International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 3, March - 2014

# Intrusion Detection and Prevention using Blocking and Back Tracking for IP Spoofing

Mr. Ritesh Kumar
2nd year,M.Tech,
Dept. of CSE,
St.Joseph College of Enginnering
Mangalore, Karnataka, India .

Mrs. Sunita G
Prof. & HOD
Dept. of CSE,
St.Joseph College of Enginnering
Mangalore, Karnataka, India .

Ms. Rajeshwari M
2nd year, M.Tech, Dept. of ISE,
NMAMIT – Nitte, Karnataka, India.

***Abstract*— Forging, or" spoofing," the IP addresses of sender, intermediate or receiver nodes provides malicious parties with anonymity and novel attack vectors. Spoofing-based attacks complicate network operator's defense techniques, tracing spoofing remains a difficult and largely manual process. Hence we come up with a technique called Back Tracking using hashing approach. We use an efficient encryption and decryption technique to keep the message safe and we also append the IP addresses of sender, intermediate nodes through whom the message is either sent or forwarded, the receiver node will get the IP addresses of all such nodes along with the decrypted message.**

***Keywords—IP addresses, Back Tracking, Encryption, Decryption.***

## I. INTRODUCTION

Internet Protocol spoofing is a method of attacking a network in order to gain unauthorized access [1]. 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. Only the destination machine responds back to the source using origination address. In spoofing attack, the intruder sends message to the node predicting him as a trusted system. To be successful, the intruder must determine the IP address of a trusted system. The recent attacks using IP spoofing are man in the middle, routing redirect, source routing, blind spoofing and flooding. IP spoofing is commonly associated with malicious network activities, such as [7].Distributed Denial of Service (DDoS) attacks, which block legitimate access by either exhausting victim server's resources or saturating stub networks access links to the Internet. The IP Source Guard feature works very well for interfaces with a single IP address, but one interface can be assigned multiple IP addresses, and that may cause problems. The best method of preventing the IP spoofing problem is to install a filtering router that restricts the input to your external interface (known as an input filter) by not allowing a packet through if it has a source address from your internal network.

IP Spoofing may be a drawback while not a simple answer, since it's inherent to the planning of the TCP/IP suite. Understanding however and why spoofing attacks are used, combined with a number of straightforward interference ways, will facilitate defend your network from these malicious cloaking and cracking techniques. The speedy enhancements of intrusions in web and alternative networks are the most factors accountable for the propagation of various threats and vulnerabilities within the computing surroundings. Thus we have a tendency to try and implement procedures known as block and backtracking to observe the entrant within the network similarly as stop him from intrusive the network by tracing back every hop and decisive at that node the wrongdoer spoofs the network.

Trace back technology plays a very important role in discovering the supply of spoofed packets. Hop-by-hop trace back and work of suspicious packets in routers are the 2 main ways for tracing the spoofed IP packets back to their supply.

When a node detects that it's a victim of flood attack, it will inform the net Service supplier (ISP). Overflowing attacks the ISP will confirm the router that's causing this stream to the victim, and so it will confirm consequent router, and so on. It reaches either to the supply of the flood attack or the top of its body domain; for this case it will raise the ISP for consequent domain to try and do an equivalent issue. This method is beneficial providing the flood is in progress.

IP spoofing may be a tough drawback to tackle; as a result of its associated with the IP packet structure. IP packets are exploited in many ways in which. As a result of attackers will hide their identity with IP spoofing, they will build many network attacks. Though there's no simple answer for the IP spoofing drawback, you will apply some straightforward proactive and reactive ways at the nodes, and use the routers within the network to assist observe a spoofed packet and trace it back to its originating supply.

IP Networks are vulnerable to source address spoofing. For example, a compromised Internet host can spoof IP packets by using a raw socket to fill arbitrary source IP addresses into

packet headers. IP spoofing consists of following steps.

- Selecting a target host (or victim)
- Identify the host that has a trust relationship with a target host
- The trusted host is then disabled and the target's TCP sequence numbers are sampled
- The trusted host is then impersonated, the sequence numbers forged
- A connection attempt is made to a service that only requires address-based authentication (no user id or password).

Thus, the proposed system detects and prevents the intruder at intermediate level using the scheme backtracking and blocking methods.

## II. PROBLEM STATEMENT

In Existing system, route-based packet filters method, each node has individual path for destination. It is detected by using Border Gate way Protocol (BGP). BGP determines the path of node name which is inside the Packet header, this path is appended with packet header. Inter domain packet filter (IDPF) takes decision about passing packets or discarding packets, so inter domain IP spoofing is avoided by using this method. It is efficient for detecting IP Spoofing attack. We present an algorithmic complexity attack that exploits worst-case signature matching behavior in a NIDS. By carefully constructing packet payloads, our attack forces the signature matcher to repeatedly backtrack during inspection, yielding packet processing rates that are up to 1.5 million times slower than average. We term this type of algorithmic complexity attack a backtracking attack. Our experiments show that hundreds of intrusions can successfully enter the network undetected during the course of a backtracking attack against a NIDS. Further, the backtracking attack itself requires very little bandwidth; i.e., a single attack packet sent once every three seconds is enough to perpetually disable a NIDS.

The fundamental idea of this scheme to utilize inherent network information that each packet carries and an attacker cannot easily forge to distinguish spoofed packets from legitimate ones. [2].The inherent network information we use here is the number of hops a packet takes to reach its destination: although an attacker can forge any field in the IP header, he cannot falsify the number of hops an IP packet takes to reach its destination, which is solely determined by the Internet routing infrastructure. The hop-count information is indirectly reflected in the Time-to-Live (TTL) field of the IP header, since each intermediate router decrements the TTL value by one before forwarding a packet to the next hop. The rationale behind Hop-Count Filtering (HCF) is that most randomly spoofed IP packets, when arriving at victims, do not carry hop-count values that are consistent with the IP addresses being spoofed. [4].As a receiver, an Internet server can infer the hop-count information and check for consistency of source IP addresses. Exploiting this observation, HCF builds an accurate IP-to-hop count (IP2HC) mapping table, while using a moderate amount of storage, by clustering address prefixes based on hop count.

## III. PROJECT SCOPE

Trace back technology plays a very important role in discovering the supply of spoofed packets. Hop-by-hop trace back and work of suspicious packets in routers are the 2 main ways for tracing the spoofed IP packets back to their supply. When a node detects that it's a victim of flood attack, it will inform the net Service supplier (ISP).

Overflowing attacks the ISP will confirm the router that's causing this stream to the victim, and so it will confirm consequent router, and so on. It reaches either to the supply of the flood attack or the top of its body domain; for this case it will raise the ISP for consequent domain to try and do an equivalent issue. This method is beneficial providing the flood is in progress.

The scope of project is to develop a blocking and backtracking architecture that can mitigate the level of IP spoofing on the internet. The feature of the scheme is to use a predefined path for data transfer. Spoofing at source node and destination node is basically eliminated.

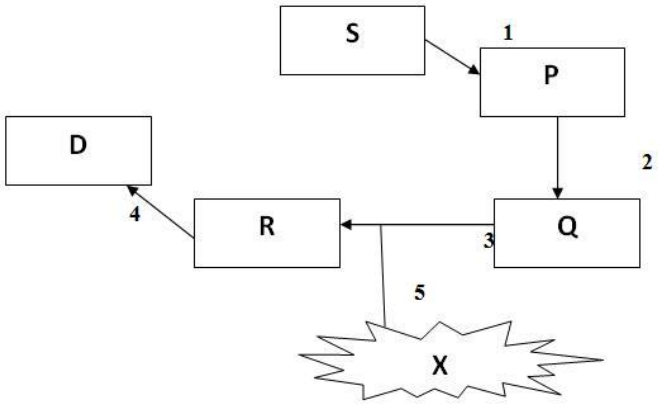
The key objectives are:

1. Blocking the intruder at the intermediate level and blacklisting the intruder.

2. Controlling the IP spoofing through backtracking.

## IV. METHODOLOGY

### *A. Architecure*




*a) : Source S sends a data to intermediate node P.*

*b) : Intermediate node P forwards the data to intermediate node Q.*

*c) : Intermediate node Q forwards the data to intermediate node R.*

*d) : Intermediate node R forwards the data to destination D.*

*e) :When intermediate node Q sends the data to intermediate node R (3), intruder X tries to spoof the data on the connection 3. In this case either intermediate node R*

*blocks the data from intruder X or it forwards the data to destination D where destination D uses the backtrack algorithm to check the identity of the nodes.*

*B. Functionalities of Different Nodes*

*a) Enrollment:* In an enrollment page which cosists of different nodes which can be selected, it can be either sender, intermediate or receiver, we fetch the corresponding IP addresses from the respective database.

*b) Sender:* An IP address of the receiver from the database is fetched, enter the subject and message which are mandatory and needs to entered compulsarily, then there is a optional attachment box where we can use and update either text or pdf files. When we click the continue button, the message in the message box will be encypted by appending the sender's IP address using a Rijndael algorithm and random key generation algorithm is also called in the process to generate a key for this algorithm, Or on the other hand we can click a change roll key in order to change its mode of operation.

*c) Intermediate:* This particular node just forwards the message that is sent by the sender. In the mean time the message is decypted and the intermediate nodes IP address needs to be added to that message and encypt this particular message. The same process is carried by all the intermediate nodes that come in this process.

*d) Receiver:* In this node the decyption of the message is performed and the message along with the senders and intermediate nodes IP addresses are retrieved. The communication of this nodes funtion in a same manner.

*e) Intruder:* Intruder is the person who tries to spoof the message by altering the IP address of either sender or intermediate node.

## V. BACK TRACKING AND BLOCKING

[1].Back Tracking algorithm is designed in such manner that we take the IP addresses appended to the message from the inbox table and transaction table of the database. We compare both the tables and if there is any change or alteration of IP addresses in these tables then we get to know that the particular IP address is being spoofed, we also can determine the node at which the IP address is being spoofed.

Blocking is a phase in which once the Back Tacking algorithm is efficiently executed then we determine the IP address which is trying to spoof the message, for a predefined number of times that particular IP address is allowed once that particular IP crosses that predefined number it is permanently blocked from using that particular network[5].

## VI. CONCLUSION

The purpose of this study is to try and prevent IP spoofing attacks. This paper gives a brief idea about Back Tracking and Blocking of IP addresses who illegitimately try spoof a network and also a brief idea about how an efficient communication process is carried out using suitable encryption and decryption techniques which helps in secure communication.

## ACKNOWLEDGMENT

I take this opportunity to express my profound gratitude and deep regards to my guide Mrs. Sunita G., Professor and Head of Computer Science and Engineering Department, St.Joseph Engineering College, Vamanjoor, for her exemplary guidance, and constant encouragement throughout.



## .REFERENCES

[1] Soundar Rajam, V.K.; Shalinie, S.M., "A novel traceback algorithm for DDoS attack with marking scheme for online system," Recent Trends In Information Technology (ICRTIT), 2012 International Conference on , vol., no., pp.407,412, 19-21 April 2012.

[2] Manusankar, C.; Karthik, S.; Rajendran, T., "Intrusion Detection System with packet filtering for IP Spoofing," Communication and Computational Intelligence (INCOCCI), 2010 International Conference on , vol., no., pp.563,567, 27-29 Dec. 2010.

[3] Bingyang Liu; Bi, Jun; Yu Zhu, "A deployable approach for inter-AS anti-spoofing," Network Protocols (ICNP), 2011 19th IEEE International Conference on , vol., no., pp.19,24, 17-20 Oct. 2011.

[4] http://www.bioinfopublication.org/files/articles/3_2_5_JDMKD.pdf.

[5] S.Savage, D.Wetherall, Anna Karlin, Tom Anderson, "Network support for IP Traceback", IEEE/ACM Transactions on Networking, Vol.9,No.3,June2001.

[6] https://www.sans.org/reading-room/whitepapers/threats/introduction-ip-spoofing-959S.Savage.

[7] http://ijarcet.org/wp-content/uploads/IJARCET-VOL-1-ISSUE-4-285-288.pdf.