Network Packet Sniffer with Alert System

✅ Introduction

In today's cybersecurity landscape, monitoring network traffic is essential to detect threats and protect systems. The **Network Packet Sniffer with Alert System** is a Python-based tool that captures live network packets, logs metadata, detects anomalies such as DoS attacks and port scans, and optionally sends email alerts. It also allows visualization of network activity using **Matplotlib** and stores data in **SQLite** for analysis.

🔹 Abstract

This project demonstrates the creation of a **real-time network monitoring tool** that identifies abnormal patterns in traffic. Using **Scapy** for packet capture, the system tracks packet headers including IPs, ports, lengths, and flags. Threshold-based anomaly detection triggers alerts, enabling timely responses. The project emphasizes **network security, packet analysis, and proactive threat detection**, providing hands-on experience in monitoring and logging network activity.

🛠️ Tools Used

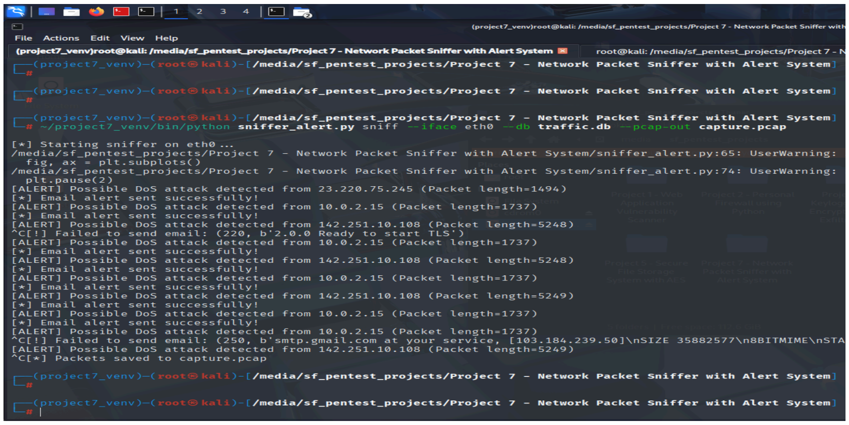
Tool	Purpose
Python 3.13	Core programming language
Scapy	Packet sniffing and analysis
SQLite	Logging packets and anomaly events
Matplotlib	Real-time traffic visualization
smtplib	Sending optional email alerts
Virtual Environment (venv)	Isolated Python environment
nmap & hping3	Testing and traffic simulation
Windows & Kali Linux	Development and testing environments

🔧 Steps Involved in Building the Project

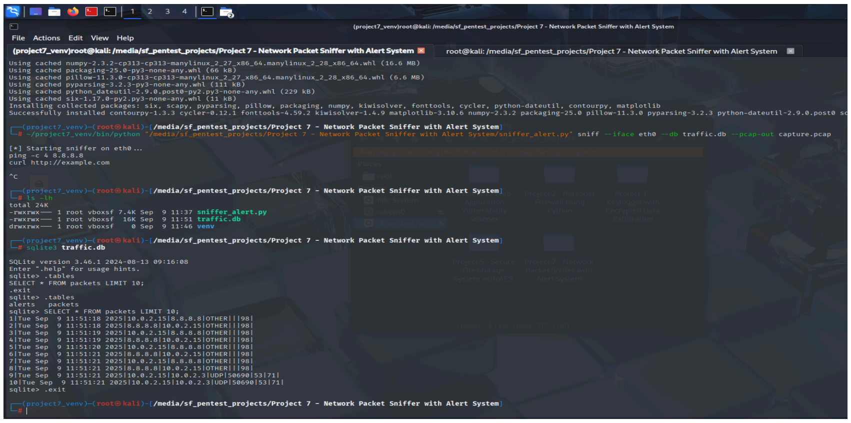
Step	Description
1. Setup Environment	Installed Python, pip, and created virtual environment; installed scapy and matplotlib.
2. Capture Packets	Used Scapy to capture live traffic; logged IP, port, packet length, and flags.
3. Detect Anomalies	Set thresholds to detect DoS attacks, port scans, and unusual traffic patterns; triggered alerts.

Step	Description
4. Log Data	Stored packet metadata and anomaly events in SQLite; ensured data integrity for analysis.
5. Email Alerts (Optional)	Configured email sending with smtplib for notifying anomalies using secure credentials.
6. Visualize Traffic (Optional)	Implemented real-time traffic graphs using Matplotlib to track network activity and anomalies.
7. Execute Sniffer	Activated virtual environment and ran the Python script to monitor, log, alert, and visualize network traffic.

📸 Screenshot


1
2
3
4
(project7_venv)root@kali: /media/sf_pentest_projects/Project 7 - Network Packet Sniffer with
File
Actions
Edit
View
Help
(project7_venv)root@kali: /media/sf_pentest_projects/Project 7 - Network Packet Sniffer with Alert System
root@kali: /media/sf_pentest_projects/Project 7 - N

```
┌──(project7_venv)─(root㉿kali)-[/media/sf_pentest_projects/Project 7 - Network Packet Sniffer with Alert System]
└─#

┌──(project7_venv)─(root㉿kali)-[/media/sf_pentest_projects/Project 7 - Network Packet Sniffer with Alert System]
└─#

┌──(project7_venv)─(root㉿kali)-[/media/sf_pentest_projects/Project 7 - Network Packet Sniffer with Alert System]
└─# ~/project7_venv/bin/python sniffer_alert.py sniff --iface eth0 --db traffic.db --pcap-out capture.pcap

[*] Starting sniffer on eth0 ...
/media/sf_pentest_projects/Project 7 - Network Packet Sniffer with Alert System/sniffer_alert.py:65: UserWarning:
  fig, ax = plt.subplots()
/media/sf_pentest_projects/Project 7 - Network Packet Sniffer with Alert System/sniffer_alert.py:74: UserWarning:
  plt.pause(2)
[ALERT] Possible DoS attack detected from 23.220.75.245 (Packet length=1494)
[*] Email alert sent successfully!
[ALERT] Possible DoS attack detected from 10.0.2.15 (Packet length=1737)
[*] Email alert sent successfully!
[ALERT] Possible DoS attack detected from 142.251.10.108 (Packet length=5248)
^C[!] Failed to send email: (220, b'2.0.0 Ready to start TLS')
[ALERT] Possible DoS attack detected from 10.0.2.15 (Packet length=1737)
[*] Email alert sent successfully!
[ALERT] Possible DoS attack detected from 142.251.10.108 (Packet length=5248)
[*] Email alert sent successfully!
[ALERT] Possible DoS attack detected from 10.0.2.15 (Packet length=1737)
[*] Email alert sent successfully!
[ALERT] Possible DoS attack detected from 142.251.10.108 (Packet length=5249)
[*] Email alert sent successfully!
[ALERT] Possible DoS attack detected from 10.0.2.15 (Packet length=1737)
[*] Email alert sent successfully!
[ALERT] Possible DoS attack detected from 10.0.2.15 (Packet length=1737)
^C[!] Failed to send email: (250, b'smtp.gmail.com at your service, [103.184.239.50]\nSIZE 35882577\n8BITMIME\nSTA
[ALERT] Possible DoS attack detected from 142.251.10.108 (Packet length=5249)
^C[*] Packets saved to capture.pcap

┌──(project7_venv)─(root㉿kali)-[/media/sf_pentest_projects/Project 7 - Network Packet Sniffer with Alert System]
└─#

┌──(project7_venv)─(root㉿kali)-[/media/sf_pentest_projects/Project 7 - Network Packet Sniffer with Alert System]
└─# |
```


1
2
3
4
(project7_venv)root@kali: /media/sf_pentest_projects/Project 7 - Network Packet Sniffer with Alert System
File
Actions
Edit
View
Help
(project7_venv)root@kali: /media/sf_pentest_projects/Project 7 - Network Packet Sniffer with Alert System
root@kali: /media/sf_pentest_projects/Project 7 - Network Packet Sniffer with Alert System

```
Using cached numpy-2.3.2-cp313-cp313-manylinux_2_27_x86_64.manylinux_2_28_x86_64.whl (16.6 MB)
Using cached packaging-25.0-py3-none-any.whl (66 kB)
Using cached pillow-11.3.0-cp313-cp313-manylinux_2_27_x86_64.manylinux_2_28_x86_64.whl (6.6 MB)
Using cached pyparsing-3.2.3-py3-none-any.whl (111 kB)
Using cached python_dateutil-2.9.0.post0-py2.py3-none-any.whl (229 kB)
Using cached six-1.17.0-py2.py3-none-any.whl (11 kB)
Installing collected packages: six, scapy, pyparsing, pillow, packaging, numpy, kiwisolver, fonttools, cycler, python-dateutil, contourpy, matplotlib
Successfully installed contourpy-1.3.3 cycler-0.12.1 fonttools-4.59.2 kiwisolver-1.4.9 matplotlib-3.10.6 numpy-2.3.2 packaging-25.0 pillow-11.3.0 pyparsing-3.2.3 python-dateutil-2.9.0.post0 sc

┌──(project7_venv)─(root㉿kali)-[/media/sf_pentest_projects/Project 7 - Network Packet Sniffer with Alert System]
└─# ~/project7_venv/bin/python "/media/sf_pentest_projects/Project 7 - Network Packet Sniffer with Alert System/sniffer_alert.py" sniff --iface eth0 --db traffic.db --pcap-out capture.pcap

[*] Starting sniffer on eth0 ...
ping -c 4 8.8.8.8
curl http://example.com

^C

┌──(project7_venv)─(root㉿kali)-[/media/sf_pentest_projects/Project 7 - Network Packet Sniffer with Alert System]
└─# ls -lh
total 24K
-rwxrwx--- 1 root vboxsf 7.4K Sep  9 11:37 sniffer_alert.py
-rwxrwx--- 1 root vboxsf  16K Sep  9 11:51 traffic.db
drwxrwx--- 1 root vboxsf    0 Sep  9 11:46 venv

┌──(project7_venv)─(root㉿kali)-[/media/sf_pentest_projects/Project 7 - Network Packet Sniffer with Alert System]
└─# sqlite3 traffic.db

SQLite version 3.46.1 2024-08-13 09:16:08
Enter ".help" for usage hints.
sqlite> .tables
SELECT * FROM packets LIMIT 10;
.exit
sqlite> .tables
alerts   packets
sqlite> SELECT * FROM packets LIMIT 10;
1|Tue Sep  9 11:51:18 2025|10.0.2.15|8.8.8.8|OTHER|||98|
2|Tue Sep  9 11:51:18 2025|8.8.8.8|10.0.2.15|OTHER|||98|
3|Tue Sep  9 11:51:19 2025|10.0.2.15|8.8.8.8|OTHER|||98|
4|Tue Sep  9 11:51:19 2025|8.8.8.8|10.0.2.15|OTHER|||98|
5|Tue Sep  9 11:51:20 2025|10.0.2.15|8.8.8.8|OTHER|||98|
6|Tue Sep  9 11:51:21 2025|8.8.8.8|10.0.2.15|OTHER|||98|
7|Tue Sep  9 11:51:21 2025|10.0.2.15|8.8.8.8|OTHER|||98|
8|Tue Sep  9 11:51:21 2025|8.8.8.8|10.0.2.15|OTHER|||98|
9|Tue Sep  9 11:51:21 2025|10.0.2.15|10.0.2.3|UDP|50690|53|71|
10|Tue Sep  9 11:51:21 2025|10.0.2.15|10.0.2.3|UDP|50690|53|71|
sqlite> .exit

┌──(project7_venv)─(root㉿kali)-[/media/sf_pentest_projects/Project 7 - Network Packet Sniffer with Alert System]
└─# |
```

🔔 Conclusion

The **Network Packet Sniffer with Alert System** offers a complete solution for real-time network monitoring. It captures and logs traffic, detects anomalies, and optionally sends email notifications. This project reinforces practical skills in **network packet analysis, anomaly detection, database management, and alerting mechanisms**. ✅ Future upgrades may include additional anomaly types, a GUI dashboard, and advanced visualization, making it a comprehensive cybersecurity tool.