**CONTENTS:**

* Introduction
* What is IP Spoofing
* Types Of Spoofing
* IP Datagram
* IP Spoofing Mechanism
* Types of IP Spoofing
* Preventing IP Spoofing
* Advantages
* Disadvantages
* Services vulnerable to IP spoofing
* Feature Scope
* Conclusion

**INTRODUCTION:-**

IP spoofing as a method of attacking a network in order to gain unauthorized access. The attack is based on the fact that Internet communication between distant computers is routinely handled by routers which find the best route by examining the destination address , but generally ignore the origination address. The origination address is only used by the destination machine when it responds back to the source. In a spoofing attack, the intruder s ends mess ages to a computer indicating that the message has come from a trusted system. To be successful, the intruder must first determine the IP address of a trusted system, and then modify the packet headers to that it appears that the packets are coming from the trusted system.

In April 1989, a Steve Bellovin of AT&T was one of the first people to identify IP spoofing as real risk to all computer networks. Robert Morris, the creator of the quite famous Internet Worm, had figured out how TCP made sequence numbers and forged a TCP sequence packet. This packet had included the destination address of the ‘victim’ and using the IP spoofing attack, Morris was able to gain root access to the victims system without a password or user name.

A common misconception is that "IP spoofing" can be used to hide your IP address while surfing the Internet, chatting on-line, sending e-mail, and so forth. This is generally not true. Forging the source IP address causes the responses to be misdirected, meaning you cannot create a normal network connection. However, IP spoofing is an integral part of many network attacks that do not need to see responses (blind spoofing). Although the popularity of these cracks, or spoofs, have been decreased due to the collapse of these services they had exploited, spoofing still can be used which, therefore, needs to be addressed by all, if possible, security administrators.

In the subsequent pages of this report, we will examine the concept of IP Spoofing:

What it is?

How it is?

**WHAT IS IP SPOOFING:-**

IP Spoofing is the creation of IP packets with a forged source. IP Spoofing is the process of replacing the source IP address with the fake IP address to hide the real identity of the sender.

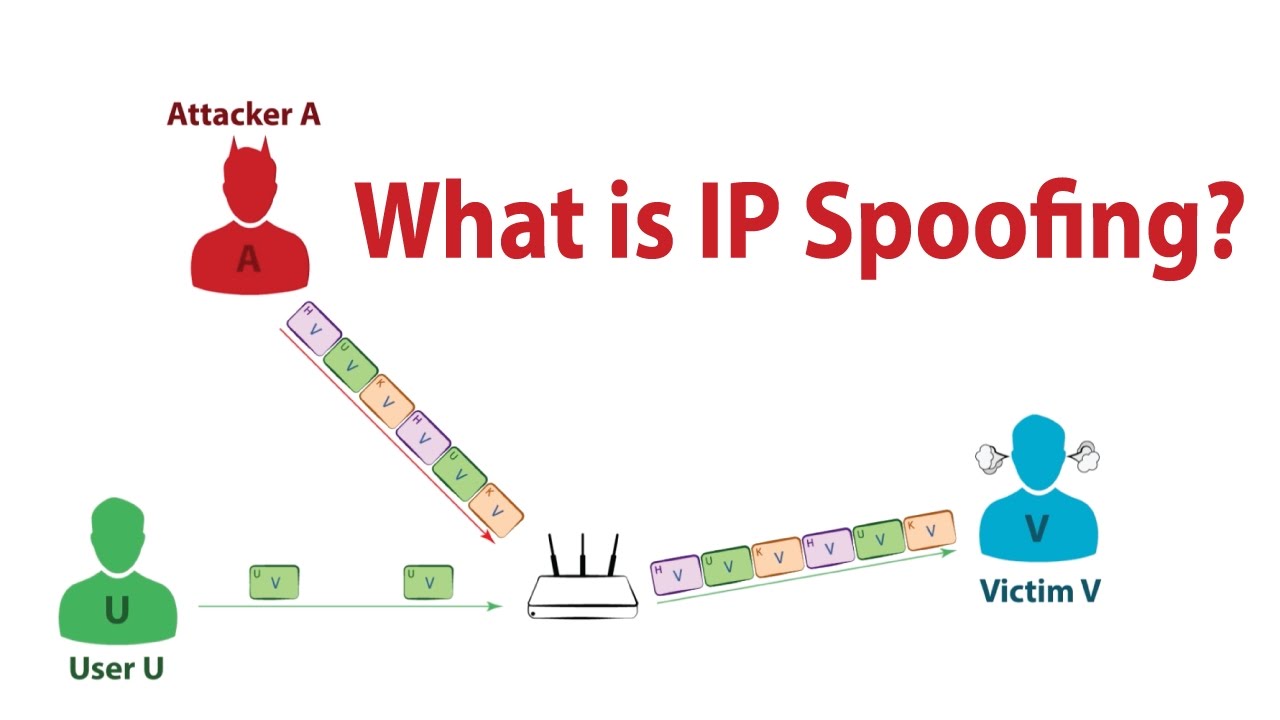
IP spoofing is a technique used to gain unauthorized access to computers, whereby the attacker sends messages to a computer with a forging IP address indicating that the message is coming from a trusted host.

Internet protocol (IP) is a network protocol which operates on the Network (3) Layer of the OSI model. This doesn’t contain information regarding the transaction state, where you would use this to route packets on a particular network, because it is a connectionless model. In addition, there is no means in place to make certain that a packet is correctly delivered to the destination.

It is similar to the process of sending the letters between two persons. Let us consider three persons living in different cities. The person living in one city will receive letter from one of the remaining two persons but the address of the letter was the address of the another person. But the person who received the letter thinks that the letter was written by the person with that address and the send reply to that letter.

As the communication between two persons is done through letters, similarly in internet or network the data communication is done in the form of sending packets. Each packet consists of IP header or the address. Here in IP spoofing the packet will be sent by one person with the IP address of another person. That is the sender is hiding his identity and sending the data packets.

The following diagram will represent the process of IP spoofing



From the above figure you can observe three actors – User U, Victim V, Attacker A. The User U in above diagram used to communicate with the Victim V through router by sending the data in the form of packet with his IP address. So let us consider the IP address as the green colour packet. So now the Victim V will identify that the packets which are in green colour are received from the User U. But here the role of the attacker comes into the attack. Here the main aim of the Attacker A is to send the IP packets with the forged source i.e. sending the packet with the IP address of another person by hiding his identity.

If you clearly observe the figure you can see only packets of one colour are from the User U, but if observe the packets from the Attacker A you can see packets of different colours likes green, orange, violet etc. Here each colour represents the packets of different users. Base on the colour the Victim V thinks that the packet was sent by the particular User U but in original the data packets are sent by the Attacker A.

So in this way the spoofing will be done by the attacker by sending the forged IP packets.

The IP spoofing is performed by the attacker in different ways .There are about four main types of IP spoofing which are explained in further.

**TYPES OF SPOOFING**:-

There are four types of IP spoofing. They are

1. Email Spoofing
2. Caller ID Spoofing
3. Website Spoofing
4. ARP Spoofing

**1. Email Spoofing**:-

Email spoofing occurs when an attacker uses an email message to trick a recipient into thinking it came from a known and/or trusted source. These emails may include links to malicious websites or attachments infected with malware. Sender information is easy to spoof and can be done in one of two ways:

* Mimicking a trusted email address or domain by using alternate letters or numbers to appear only slightly different than the original
* Disguising the ‘From’ field to be the exact email address of a known and/or trusted source

**2. Caller ID Soofing:-**

With caller ID spoofing, attackers can make it appear as if their phone calls are coming from a specific number—either one that is known and/or trusted to the recipient, or one that indicates a specific geographic location. Attackers can then use social engineering—often posing as someone from a bank or customer support to provide sensitive information such as passwords, account information, social security numbers, and more.

**3. Website Spoofing:-**

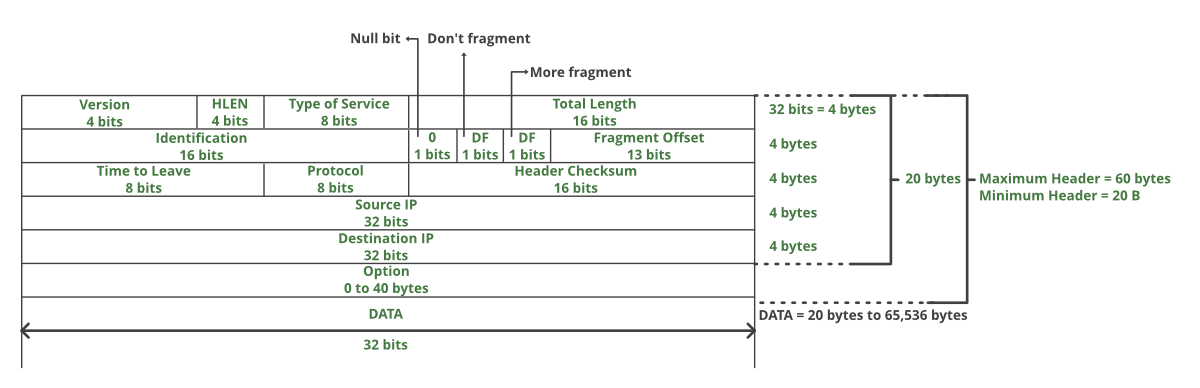
Website spoofing refers to when a website is designed to mimic an existing site known and/or trusted by the user. Attackers use these sites to gain login and other personal information from users.

**4. ARP Spoofing:-**

Address Resolution Protocol (ARP) is a protocol that resolves IP addresses to Media Access Control (MAC) addresses for transmitting data. ARP spoofing is used to link an attacker’s MAC to a legitimate network IP address so the attacker can receive data meant for the owner associated with that IP address. ARP spoofing is commonly used to steal or modify data but can also be used in denial-of-service and man-in-the-middle attacks or in session hijacking.

**IP DATAGRAM**

The network layer is the third layer (from bottom) in the OSI Model. The network layer is concerned with the delivery of a packet across multiple networks. The network layer is considered the backbone of the OSI Model. It selects and manages the best logical path for data transfer between nodes.



**VERSION*:*** Version of the IP protocol (4 bits), which is 4 for IPv4

**HLEN*:*** IP header length (4 bits), which is the number of 32 bit words in the header. The minimum value for this field is 5 and the maximum is 15.

**Type of service*:***Low Delay, High Throughput, Reliability (8 bits)

**Total Length:**Length of header + Data (16 bits), which has a minimum value 20 bytes and the maximum is 65,535 bytes.

**Identification*:*** Unique Packet Id for identifying the group of fragments of a single IP datagram (16 bits)

**Flags*:*** 3 flags of 1 bit each reserved bit (must be zero), do not fragment flag, more fragments flag (same order)

**Fragment Offset*:*** Represents the number of Data Bytes ahead of the particular fragment in the particular Datagram. Specified in terms of number of 8 bytes, which has the maximum value of 65,528 bytes.

**Time to live*:*** Datagram’s lifetime (8 bits), It prevents the datagram to loop through the network by restricting the number of Hops taken by a Packet before delivering to the Destination.

**Protocol*:***Name of the protocol to which the data is to be passed (8 bits)

**Header Checksum*:*** 16 bits header checksum for checking errors in the datagram header

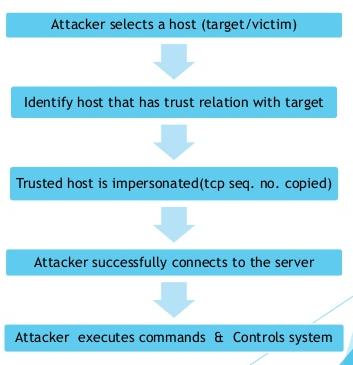
**Source IP address*:*** 32 bits IP address of the sender

**Destination IP address:** 32 bits IP address of the receiver

**Option:** Optional information such as source route, record route. Used by the Network administrator to check whether a path is working or not.

**IP SPOOFING MECHANISM**

The IP Spoofing Mechanism describes the step by step process of how spoofing will be done by the attacker. As shown in the below figure first the attacker selects a host (target/victim). After selecting the victim he selects the host that is having trust relationship with the target. Later the TCP sequence number which is communicated between the two is copied by the attacker. With the sequence number copied by the attacker the attacker successfully connects to the victim server. Now he starts sending the data packets with the forges IP address to the victim. Finally in the last step the attacker execute the commands and controls system.



**TYPES OF IP SPOOFING ATTACKS**

There are four types of IP Spoofing. They are

1. Blind Spoofing Attack

2. Non Blind Spoofing Attack

3. Man in the Middle Attack

4. Denial of Service (DOS) Attack

**1**. **Blind Spoofing Attack:-**

In Blind spoofing the attacker does not have access to reply. This is because the attacker in spoofing will send the data packet with the forged IP address of another user, so when the victim receives the packet then he then gives reply to the IP address from which the packet has come . Since the packet is sent by the attacker and the IP address in that packet is forged so the victim will send reply to the IP address present in the packet.

Let us consider an example which explains the blind spoofing.

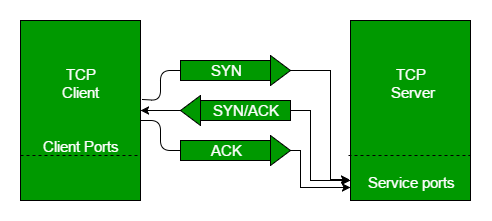


**Example:** Here in this example HOST C will act as an attacker, he will send the IP packet with the address of some other host (HOST A) as the source address to HOST B. Now based on the address on the packet the HOST B thinks that the packet was sent by HOST A and replies to HOST A. Here the HOST C is not having any access to reply.

Before going to non-blind spoofing attack you need to know about the TCP handshake process.

**TCP HANDSHAKE PROCESS:-**

TCP stands for Transmission Control Protocol which indicates that it does something to control the transmission of the data in a reliable way. The process of communication between devices over the internet happens according to the current **TCP/IP** suite model(stripped out version of OSI reference model). The two important protocols of this layer are – TCP, **UDP (User Datagram Protocol)** out of which TCP is prevalent (since it provides reliability for the connection established). However you can find application of UDP in querying the DNS server to get the binary equivalent of the Domain Name used for the website.



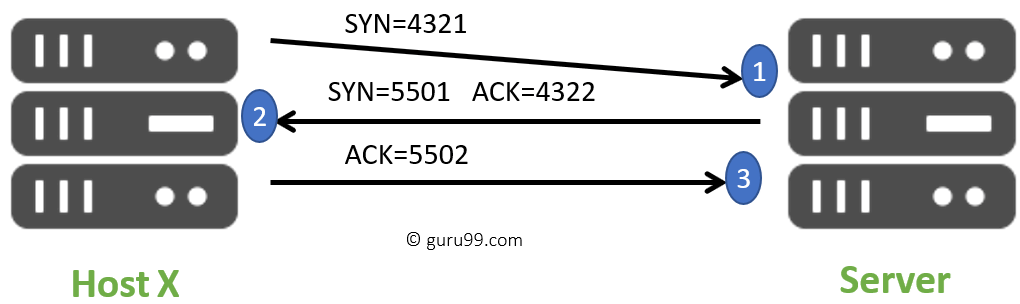
TCP provides reliable communication with something called **Positive Acknowledgement with Re-transmission (PAR)**. You can realize from above mechanism that three segments are exchanged between sender(client) and receiver(server) for a reliable TCP connection to get established. Now let us discuss step by step how TCP handshake process takes place.

 Step **1 (SYN):** In the first step, client wants to establish a connection with server, so it sends a segment with SYN (Synchronize Sequence Number) which informs server that client is likely to start communication and with what sequence number it starts segments with.

 Step **2 (SYN + ACK):** Server responds to the client request with SYN-ACK signal bits set. Acknowledgement (ACK) signifies the response of segment it received and SYN signifies with what sequence number it is likely to start the segments with.

 Step **3 (ACK):** In the final part client acknowledges the response of server and they both establish a reliable connection with which they will start the actual data transfer.

The steps 1, 2 establish the connection parameter (sequence number) for one direction and it is acknowledged. The steps 2, 3 establish the connection parameter (sequence number) for the other direction and it is acknowledged. With these, a full-duplex communication is established. One of the real world example is.



The packets contain a random sequence number (For example, 4321) that indicates the beginning of the sequence numbers for data that the Host X should transmit.

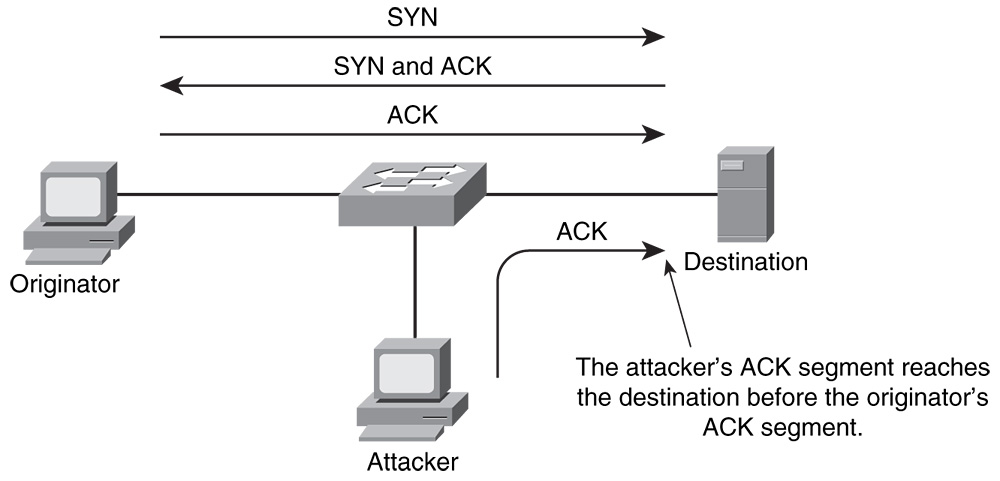
After that, the Server will receive the packet, and it responds with its sequence number. It's response also includes the acknowledgment number, that is Host X's sequence number incremented with 1 (Here, it is 4322).

Host X responds to the Server by sending the acknowledgment number that is mostly server's sequence number that is incremented by 1.

After the data transmission process is over, TCP automatically terminates the connection between two separate endpoints.

**2**. **Non-** **Blind Spoofing Attack:-**

This type of attack takes place when the attacker is on the same subnet as the victim. The sequence and acknowledgement numbers can be sniffed, eliminating the potential difficulty of calculating them accurately. The biggest threat of spoofing in this instance would be session hijacking. This is accomplished by corrupting the data stream of an established connection, then re-establishing it based on correct sequence and acknowledgement numbers with the attack machine. Using this technique, an attacker could effectively bypass any authentication measures to build the connection. The diagrammatic representation of Non blind Spoofing is as follows.

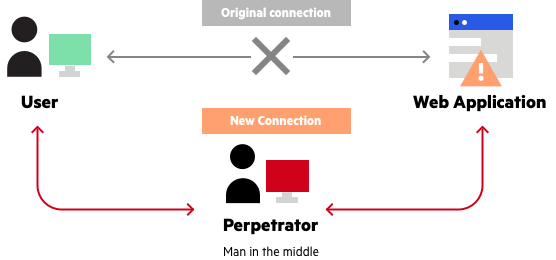
****

As shown in the above figure here the attacker also will be in the same host. He hacks the sequence number and the acknowledgement number and captures the communication channel between two hosts.

**3**. **Man in The Middle Attack:-**

This attack is also known as connection oriented hijacking. In this attack mainly the attacker or the interrupter will attack the legal communication between two parties and eliminates or modifies the information shared between the two hosts without their knowledge. This is how the attacker will fool a target host and steal the data by forging the original host’s identity. The goal of an attack is to steal personal information, such as login credentials, account details and credit card numbers. Targets are typically the users of financial applications, SaaS businesses, e-commerce sites and other websites where logging in is required.

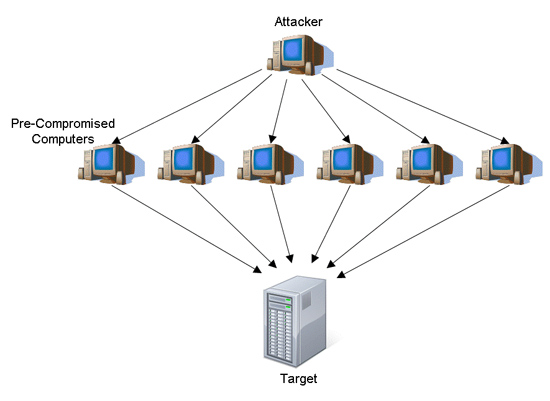
Information obtained during an attack could be used for many purposes, including identity theft, unapproved fund transfers or an illicit password change. The Man in the middle attack comes under active attack.



**4**. **Denial of Service (DOS) Attack:-**

It means a single attacker attacking the single target. A denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. Services affected may include email, websites, online accounts (e.g., banking), or other services that rely on the affected computer or network. A denial-of-service condition is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users. DoS attacks can cost an organization both time and money while their resources and services are inaccessible. DOS attack is an attack made by the hackers to make a network resource unavailable. Attackers are concerned with consuming bandwidth and resources by flooding the target with as many packets as possible in short amount of time.

Below is the diagrammatic representation of the denial of service attack.

****

**PREVENTING IP SPOOFING**

There are many tools and practices that organizations can employ to reduce the threat of spoofing attacks. Common measures that organizations can take for spoofing attack prevention include:

* **Packet filtering:** Packet filters inspect packets as they are transmitted across a network. Packet filters are useful in IP address spoofing attack prevention because they are capable of filtering out and blocking packets with conflicting source address information (packets from outside the network that show source addresses from inside the network and vice-versa).
* **Avoid trust relationships:** Organizations should develop protocols that rely on trust relationships as little as possible. It is significantly easier for attackers to run spoofing attacks when trust relationships are in place because trust relationships only use IP addresses for authentication.
* **Use spoofing detection software:** There are many programs available that help organizations detect spoofing attacks, particularly [ARP Spoofing](https://www.veracode.com/node/663). These programs work by inspecting and certifying data before it is transmitted and blocking data that appears to be spoofed.
* **Use cryptographic network protocols:** Transport (TLS), Secure Shell (SSH), HTTP Secure (HTTPS) and other secure communications protocols bolster spoofing attack prevention efforts by encrypting data before it is sent and authenticating data as it is received.

These are the main preventing methods in IP spoofing. There are some of the preventing methods in IP spoofing they are as follows.

1. Use authentication based on key exchange between the machines on your network; something like IPsec will significantly cut down on the risk of spoofing.
2. Use an access control list to deny private IP addresses on your downstream interface.
3. Implement filtering of both inbound and outbound traffic.
4. Configure your routers and switches if they support such configuration, to reject packets originating from outside your local network that claim to originate from within.
5. Enable encryption sessions on your router so that trusted hosts that are outside your network can securely communicate with your local hosts.

**ADVANTAGES**

**1. Multiple Servers:**

Sometimes you want to change where packets heading into your network will go. Frequently this is because you have only one IP address, but you want people to be able to get into the boxes behind the one with the `real' IP address.

**2. Transparent Proxying:**

Sometimes you want to pretend that each packet which passes through your Linux box is destined for a program on the Linux box itself.

This is used to make transparent proxies: a proxy is a program which stands between your network and the outside world, shuffling communication between the two.

**DISADVANTAGES**

**1. Blind to Replies**

A drawback to IP source address spoofing is that reply packet will go back to the spoofed ip address rather than to the attacker.

This is fine for many type of attack packet. However in the scanning attack as we will see next the attacker may need to see replies .in such cases, the attacker can not use ip address spoofing.

**2. Serial attack platforms :**

However, the attacker can still maintain anonymity by taking over a chain of attack hosts. The attacker attacks the target victim using a point host-the last host in the attack chain.

Even if authorities learn the point host’s identity .They might not be able to track the attack through the chain of attack hosts all the way back to the attacker’s base host.

The transparent part is because your network won't even know it's talking to a proxy, unless of course, the proxy doesn't work.

**SERVICES VULNERABLE TO IP SPOOFING**

**1. RPC (Remote Procedure Call services)**

RPC multiplexes many services on top of one framework. Portmapper directs clients to the service that they want. Some of these services include NIS, NFS, and Exchange mail. Portmapperis usually secure, but the services below it often are not.

**2. X Window system**

You can run programs on other people's displays, snoop their keystrokes and mouse movements, lock their screens etc.

**3. R services suite (rlogin, rsh, etc.)**

To prevent these sorts of attacks, users should have uncrackable passwords, and all shell access should be strongly authenticated and encrypted.

**FEATURE SCOPE:-**

If the suggestion as given in my paper will be implemented practically; it is the most chances to free our internet from IP Spoofed Attack and also chances to explore my idea in future to enhance the security in the field of Internet & Network too.

**CONCLUSION:-**

IP spoofing is less of a threat today due to the patches to the Unix Operating system and the widespread use of random sequence receive numbering.

Many security experts are predicting a shift from IP spoofing attacks to application-related spoofing in which hackers can exploit a weakness in a particular service to send and information under false identities.

As Security professionals, we must remain current with the Operating Systems that we use in our day to day activities. A steady stream of changes and new challenges is assured as the hacker community continues to seek out vulnerabilities and weaknesses in our systems and our networks.