# Task-05

# “ Network Packet Analyzer

BY: OMAR MAHMOOD

# Table of Contents

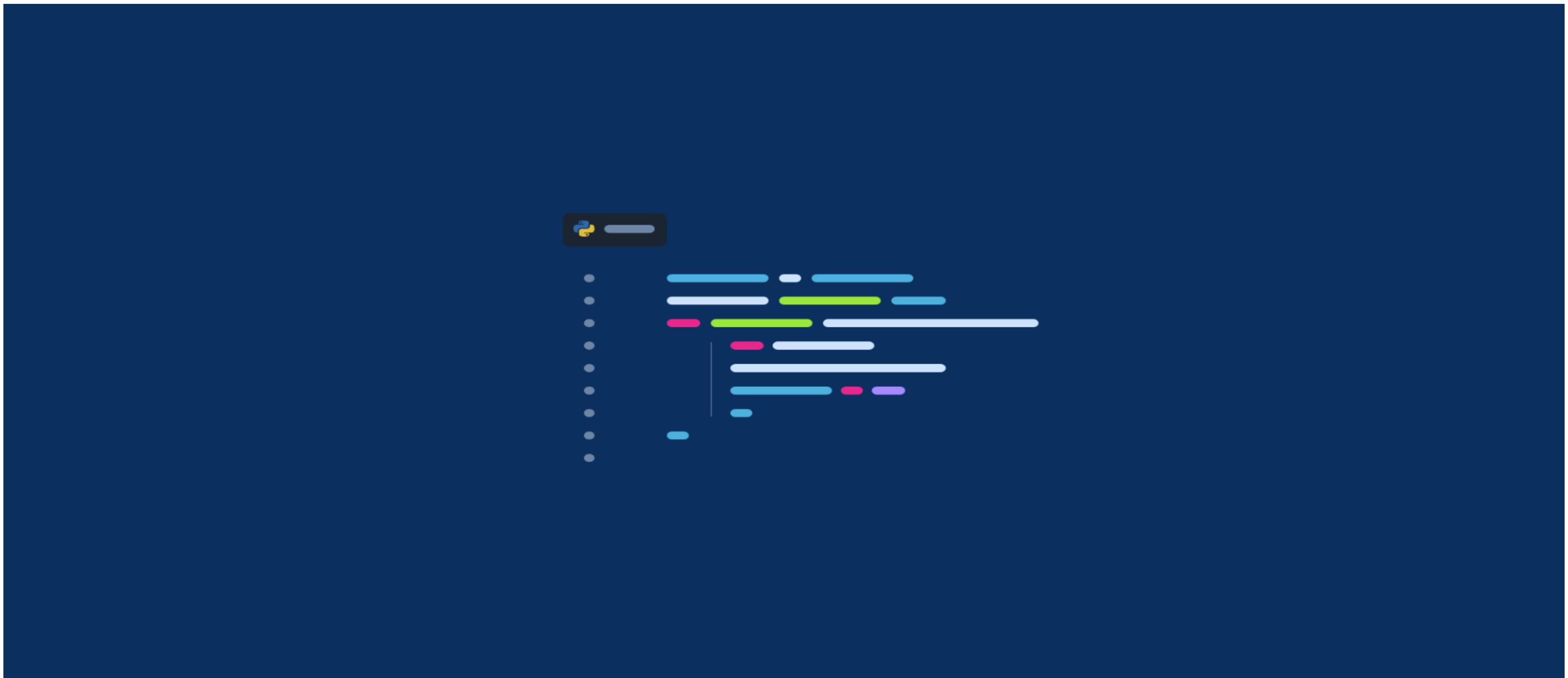
# 1. Introduction

- **The Network Packet Capture/Analyzer Tool is a software solution to capture and analyze network packets efficiently. This tool aims to provide network administrators and security professionals with a convenient way to monitor network traffic, identify potential threats, and troubleshoot network issues.**

# 2. Objectives

The primary objectives of this project were as follows:

- Develop a user-friendly tool for capturing network packets.
- Implement features for analyzing captured packets, including displaying IP addresses, protocols, and payload data.
- Ensure compatibility with both Linux and Windows operating systems.
- Provide clear instructions for using the tool effectively.



# 3. Methodology

- **The tool was developed using Python programming language and several third-party libraries, including pyshark, colored, and tqdm. The development process involved several iterations to implement and test various features, ensuring robustness and reliability.**

# 4. Tool Features

**Packet Analysis:**

- **Provides options for analyzing captured packets, including displaying IP addresses, protocols, and payload data.**
- **Enables users to select specific analysis options based on their requirements.**

**User Interface Enhancements:**

- **Incorporates ASCII art welcome banner for visual appeal.**
- **Utilizes colored text and formatting for improved readability.**
- **Includes informative prompts and messages to guide users through tool usage.**

# 5. Usage Instructions

**Installation:**

- **Ensure that required Python packages (pyshark, colored, tqdm) are installed.**
- **Clone the repository containing the tool source code.**

**Running the Tool:**

- **Execute the main script (network_packet_tool.py) using Python.**
- **Follow the on-screen prompts to select desired actions (capture, analyze, or exit).**

## Capture Mode:

- Select 'c' to initiate packet capture.
- Choose the network interface and specify the number of packets to capture.

## Analysis Mode:

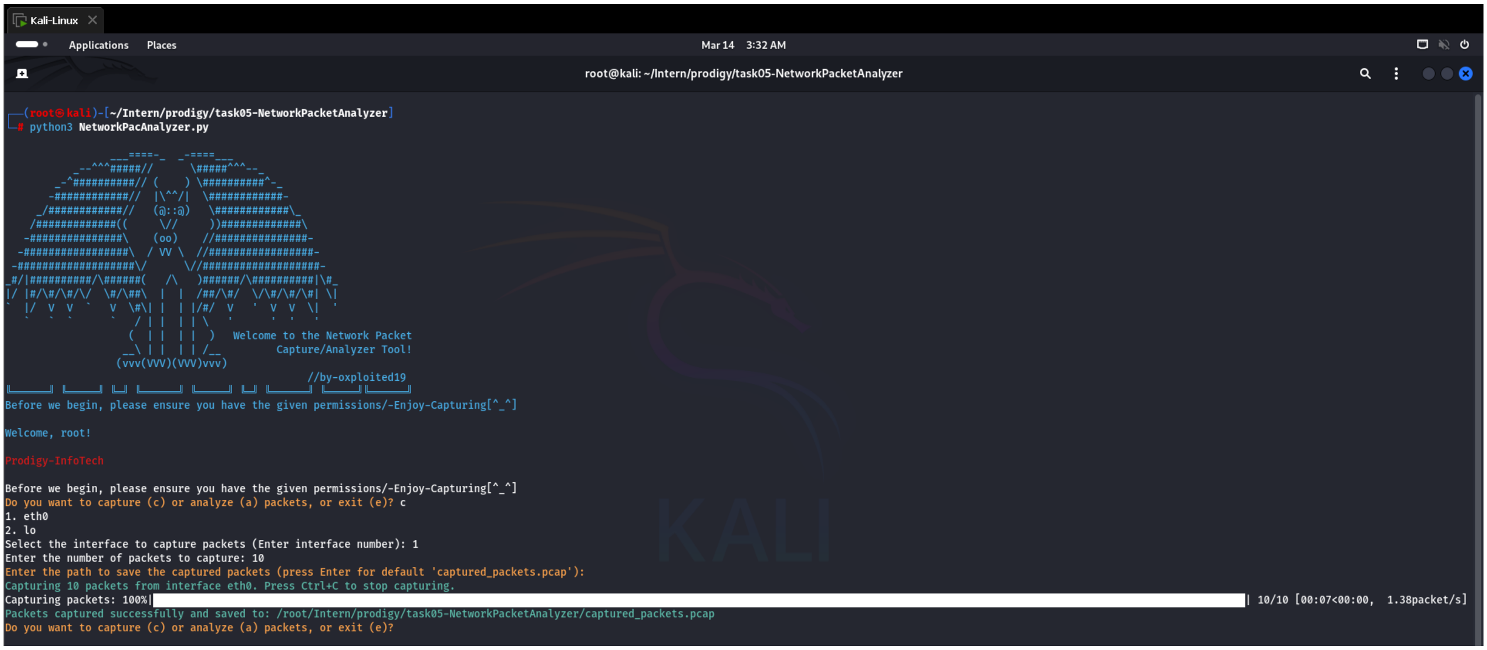
- Select 'a' to analyze captured packets.
- Enter the path to the captured packets file when prompted.
- Choose from available analysis options to display relevant information.

## Exiting the Tool:

- Select 'e' at any time to exit the tool.

# 6. Results and Analysis

**The Network Packet Capture/Analyzer Tool has been successfully developed and tested. It provides an intuitive interface for capturing and analyzing network packets, enabling users to gain insights into network traffic and identify potential issues.**



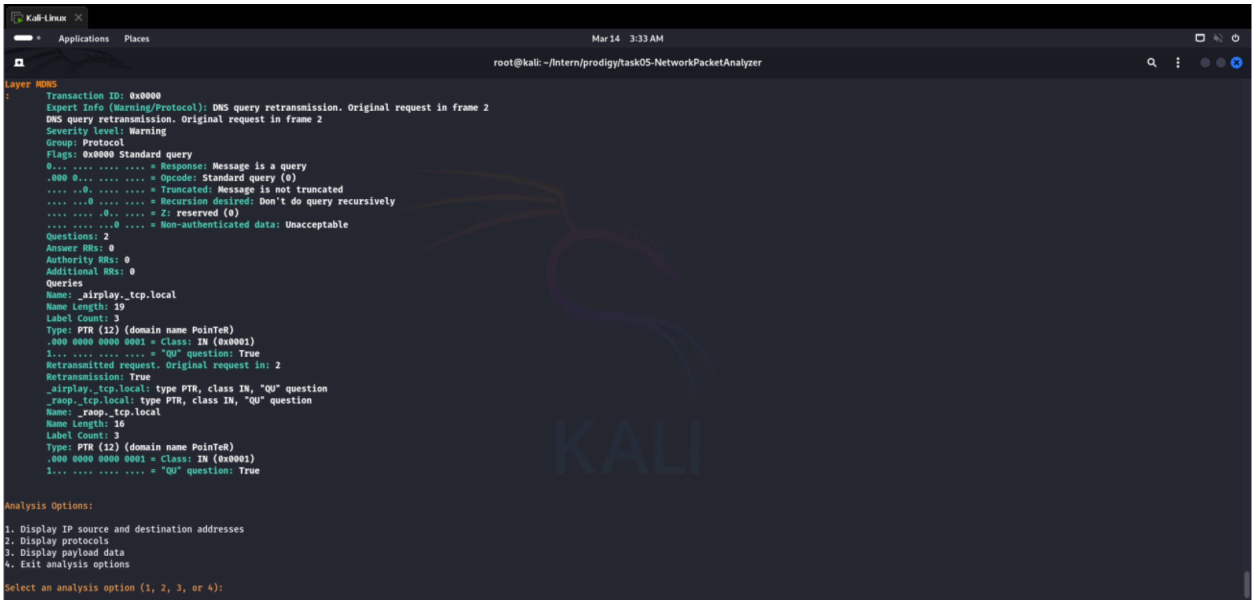
```
┌──(root㉿kali)-[~/Intern/prodigy/task05-NetworkPacketAnalyzer]
└─# python3 NetworkPacAnalyzer.py

                    ___====-_  _-====___
              _--^^^#####//      \\#####^^^--_
           _-^##########// (    ) \\##########^-_
          -############//  |\^^/|  \\############-
        _/############//   (@::@)   \\############\_
       /#############((     \\//     ))#############\
      -###############\\    (oo)    //###############-
     -#################\\  / VV \  //#################-
    -###################\\/      \//###################-
   _#/|##########/\######(   /\   )######/\##########|\#_
   |/ |#/\#/\#/\/  \#/\##\  |  |  /##/\#/  \/\#/\#/\#| \|
   `  |/  V  V  `   V  \#\| |  | |/#/  V   '  V  V  \|  '
      `   `  `      `   / | |  | | \   '      '  '   '
                       (  | |  | |  )  Welcome to the Network Packet
                      __\ | |  | | /__        Capture/Analyzer Tool!
                     (vvv(VVV)(VVV)vvv)
                                               //by-oxploited19
╚═════╝ ╚═════╝ ╚═╝ ╚═══════╝ ╚═════╝ ╚═╝ ╚═══════╝ ╚═════╝╚═════╝
Before we begin, please ensure you have the given permissions/-Enjoy-Capturing[^_^]

Welcome, root!

Prodigy-InfoTech

Before we begin, please ensure you have the given permissions/-Enjoy-Capturing[^_^]
Do you want to capture (c) or analyze (a) packets, or exit (e)? c
1. eth0
2. lo
Select the interface to capture packets (Enter interface number): 1
Enter the number of packets to capture: 10
Enter the path to save the captured packets (press Enter for default 'captured_packets.pcap'):
Capturing 10 packets from interface eth0. Press Ctrl+C to stop capturing.
Capturing packets: 100%|██████████████████████████████████████████████████| 10/10 [00:07<00:00,  1.38packet/s]
Packets captured successfully and saved to: /root/Intern/prodigy/task05-NetworkPacketAnalyzer/captured_packets.pcap
Do you want to capture (c) or analyze (a) packets, or exit (e)?
```



```
Layer MDNS
:       Transaction ID: 0x0000
        Expert Info (Warning/Protocol): DNS query retransmission. Original request in frame 2
        DNS query retransmission. Original request in frame 2
        Severity level: Warning
        Group: Protocol
        Flags: 0x0000 Standard query
        0... .... .... .... = Response: Message is a query
        .000 0... .... .... = Opcode: Standard query (0)
        .... ..0. .... .... = Truncated: Message is not truncated
        .... ...0 .... .... = Recursion desired: Don't do query recursively
        .... .... .0.. .... = Z: reserved (0)
        .... .... ...0 .... = Non-authenticated data: Unacceptable
        Questions: 2
        Answer RRs: 0
        Authority RRs: 0
        Additional RRs: 0
        Queries
        Name: _airplay._tcp.local
        Name Length: 19
        Label Count: 3
        Type: PTR (12) (domain name PoinTeR)
        .000 0000 0000 0001 = Class: IN (0x0001)
        1... .... .... .... = "QU" question: True
        Retransmitted request. Original request in: 2
        Retransmission: True
        _airplay._tcp.local: type PTR, class IN, "QU" question
        _raop._tcp.local: type PTR, class IN, "QU" question
        Name: _raop._tcp.local
        Name Length: 16
        Label Count: 3
        Type: PTR (12) (domain name PoinTeR)
        .000 0000 0000 0001 = Class: IN (0x0001)
        1... .... .... .... = "QU" question: True


Analysis Options:

1. Display IP source and destination addresses
2. Display protocols
3. Display payload data
4. Exit analysis options

Select an analysis option (1, 2, 3, or 4):
```

# 6. CONCLUSION

**The development of the Network Packet Capture/Analyzer Tool represents a significant step forward in network monitoring and analysis. With its user-friendly interface and robust features, the tool is well-equipped to meet the needs of network administrators and security professionals.**