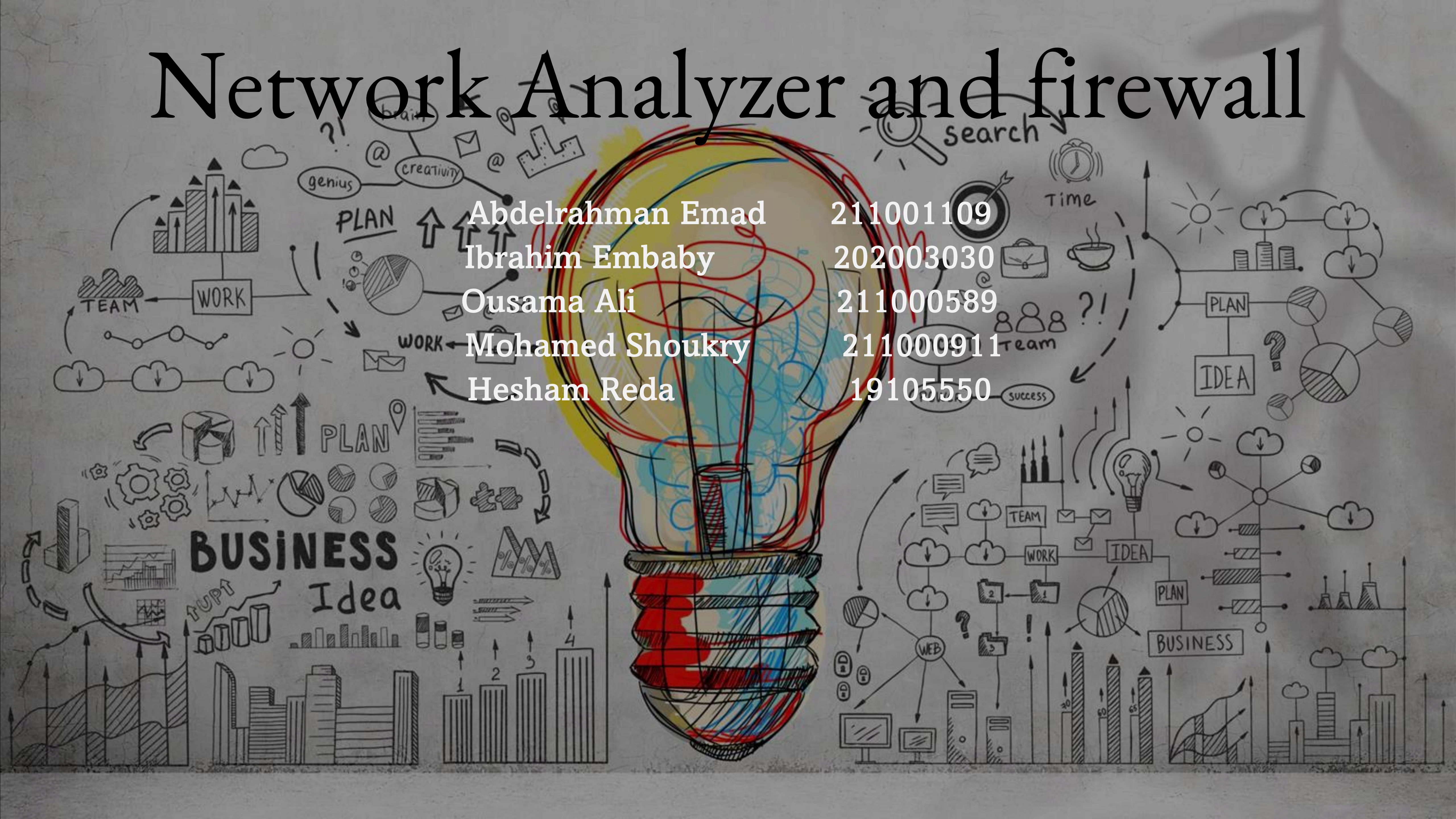
Network Analyzer and firewall



Abdelrahman Emad	211001109
Ibrahim Embaby	202003030
Ousama Ali	211000589
Mohamed Shoukry	211000911
Hesham Reda	19105550

Introduction

Robust Protection: The Analyzer Firewall offers a strong defense against cyber threats.

Customizable Policies: Organizations can tailor security policies to their specific needs, allowing for precise control over network access and ensuring that only authorized traffic is permitted.

Benefits

- Enhanced Security
- Improved Performance
- Centralized Management
- Scalability

Network Traffic Analyzer And Firewall

Brief overview

- The Program’s aim is to analyze network traffic for suspicious packets and to block specific suspicious Ip addresses.

- Tools used: Python, Scapy, tkinter

Main Components

- Packet analysis function
- Live capture feature
- PCAP file analysis
- IP block, unblock, and view blocklist functionality.

Packet Analysis Function

- Analyzes packets for TCP, UDP, and ICMP protocols
- Detects and logs suspicious packets in a “.log file”

Live Capture Feature

- Captures live network traffic for analysis
- Threaded implementation for continuous capture
- Start and stop buttons for control
- Exit Button For Live Capture Termination
- Real-time blocking of suspicious packets
- Identify blocked addresses of packets and recognize them as blocked.

PCAP File Analysis

- Analyzes pre-recorded network traffic from PCAP files
- Uses Scapy's sniff function with the offline parameter
- Button to browse and select PCAP files
- Checks the PCAP files’ IPs for easier accessibility and to ensure whether they are blocked

Test Packets

- Pre-recorded Test packets using WireShark
- 3 test packets each one represents a different error : (TCP, UDP, ICMP) respectively.
- The Program successfully recognizes the specific error in each of these packets with their full IPs, also ensuring they are not blocked.

Logging

- Logs analysis results to a log file named “Traffic analysis.log”
- Uses the logging module in Python To store Packets that were found suspicious in a clear format in the log file.
- Logs each packet’s IP in detail
- Logs blocked and unblocked ip addresses with a feature to view blocklist

conclusion

- The Analyzer Firewall is a powerful solution that enhances network security, mitigates risks, and protects critical assets from cyber threats.
- By deploying the Analyzer Firewall, your organization can achieve a secure and resilient network infrastructure.
- ensuring your data's confidentiality, integrity, and availability.

THANK YOU FOR YOUR ATTENTION :)