NAME Soham Desai ROLL NO-11
BATCH-B XIE ID - 202003021

# Xavier Institute of Engineering

## Department of Information Technology

## Subject: CNND (SE SEM IV)

### AY- 2021-22

## Lab Assignment 2

**Q. 1. What Is Ping Utility? What is Ping of Death attack? How is it performed? Discuss methods to mitigate this attack. (LO1)**

Ans:

- A ping (Packet Internet or Inter-Network Groper) is a basic Internet program that allows a user to test and verify if a particular destination IP address exists and can accept requests in computer network administration. The acronym was contrived to match the submariners' term for the sound of a returned sonar pulse.
- A Ping of death (PoD) attack is a denial-of-service (DoS) attack, in which the attacker aims to disrupt a targeted machine by sending a packet larger than the maximum allowable size, causing the target machine to freeze or crash.
- A correct Internet Protocol version 4 (IPv4) packet is formed of 65,535 bytes, and most legacy computers cannot handle larger packets. Sending a ping larger than this violates the IP, so attackers send packets in fragments which, when the targeted system attempts to reassemble, results in an oversized packet that can cause the system to crash, freeze, or reboot.
- To mitigate the losses caused due to Ping Of Death Attack, various websites are strengthening their inbuilt security parameters to block the ICMP ping messages.
- An alternative method can be blocking the fragmented pings from your device. This would prevent the size of packet recombination from exceeding the permissible levels. It means that the pings can pass your system in an unhindered manner.
- Increasing the memory buffer can be another way to stay protected from the Ping Of Death Attacks.

NAME Soham Desai ROLL NO-11
BATCH-B XIE ID - 202003021

**Q.2. What is Network Simulation? Discuss various types of simulators available. Compare network simulator and network emulation. (LO2)**

Ans:

A network simulator is a software program that can predict the performance of a computer network. Since communication networks have become too complex for traditional analytical methods to provide an accurate understanding of system behavior, network simulators are used. In simulators, the computer network is modeled with devices, links, applications, etc., and the network performance is reported. Simulators come with support for the most popular technologies and networks in use today such as 5G, Internet of Things (IoT), Wireless LANs, mobile ad hoc networks, wireless sensor networks, vehicular ad hoc networks, cognitive radio networks, LTE etc.

The different types of network simulators/ network simulation tools are open source and commercial

- Network Simulator version 2 (NS-2)
- Ns3
- Netkit
- Marionnet
- JSIM (Java-based Simulation)
- OPNET
- QualNet
- The open-source simulators are Marrionet, Netkit, NS2, JSIM
- The commercial simulators are OPNET and QualNet

Network simulators:
On a basic level, a network simulator uses mathematical formulas to create a theoretical and entirely virtual model of a network. Simulators are software solutions and different types are available for different applications. While used primarily for research and educational purposes, they can also act as crucial testing tools in the design and development of a network.

Simulators, such as ns-3, are used to simulate networking and routing protocols. OPNET, which was acquired by Riverbed in 2012 and applied to their SteelCentral product line, also provided a standalone simulation environment.

Both of these network simulators use *discrete event simulation* which chronologically queues and processes events like data flow. This allows a network architect or engineer to build and evaluate an experimental model of a network, including its topology and application flow. Since a variety of theoretical scenarios can be introduced to a network where anything can be built and applied, performance can be hypothesized before the network itself has even been implemented within the real-world.

Network emulators:
A network emulator, also referred to as a *WAN emulator*, is used to test the performance of a real network. These devices can also be used for such purposes as quality assurance, proof of concept, or troubleshooting. Available as hardware or software solutions, a network emulator allows network architects, engineers, and developers to accurately gauge an application's responsiveness, throughput, and quality of end-user experience prior to applying making changes or additions to a system.

By physically placing it between two LAN segments, a network emulator can accurately replicate a client/server WAN connection without the need for a router, modem, or even live traffic. It can then be configured to manipulate bandwidth constraints and apply impairments, such as packet loss, delay, and jitter, to the mirrored network. Latency can be specified to emulate the transfer of data over large distances and applications behave and respond as if they're actually physically separated. Application performance and end-user experience can then be observed, tested, and validated under such conditions in real-time.

Software solutions, such as NetEm, which comes prepackaged within the Linux kernel, are ideal for testing at low data rates, but are limited by the testing machines on which they're run.

**Q.3. What is network performance? Discuss various ways to measure network performance. Also list tools available to measure network performance. (LO3)**

**Ans:**

- Network performance is the analysis and review of collective network statistics, to define the quality of services offered by the underlying computer network.
- It is a qualitative and quantitative process that measures and defines the performance level of a given network. It guides a network administrator in the review, measure and improvement of network services.
- When optimizing network performance there are important metrics that must be measured. Some common metrics used to measure network traffic performance include latency, packet loss indicators, jitter, bandwidth, and throughput.
- Top ten network monitoring tools:

  While network monitoring tools focus on aspects like performance monitoring, fault monitoring, and account monitoring, they're also used to examine components such as applications, email servers, and more. While there are several network monitoring tools available in the market, choosing the right device with in-depth research and tracking capability is challenging.

  - SolarWinds Network Performance Monitor
  - Nagios
  - Zabbix
  - Spiceworks
  - Icinga
  - PRTG Network Monitor

- Site 24×7
- Atera
- ManageEngine OpManager
- Zenoss Cloud

**Q.4. What is Socket programming? Discuss in detail. (LO4)**

**Ans:**

- A socket is a communications connection point (endpoint) that you can name and address in a network. Socket programming shows how to use socket APIs to establish communication links between remote and local processes.
- The processes that use a socket can reside on the same system or different systems on different networks. Sockets are useful for both stand-alone and network applications. Sockets allow you to exchange information between processes on the same machine or across a network, distribute work to the most efficient machine, and they easily allow access to centralized data. Socket application program interfaces (APIs) are the network standard for TCP/IP. A wide range of operating systems support socket APIs. i5/OS sockets support multiple transport and networking protocols. Socket system functions and the socket network functions are threadsafe.
- Programmers who use Integrated Language Environment® (ILE) C can refer to this topic collection to develop socket applications. You can also code to the sockets API from other ILE languages, such as RPG.
- The Java™ language also supports a socket programming interface.

**Q.5. Why is network design important? Discuss various tools available for network design. (LO6)**

**Ans:**

Networks that are part of a designed plan rather than those who are just pieced together, perform typically better due to taking into consideration the needs of the network. A good network design will be more robust and allow for better performance overall. Good networks work quickly and efficiently, providing the best platform for all the applications that you wish to use. If there is lag or delayed response time, then any work which is trying to be done by employees will be affected, this is one of the reasons why it's important to consider the network design first before implementing any changes or when starting the initial installation.

- **Strong Networks Mean Scalability**

If you have a strong network, then when you need to scale you won't have to think about a re-design, rather you can increase the numbers of users and computers more easily from the original design and also minimise any potential downtime. We will verify what structure you need for the data cabling and provide quality feedback as to what installation is best. Regulated hardware and

software that is used bi the network will also ensure that you have networks that need less maintenance or updates. If you are allowing for future growth, then we can build different options into the design.

- **Improved Service Levels**

By having a fresh design and installation of cabling for your business's network, you will find that you always enjoy prompt service and performance. The range of reaction times to tasks will be much more effective and avoid in instances like loss within a client's session. Users like to login and expect the business's systems to work, so to that effect having a well-planned network design will minimise security issues as well as an increase in speed and performance.

- **Cost-effective LAN Design**

There is a chance to considerably save on costs when it comes to doing a completely fresh network design and installation, compared to working on patches of cabling. The cost of design and install could mean that you invariably save money on having to buy new hardware. The ultimate goal of cost-effective network installation from AEL Systems is that you have the type of controlled network that you need, one that provides security against risk and improves usability at the same time. We will evaluate any potential risks before proceeding with the design and installation. We will also try to look at where we can maximise performance of your currently installed data cabling system.

- **Security of Networks**

We should always consider the security of the networks, with the goal being to avoid any attacks being repeated throughout the business. A disaster recovery plan is also part of any network design and there should be provisions for backup power where needed. On a side note, and pertaining to the safety of business's data, data should also be backed up daily to minimise risk of loss should anything happen to the systems due to fire or other security breach.

1. **SolarWinds Network Topology Mapper**
2. **CADE**
3. **Dia Diagram Editor**
4. **Microsoft Visio**