

# 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-6najiye5cq-uc.a.run.app>

**OS:** Kali Linux

In this project, "anomaly detection on a <https://react-test-6najtje5cq-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 provides 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:

Kali-Linux-2022-SIT218 (Snapshot 2) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4

6:26

kali@kali -

File Actions Edit View Help

```
(kali@kali)-[~]
└─$ nslookup -q=ra react-test-6na3yje5cq-uc.a.run.app
Server:      192.168.43.1
Address:     192.168.43.1#53

Non-authoritative answer:
Name:   react-test-6na3yje5cq-uc.a.run.app
Address: 216.239.38.53
Name:   react-test-6na3yje5cq-uc.a.run.app
Address: 216.239.34.53
Name:   react-test-6na3yje5cq-uc.a.run.app
Address: 216.239.32.53
Name:   react-test-6na3yje5cq-uc.a.run.app
Address: 216.239.36.53
```

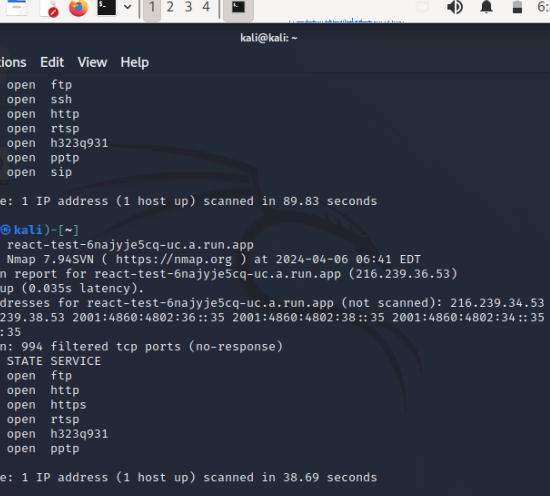
```
(kali@kali)-[~]
└─$
```

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.

[illegible][illegible]

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



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal displays the results of an Nmap scan performed on a React-Test application. The scan was conducted on 2024-04-06 at 06:41 EDT. The results show that the application is up and running on port 80 (HTTP) and port 443 (HTTPS). The terminal output is as follows:

```
kali@kali: ~
File Actions Edit View Help

21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
554/tcp open  rtsp
1720/tcp open h323q931
1723/tcp open  pptp
5060/tcp open  sip

Nmap done: 1 IP address (1 host up) scanned in 89.83 seconds

(kali@kali)-[~]
$ nmap react-test-6najyje5cq-uc.a.run.app
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-06 06:41 EDT
Nmap scan report for react-test-6najyje5cq-uc.a.run.app (216.239.36.53)
Host is up (0.035s latency).
Other addresses for react-test-6najyje5cq-uc.a.run.app (not scanned): 216.239.34.53 216.239.32.53 216.239.38.53 2001:4860:4802:36::35 2001:4860:4802:38::35 2001:4860:4802:34::35 2001:4860:4802:32::35
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https
554/tcp   open  rtsp
1720/tcp  open  h323q931
1723/tcp  open  pptp

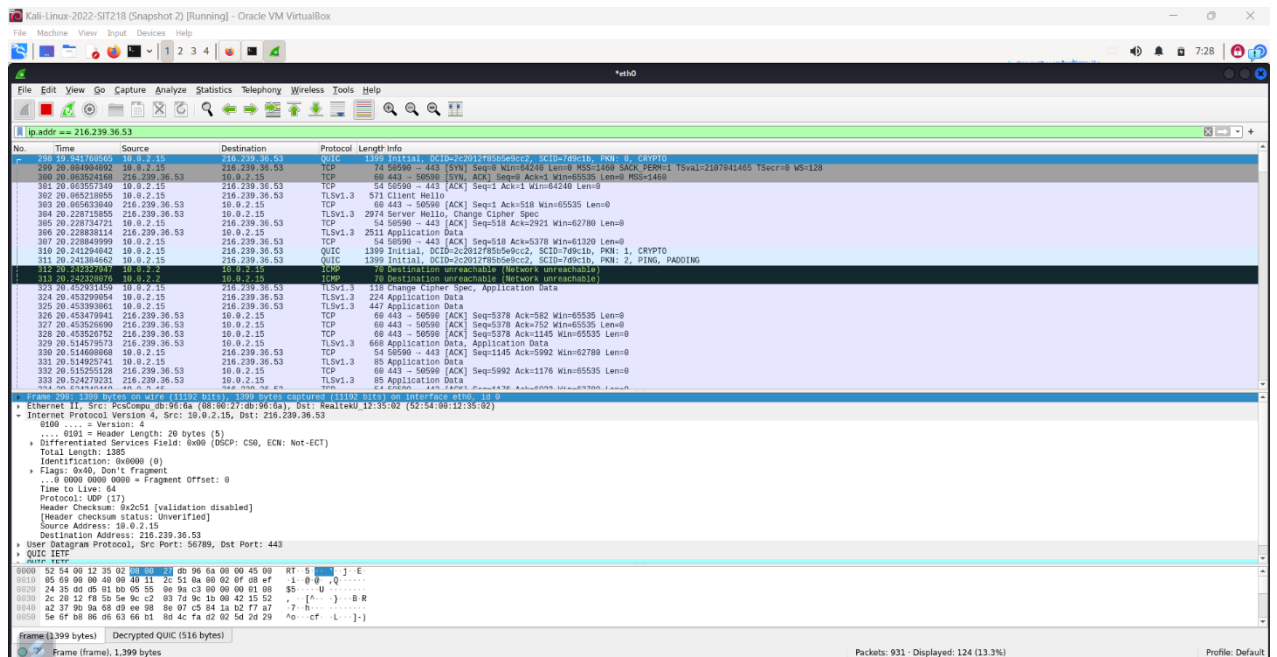
Nmap done: 1 IP address (1 host up) scanned in 38.69 seconds

(kali@kali)-[~]
$
```

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

**Work in progress to analyze captured packet for any anomaly**