### Vulnerability Assessment and Penetration Testing Lab Experiments

**Experiment 1:**

**Monitoring Network Traffic**

**Aim:**

Network traffic monitoring is the process of analyzing, diagnosing, and resolving network usage issues that impact the security and performance of applications running on the network. Here we'll cover both the benefits of monitoring network traffic and how best to implement network monitoring.

**Procedure:**

Some specific steps you can follow to learn how to monitor network traffic on any device.

Step 1: Choose a data source of best fit

Flow Data.  Or Packet Data or WiFi Data.

### **Step 2: Discover main applications running on your network**

After identifying a data source of best fit, discovering how users are accessing your

network will allow you to track usage back to the user's origin.

### **Step 3: Apply network monitor tools**

In addition to a network topology mapper, there are multiple network monitoring tools

you'll want to consider utilizing to have total control of your network's traffic and

security.

Example tool is Wireshark

**Wireshark:**

One of the most widely used network monitoring and analysis tools, Wireshark is known for being a powerful tool for system administrators and IT professionals across the board. Wireshark detects network issues quickly and lets system administrators troubleshoot network errors in real-time. Wireshark detects suspicious activity on the network and lets administrators drill down into the traffic and find the root cause of the issue.

Main Features

* [Deep inspection of hundreds of protocols](https://www.wireshark.org/docs/dfref/), with more being added all the time
* Live capture and offline analysis
* Multi-platform: Runs on Windows, Linux, OS X, and many others
* Captured network data can be browsed via a GUI,mode with most powerful display filters
* Rich VoIP(Voice over IP) analysis
* Read/write many different capture file formats:

Down load wire shark tool

And capture analysis on protocalls

**Experiment 2:**

**Host & Services Discovery using Nmap**

**Aim:**

information gathering about the host in the respective network.. identifies the available network services by attempting to initiate many sessions to different applications with each device in a target group of devices.

Host discovery is also known as [ping scan](https://www.geeksforgeeks.org/what-is-ping/). Nmap uses options like ping or built-in script to look after ports, services, and running servers on respective IPs using [TCP](https://www.geeksforgeeks.org/what-is-transmission-control-protocol-tcp/).

### The function of Host & Service discovery in Nmap:

1. **List Scan:**A list scan generally lists the possible host without sending any packets to the targeted host.

### *$ nmap -sL Host name(Website)*

1. **Ping Sweep:**Ping sweep discovers on the basis the host is powered on.

***$ nmap -sP Host name(Website)***

1. **Disable ARP Ping:**Nmap mostly uses [ARP](https://www.geeksforgeeks.org/how-address-resolution-protocol-arp-works/) ping to discover the other host in the network. To disable ARP Ping, use option –disable-arp-ping.

***$ nmap -sn Host name - -disable-arp-ping***

1. **TCP SYN Ping:**Nmap checks whether a host is online.

***$ nmap -PS Host name***

1. **TCP ACK Ping:**Nmap checks whether the host is responding.

***$ nmap -sA Host name***

1. **IP Protocol Ping:**Nmap tries to send different packets using different protocols.

*$* ***nmap -v -PO Host name***

1. **Traceroute:**Traceroute helps to discover the following hops or pathways to the targeted host.

***$ nmap -sn –traceroute******Host name***

1. ***$ nmap -sS Host name(Website)***
2. ***$ nmap -sT Host name(Website)***

***10) $ nmap -sV Host name(Website)***

1. ***$ nmap –sO Host name(Websit****e)*