SIT764 Team Project

Team: Chameleon Security

Project name: Anomaly Detection “Investigate the MOP website and establish a baseline of normal network behaviour”

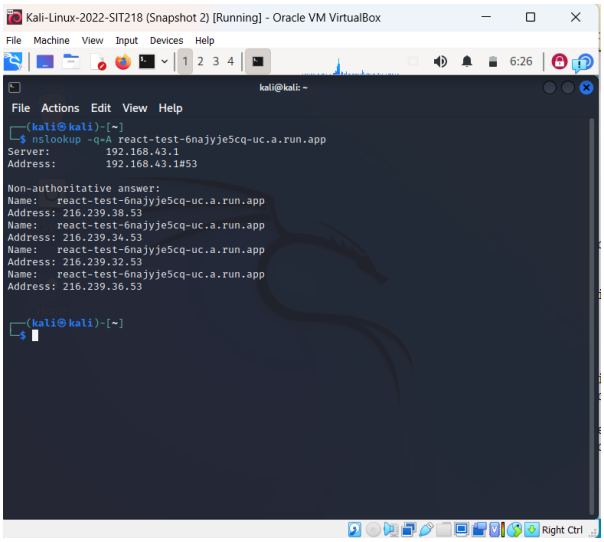
Tools: Nmap and Wireshark

MOP website: https://react-test-6najyje5cq-uc.a.run.app

OS: Kali Linux

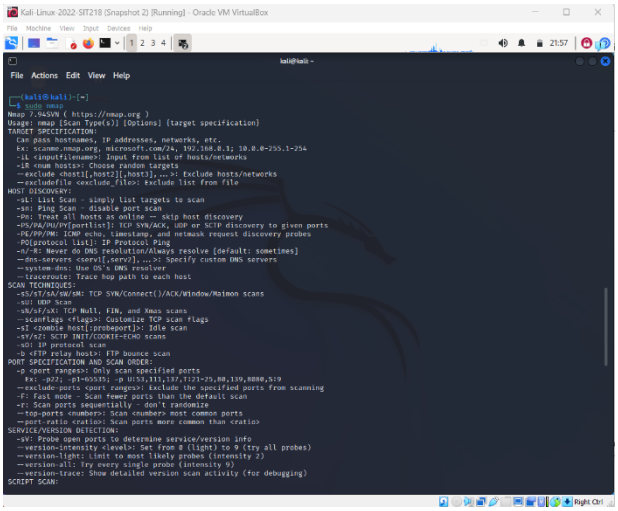
In this project, "anomaly detection on a https://react-test-6najyje5cq-uc.a.run.app/ using Nmap and Wireshark", the steps to be carried out would be used to identify and investigate any unusual or suspicious activity on the network hosting the web application. The Nmap scan provides an overview of the network, and the Wireshark analysis offers a detailed view of the network traffic, allowing for a thorough investigation of any potential anomalies.

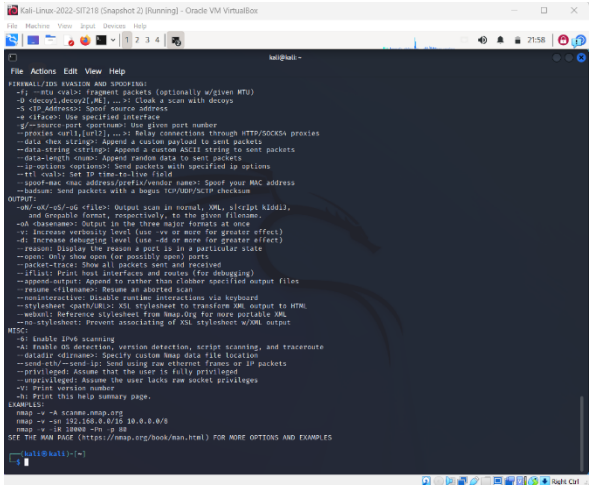
Using the NSLOOKUP command to scan the MOP website to detect IP address:



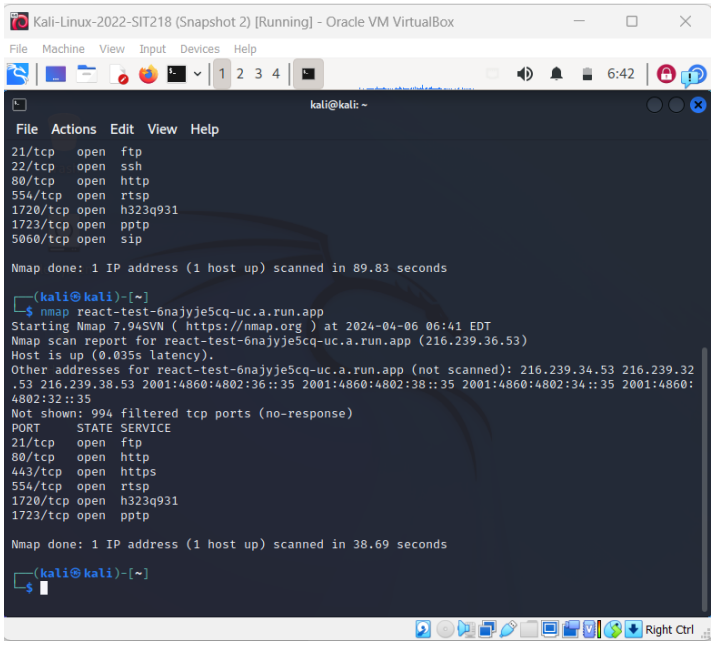
From this result, it shows that the IP address of the MOP website is 216.239.36.53

Install Nmap tool. This tool will be used to scan the MOP website for open ports.





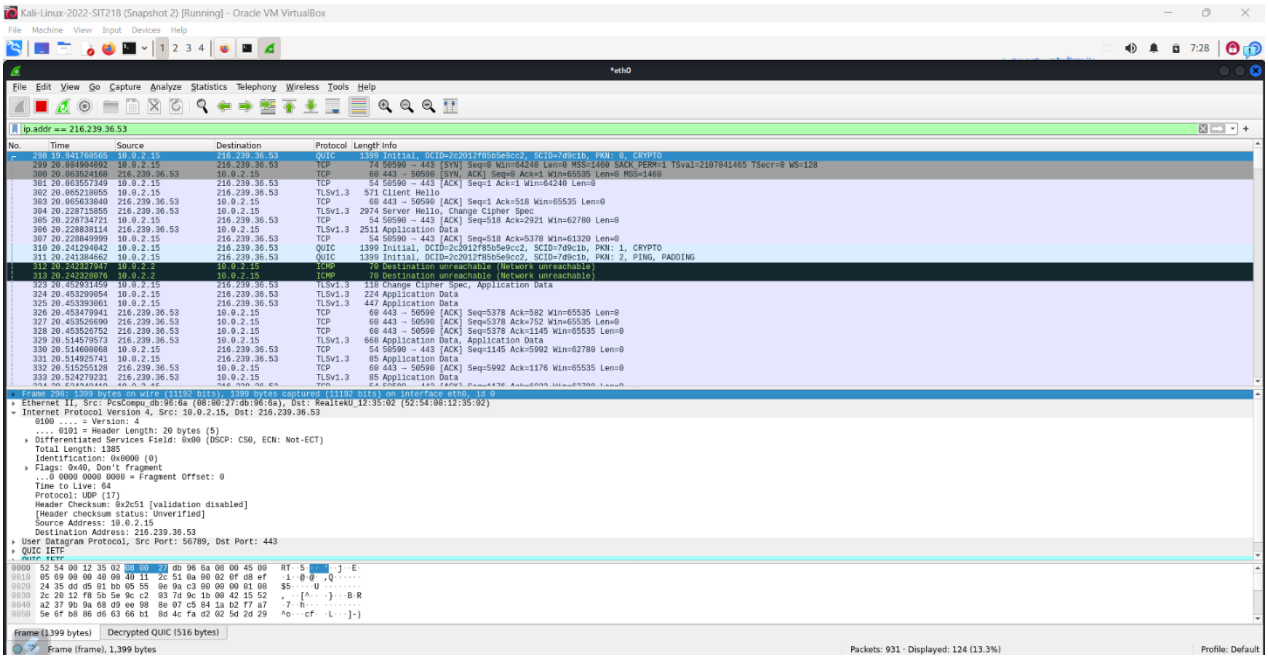
Scan MOP website using Nmap command, and the result is given below:



From the scan results, the following TCP ports are open, 21,80, 443, 554,1720 and 1723.

Using TCP port 443 for listening port (open) through a 3-way handshake connection between the source and destination port. Since the port is open, the source requested a SYN packet, a response destination sent SYN and ACK packets, the source sent ACK packets, and lastly source again sent RST and ACK packets.

Use the following command Nmap -sT -p 443 216.239.36.53 and open Wireshark to capture the packet:



Investigating these results shows that a 3-way handshake was established,

- Source “10.0.2.15” sent SYN packet to the destination “ 216.239.36.53”
- Destination sent SYN, and ACK to the source
- Source sent ACK packet to the destination

SYN: synchronize

ACK: Acknowledge

Analyze captured packet for any anomaly and set baseline profile for stability

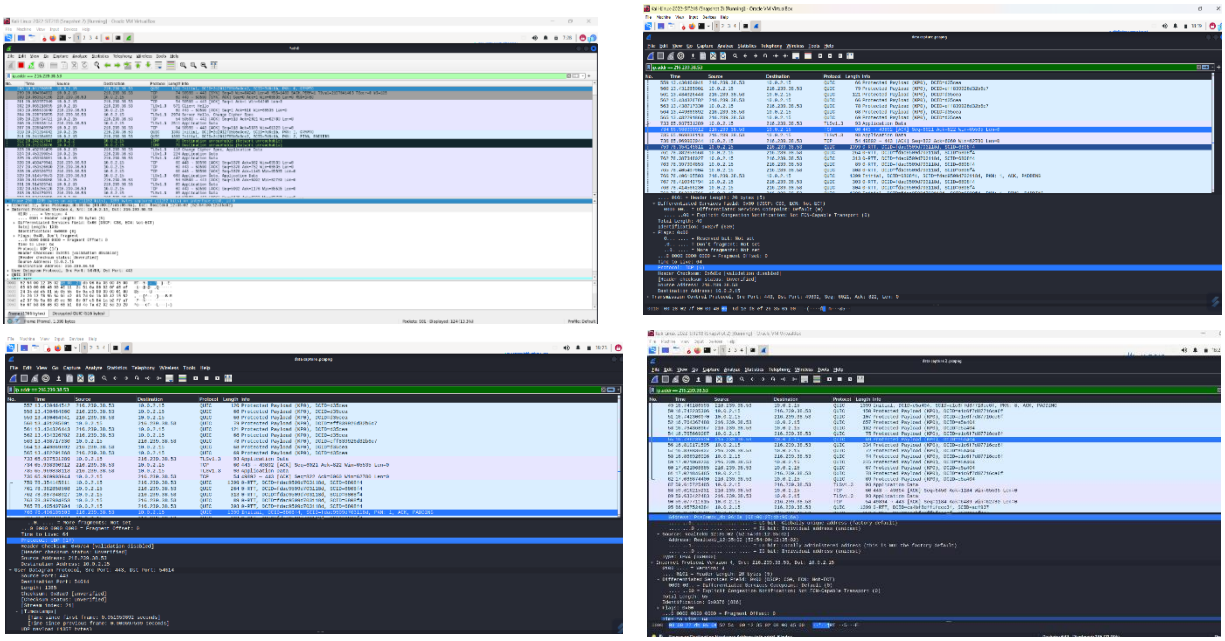
Most security monitoring systems utilize a signature-based approach to detect threats. Packets are generally monitored on the network and they look for patterns in the packets that match their database of signatures representing pre-identified known security threats. Network behavior anomaly detection (NBAD)-based systems are particularly helpful in detecting security threat vectors in two instances where signature-based systems cannot: (i) new zero-day attacks, and (ii) when the threat traffic is encrypted.

Consider Candidate packet attributes for traffic profiling such as:

- marginal distributions of the fractions of packets having various:
- IP protocol-type values
- packet size
- server port numbers, i.e., the smaller of the source port number and the destination port number
- source/ destination IP prefixes
- Time-to-Live (TTL) values
- IP/TCP header lengths
- TCP flag patterns.
- Also, consider the joint distribution of the fraction of packets having various combinations, such as:
- packet-size and protocol-type
- server port number and protocol-type
- source IP prefix
- TTL values, etc.
- fractions of packets such as:

- use IP fragmentation and
- bear incorrect IP/TCP/UDP checksums

sample of data packets analysis of MOP website for normal behavior:

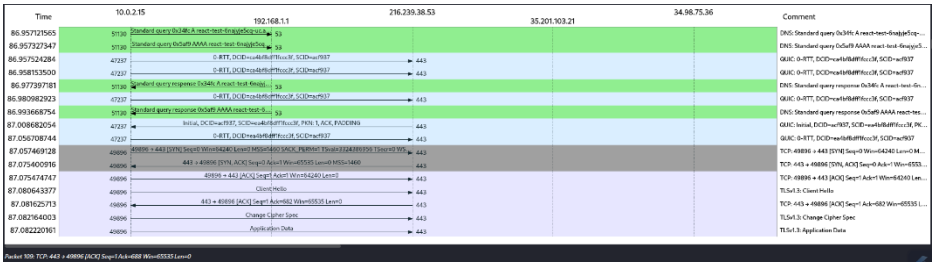


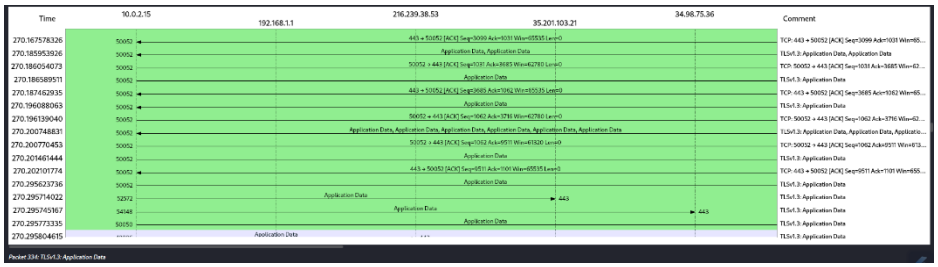
FLOW-BASED ANOMALY DETECTION APPROACH:

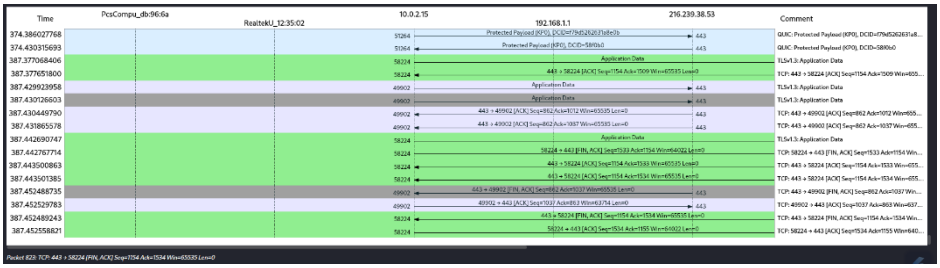
Flow-based anomaly detection is fundamentally about analyzing network flows. A network flow is represented by a flow record, which serves as a condensed signal that a specific network flow has occurred, indicating that two network endpoints have interacted at some point in the past. A flow record usually includes the IP addresses of the two hosts, network ports, network protocol, the volume of data transmitted during the connection, the timestamp of the flow, and several additional flags. The effectiveness of flow-based methods is largely dependent on the network devices' capacity to produce flow data.

Based on the analysis of the data captured by Wireshark and the network scan by Nmap, identify any anomalies or suspicious activities. This could be unexpected traffic, unusual ports being used, or unfamiliar protocols being implemented.

- Analyzing traffic flow patterns using Flow Graph tools in Wireshark to query, visualize, and correlate flow data to identify patterns, trends, and anomalies in network traffic.







By comparing the current flow data captured at different times and intervals to set the baselines that define the expected normal behavior of the network. The data were investigated such as logs, packets, events, and domain knowledge. Further investigation was carried out to detect source and destination of anomalous traffic such as IP addresses, hostnames, geolocations, or domains; protocol and application of anomalous traffic such as TCP or UDP ports, service names, or application types; duration and frequency of anomalous traffic such as start and end times, intervals, or periodicity; volume and bandwidth of anomalous traffic such as bytes, packets, or bits per second; flags and status of anomalous traffic such as TCP flags, QUIC protocol, or flow end reason.

This analysis shows that there were no detected suspicious activities. Such that:

- The analysis detects no sudden increase or decrease in traffic volume which may indicate a denial-of-service attack
- a connection or activity from an unusual IP address which may suggest a malware infection
- a congestion in a network segment which may point to a misconfiguration
- a deviation from the typical traffic profile which may signal a change in user behavior.

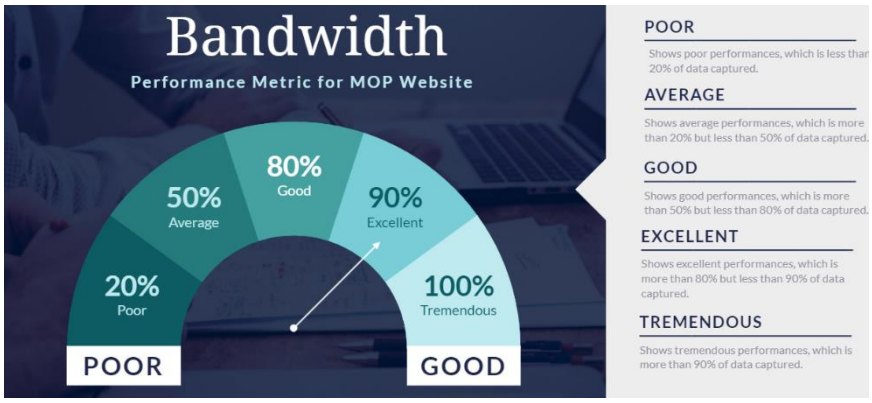
MOP WEBSITE NETWORK PERFORMANCE METRIC BASELINE:

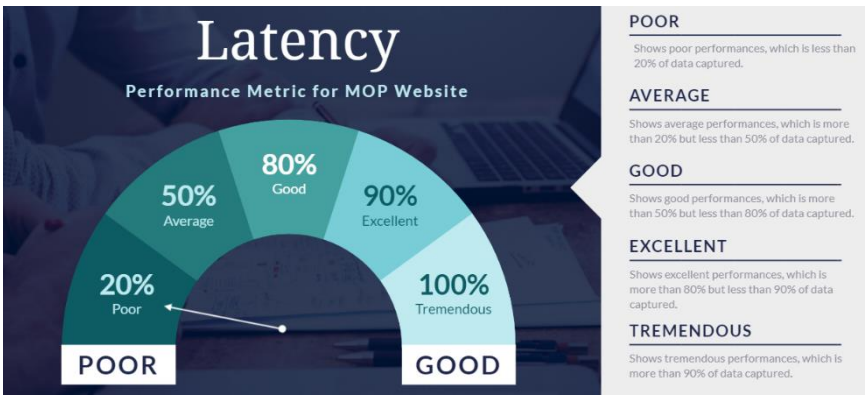
Establishing a network baseline provides early signs that the demands of applications and the network are nearing the available capacity, enabling the MOP team to strategize for enhancements. By aligning network performance baselines with existing network service-level agreements (SLAs), the Chameleon Company can maintain within capacity limits and pinpoint areas that are deviating from compliance. However, there isn't a universally accepted method for setting performance baselines.

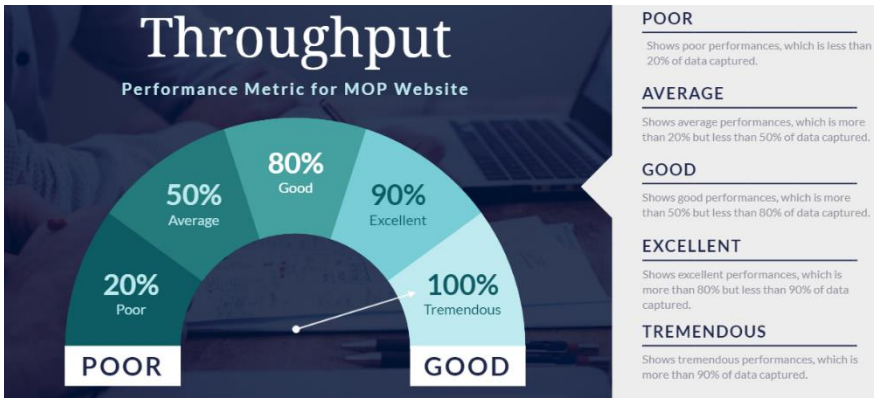
My baseline for MOP website is set using common network performance metrics:

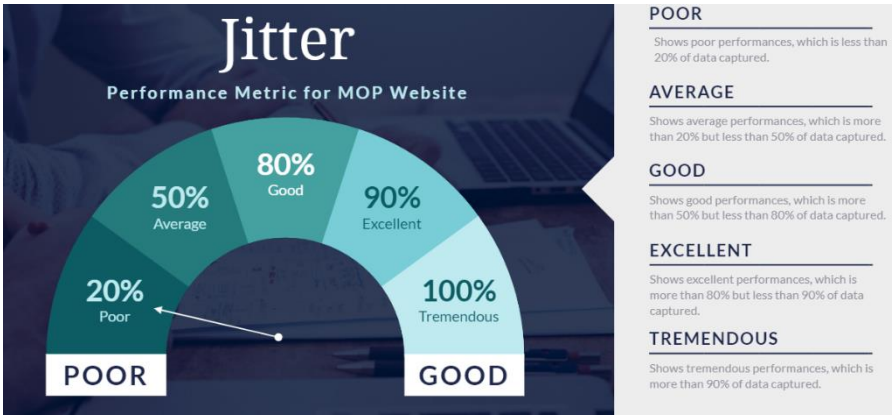
- Bandwidth: It's the maximum data transmission capacity.
- Latency: crucial for services requiring real-time data.
- Throughput: Throughput is the actual rate at which data is transferred
- Jitter: Jitter is the variation in the amount of time taken for packets to travel across the network.
- Packet loss: Packet loss occurs when data packets traveling across a network fail to reach their destination.

Baseline graph:









Checking the performance of the MOP website to ascertain its responsiveness and availability using GTmetrix grade shows that the website is actively normal.

Evidence is given below: