International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 6, September-October 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

# IP Spoofing

**Mr. Satish Bharadwaj[1], Prof. Abhijit Desai[2]**

[1]Student, [2]Asistant Professor,

[1,2]Bharati Vidyapeeth's Institute of Management and Information Technology, Navi Mumbai, Maharashtra, India

**ABSTRACT**

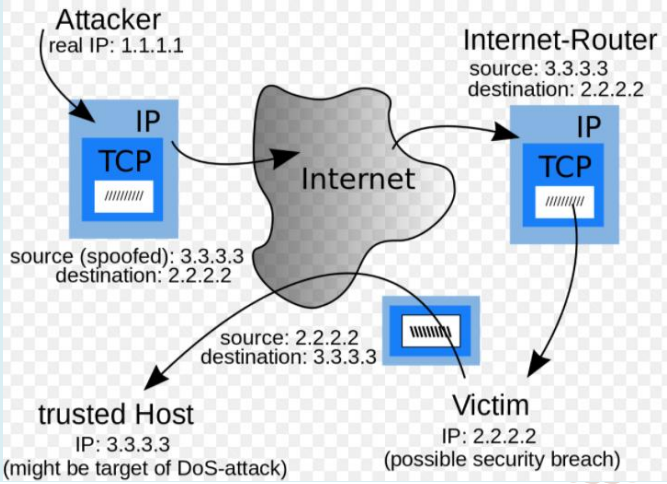
The intention behind writing this paper on this subject is to anticipate IT students or novice in the field of data communication and network security about spoofing attacks, how vulnerable and the prevention from the attacks.

Nowadays, several malicious attacks and contents are found on the internet. So, to overcome the probability of risk, it is must be implemented to prevent the end user from these.

IP address spoofing is basically a technique to alter(spoof) the packets of original source address in the header section intended to compromise or retrieve sensitive information from another trusted host or a machine.

The meaning of spoofing is to provide the false information, in the area network security and it comprises of many types which includes:

- IP ADDRESS SPOOFING
- E-MAIL SPOOFING
- WEB SPOOFING
- ARP (ADDRESS RESOLUTION PROTOCOL) SPOOFING




***How to cite this paper:*** Mr. Satish Bharadwaj | Prof. Abhijit Desai "IP Spoofing" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-6, October 2020, pp.663-664, URL: www.ijtsrd.com/papers/ijtsrd33246.pdf

IJTSRD33246



***KEYWORDS:*** *IP Spoofing, Bogus, Intrusion Detection System, Packet Filtering, Man In the Middle Attack*

## I. INTRODUCTION

IP spoofing is generally a packet filtering of data in the form of address which primarily uses a source and destination, which the attacker will spoof the source address in other words changing the header in the packets that is and request for the information via internet to the server, from their the victim gets compromised.

And the trusted host is the target of DoS attack. Once the unauthorized access is gained by the attacker, he has access to all the sensitive and confidential data and might also send malicious messages pretending to be as a trusted host.

The true identity is masked for retrieving the information from the attacked machine. Actually, the target machine is flooded with ICMP attacks that sends large number of requests to crash their system. There is also a direct attack which is known as SYN attack.

## II. Applications

Most of the attacks are dependent on the IP spoofing mechanism which triggers an attack. SMURF attack, in which number of requests are send by the attacker to the target address.

This is also known as ICMP attack. The use of Botnet is done for the attack on the systems. Nothing major resources is needed in botnet attack just a script or a command to flood the network.

Armies of infected script attack is done on a particular system, to avoid this attack anti-spoofing prevention is done. IDS (Intrusion Detection System) is also used for the prevention as detecting the intruder into the system.

## III. Prevention

"Prevention is always better than the cure", as the statement suggests anti-spoofing techniques are better

than rectifying the mistakes done. The Intrusion Detection System is utilized for the prevention of attack done on the system.

To avoid such attacks majorly the implementation of packet filtering is done. Few methods is listed below.

➢ **Ingress filtering**

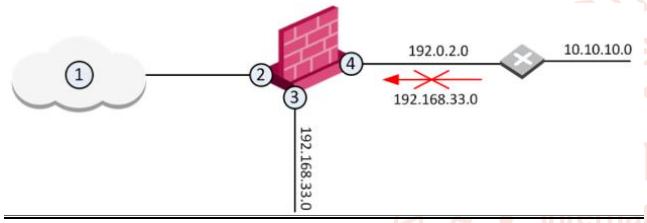
Ingress filtering is a method that assures the incoming packets are from the intended network, from which the communication is done and not from any other network which pretend to be.

It is used to prevent the companies or a corporate network from unwanted spoofing traffic.

➢ **Egress filtering**

Egress filtering is a method of monitoring and revoking the information from a network to other network.

All the packets that are sent from the inbound networks are firstly monitored via router or a firewall, if there is no match then the particular network is denied.




## IV. Advantages

"A coin has two sides", hence there is also advantage in using of ip address spoofing. The use of it is majorly done on large accounts in a corporate sector basically to test their system or network

Many organizations approaches company to grant their employees (virtual users) to test their network with different ip address by spoofing the source network. This method indicates that, if volume of end users visits their network, how would it perform.

So, the network can be improved on the basis of the result. Sometimes, the most number of visitors at the same time can crash the network.

## V. Disadvantages

Hackers (by writing scripts) and Crackers(by using tools) mostly use bogus ip address to gain unauthorized network and retrieve sensitive data or information.

They just deploy the spoofed ip address in the source header packet of the IP/TCP layer, in return to use DDoS (Distributed Denial of Service) attack. This would just cause millions or crores financially to the organization.

Man-In-The-Middle (MIMD) attack is also used to deploy malicious scripts or alter data in between conversation. This attack takes exchange of data between two networks, and then emerging as a eavesdropper in-between.

IPv4 Network Packet Headers

| | | | |
|---|---|---|---|
| Version | IHL | Type of Service | Total Length |
| Identification | | Flags | Fragment Offset |
| Time To Live | | Protocol | Header Checksum |
| Source IP Address | | | |
| Destination IP Address | | | |
| Options | | | |
| Data | | | |

## VI. Conclusion

Nowadays, this attack is not much applicable in the corporate sectors because the design of new network protocols and services is not dependent on old source header spoofing.

## VII. References

[1] T., Kirda, Egele M Scholte, E. Kruegel, C.: With Generalization and in the Anomaly-support Detection Characterization methods of Cyber Attacks. US .2006.

[2] P. M., Salvaneschiy, G., Kirdaz, E., Kolbitsch, C., Kruegel, C., Zaneroy, Comparetti, S.: searching dormant functionality in software programs maintaining the efficient of dynamic software analysis. In: IEEE Security and Privacy, Oakland May 2010.

[3] Canto, J., Dacier, M., Kirda, E., Leita, C.: Large scale software collection – lessons learned. In: IEEE SRDS Workshop on Sharing Field Information and Experiment a Measurements on Resilience of Distributed Computing Systems, Naples, Rome Oct 2008.

[4] Kruegel, C., Vigna, G., Robertson, W.: multi-model approach to detection of cyber attack. 48(5) (July 2005).