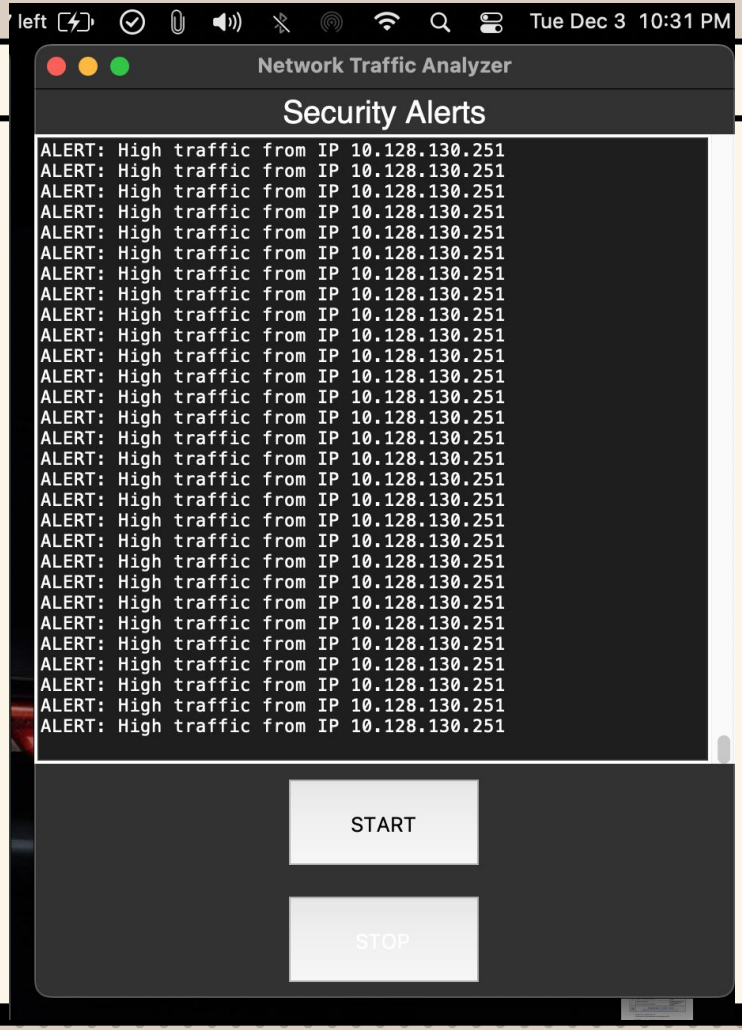
Outcome:

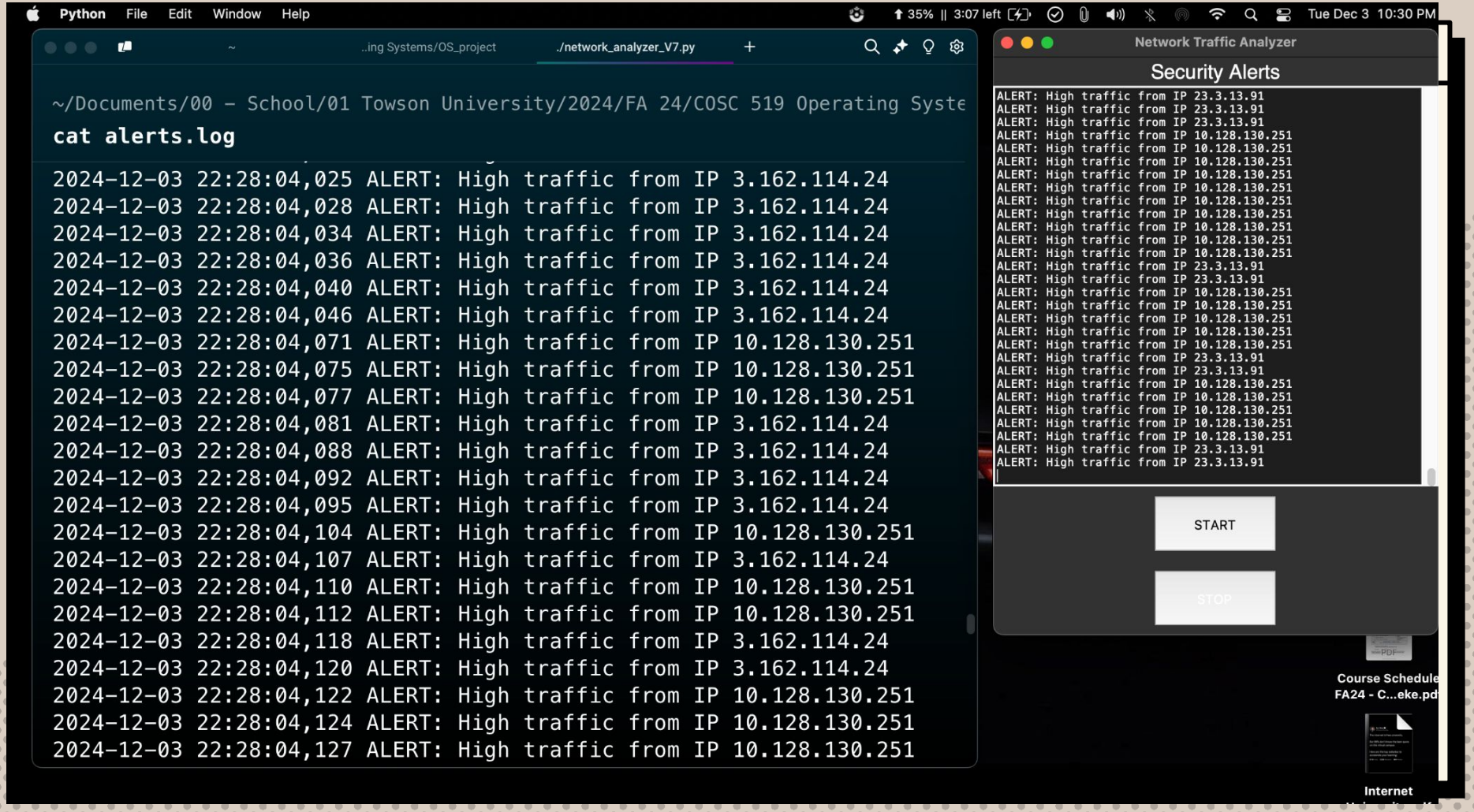
- Functional network analyzer with a responsive GUI on MacOS

Key Features:

- Monitors traffic on ens160.
- Logs IPs with high traffic or port scans
- GUI displays real-time alerts
- Run on Mac OS instead of Linux

```
    alert_textbox.insert(tk.END, f"{message}\n")
    alert_textbox.see(tk.END)  # Auto-scroll to the latest alert
    logging.info(message)

# Function to start sniffing packets
def start_sniffing():
    sniff(prn=packet_callback, store=False)

# Function to stop the application
def stop_sniffing():
    root.quit()

#####################################

#GUI SECTION

# Set up the GUI
root = tk.Tk()
root.title("Network Traffic Analyzer")

# Adding a label
label = tk.Label(root, text="Security Alerts", font=("Helvetica", 16))
label.pack()

# Adding a scrolling text box for displaying alerts
alert_textbox = scrolledtext.ScrolledText(root, wrap=tk.WORD, height=30, width=80)
alert_textbox.pack()

# Adding start and stop buttons
start_button = tk.Button(root, text="Start", command=start_sniffing, width=10, bg="white", fg="black")
start_button.pack(pady=7)

stop_button = tk.Button(root, text="Stop", command=stop_sniffing, width=10, bg="red", fg="white")
stop_button.pack(pady=7)

# Running the GUI event loop
root.mainloop()
```


left
Tue Dec 3 10:31 PM
Network Traffic Analyzer
Security Alerts
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
START
STOP


Python File Edit Window Help
35% || 3:07 left
Tue Dec 3 10:30 PM
~
..ing Systems/OS_project
./network_analyzer_V7.py
~/Documents/00 - School/01 Towson University/2024/FA 24/COSC 519 Operating Syste
cat alerts.log
2024-12-03 22:28:04,025 ALERT: High traffic from IP 3.162.114.24
2024-12-03 22:28:04,028 ALERT: High traffic from IP 3.162.114.24
2024-12-03 22:28:04,034 ALERT: High traffic from IP 3.162.114.24
2024-12-03 22:28:04,036 ALERT: High traffic from IP 3.162.114.24
2024-12-03 22:28:04,040 ALERT: High traffic from IP 3.162.114.24
2024-12-03 22:28:04,046 ALERT: High traffic from IP 3.162.114.24
2024-12-03 22:28:04,071 ALERT: High traffic from IP 10.128.130.251
2024-12-03 22:28:04,075 ALERT: High traffic from IP 10.128.130.251
2024-12-03 22:28:04,077 ALERT: High traffic from IP 10.128.130.251
2024-12-03 22:28:04,081 ALERT: High traffic from IP 3.162.114.24
2024-12-03 22:28:04,088 ALERT: High traffic from IP 3.162.114.24
2024-12-03 22:28:04,092 ALERT: High traffic from IP 3.162.114.24
2024-12-03 22:28:04,095 ALERT: High traffic from IP 3.162.114.24
2024-12-03 22:28:04,104 ALERT: High traffic from IP 10.128.130.251
2024-12-03 22:28:04,107 ALERT: High traffic from IP 3.162.114.24
2024-12-03 22:28:04,110 ALERT: High traffic from IP 10.128.130.251
2024-12-03 22:28:04,112 ALERT: High traffic from IP 10.128.130.251
2024-12-03 22:28:04,118 ALERT: High traffic from IP 3.162.114.24
2024-12-03 22:28:04,120 ALERT: High traffic from IP 3.162.114.24
2024-12-03 22:28:04,122 ALERT: High traffic from IP 10.128.130.251
2024-12-03 22:28:04,124 ALERT: High traffic from IP 10.128.130.251
2024-12-03 22:28:04,127 ALERT: High traffic from IP 10.128.130.251
Network Traffic Analyzer
Security Alerts
ALERT: High traffic from IP 23.3.13.91
ALERT: High traffic from IP 23.3.13.91
ALERT: High traffic from IP 23.3.13.91
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 23.3.13.91
ALERT: High traffic from IP 23.3.13.91
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 23.3.13.91
ALERT: High traffic from IP 23.3.13.91
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 10.128.130.251
ALERT: High traffic from IP 23.3.13.91
ALERT: High traffic from IP 23.3.13.91
START
STOP
Course Schedule
FA24 - C...eke.pd
Internet

DEMO LINK

https://somup.com/cZlfeUJLJF

JOHN NWEKE

Future Improvements

Ideas for Improvements

- Add real-time traffic graphs using matplotlib.
- Implement email notifications for critical alerts.
- Enhance GUI with filtering options for different protocols.
- Optimize packet processing for large networks.

THE END:
NETWORK TRAFFIC ANALYZER

My Journey in Network Monitoring and GUI Development

JOHN NWEKE