Assignment # 6

Problem 4. Problems in chat application using peer-to-peer model:

Since P2P systems inherently rely on the dependence of peers with each other, security implications arise from abusing the trust between peers. In a traditional client-server model, internal data need not be exposed to the client, but with P2P, some internals must be exposed to fellow peers in the name of distributing the workload. Attackers can leverage this in compromising P2P networks.

There are multiple security issues like:

1. **Distributed Denial-of-Service :** In a traditional denial-of-service (DoS) attack, a server is usually the target of massive connections, rendering the server inoperable. A classic example of this is a TCP SYN flood attack, in which the client sends the server a SYN message, the server responds with a SYN-ACK message, and the server awaits an ACK message from the client. However, the attacking client simply does not reply with an ACK message, hence tying up server resources (memory) as it futilely waits. Meanwhile, the client can continue to open many more new non-ACK'ed connections, bring the server ultimately to its knees, and hence a denial-of-service to other legitimate clients.

2. **Poisoning the Network :** Another approach towards attacking a P2P network is to inject useless data (poison) into the system. Since P2P networks must implement a lookup service in some way, whether it be a centralized directory or a DHT, an attacker can inject large amounts of useless lookup key-value pairs into the index. Bogus items in the index could slow down query times or, worse, yield invalid queries results.

3. **Privacy and Identity :** P2P networks also present privacy and identity issues. In respect to privacy, a peer's data stream may be compromised by fellow peers who assist in transmitting the data. A direct example is that of VoIP applications, such as Skype, which route traffic in a P2P fashion. Though the data stream is encrypted, a peer which carries the stream now has direct access to the data packets, which would not be the case in traditional routing.

Problem 6:

1. DNS: Domain Name System : Binds the specific domain names with their corresponding IP addresses.

DHCP: Dyanmic Host Configuration Protocol : Dynamically assigning network configurations such as IP addresses to systems in a network.

2. TCP is more reliable as it manages message acknowledgment, retransmission and timeout but in UDP there is no concept of acknowledgment, retransmission, or timeout.
In TCP, if two messages are sent over a connection in sequence, the first message will reach the receiving application first where as in UDP no such sequencing is ensured.

3. Layers are kind of abstractions done in the network configuration in order to achieve effective managment of network. Every layer has a set of particular tasks which they perform and also maintains a hierarchy of tasks from very basic to advanced ones.

4. Home folder of a perticualar student account is same irrespective of where you access it. File-system if of type **ext4.**
10.8.0.200

```
Server:		127.0.1.1
Address:	127.0.1.1#53

200.0.8.10.in-addr.arpa	name = nis.complab.kmd.user.svr.
```

I think it corresponds to the computer lab's admin IP address.

5. BSNL and Reliance.

6. As we are using a proxy and DNS server which provides us a virtual IP address coressponding to our IIT Mandi network, we are not located by outside servers directly. That's why, ip2location.com is unable to locate our physical address as proxy server is maintaining annonymity for us.

7. Its the student gateway of IIT Mandi.

8. **0.0.0.0:** NXDOMAIN i.e. non-existent domain
255.255.255.255: No reply from here but probably its also a NXDOMAIN.

9. No, we can't do it inside IIT Mandi. As we can't process the outside world's request without proxy server which assigns a dynamic IP address to each packet and thus we can't say which packet belonged to which user.
Yes, from home, we can build a web server from our laptop.

10. We can't go beyond our gateway while using traceroute as it is blocked due to security reasons.