A Study on IP Spoofing Attack and Defense in Network

A. Mahalakshmi[1], Dr. V Saravanan A[2]
Department of Information Technology
[1]PG Scholar, Hindusthan College of Arts and Science (Autonomous)
[2]Associate Professor and Head, Hindusthan College of Arts and Science (Autonomous)

Abstract-*Networks have become an integral part of today's world. The ease of deployment, low-cost and high data rates have contributed significantly to their popularity. Network introduces security problems, threats, risks and other type of attacks like internal and external attacks. Spoofing means impersonating another person or computer, usually by providing false information (E-mail name, URL or IP address). Spoofing can take on many forms in the computer world, all of which involve some type false representation of information. A technique to perform this activity is made possible by preventing the discovery of the sender's identity through IP Spoofing .This paper gives a view of IP Spoofing attack and defense in the network.*

Keywords-IP Spoofing, Non-Blind spoofing, Blind spoofing, Man-in-the-Middle Attack.

I. INTRODUCTION

IP spoofing is a technique used to gain unauthorized access to computers, where by the attacker sends messages to a computer with a forging IP address indicating that the message is coming from a trusted host. Attacker puts an internal, or trusted, IP address as its source. The access control device sees the IP address as trusted and lets it through. IP spoofing occurs when a hacker inside or outside a network impersonates the conversations of a trusted computer.

Two general techniques are used during IP spoofing:

1) A hacker uses an IP address that is within the range of trusted IP addresses.
2) A hacker uses an authorized external IP address that is trusted.

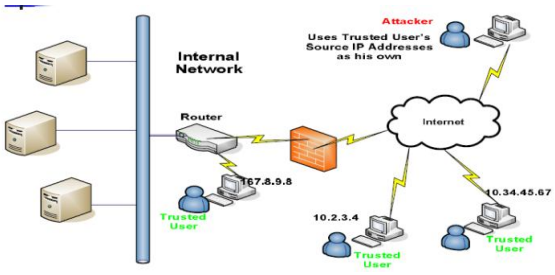

Fig 1: IP Spoofing

II. ATTACKS THROUGH IP SPOOFING

There are a few variations on the types of attacks that successfully employ IP spoofing. Although some are relatively dated, others are very pertinent to current security concerns.

Non-Blind Spoofing

Non-Blind Spoofing attacks work on those networks where the attacker and victim are on the same subnet. In this situation, the attacker can sniff the network packets to know the sequence and acknowledgement numbers being sent in the packets. The biggest threat of spoofing in this type of attack would be session hijacking. This can be done by corrupting the data stream of an established connection with a valid user, then re-establishing the connection based on the correct sequence and acknowledgement numbers with the attack machine.

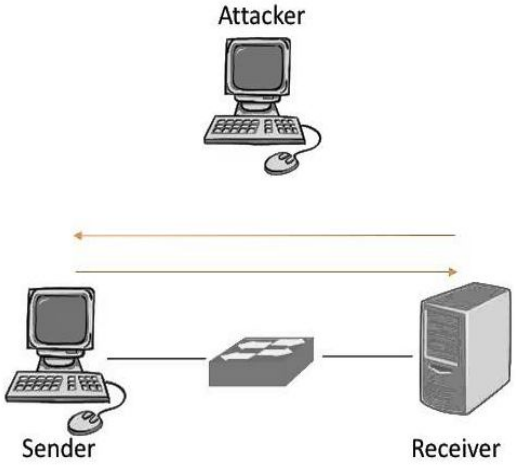

Fig 2: Non Blind IP Spoofing

Blind Spoofing

This attack is complicated and difficult in comparison to the Non-Blind attack because the sequence and acknowledgement numbers cannot be sniffed. In order to get the correct sequence number and acknowledgement, the attacker will send several packets to the target machine, guessing sequence and acknowledgement numbers in order to sample sequence numbers. Nowadays the sequence numbers

are generated randomly to make it unpredictable. After sending several packets there may be a possibility to guess the right sequence number. This attack takes a great deal of time and has a lesser probability of success.

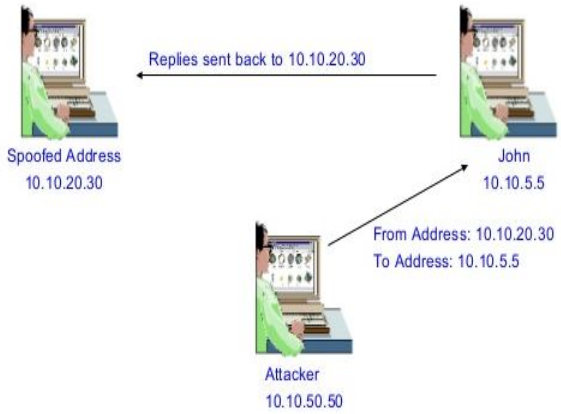

Fig 3: Blind Attack

Man-in-the-Middle Attack

The man-in-the-middle attack (MITM) is a common security violation that is formed by both types of spoofing we have discussed above. In this attack, an attacker intercepts a legitimate communication between two machines (server and client).Then, the attacker controls the flow of data. He can alter the information being exchanged by two machines without the knowledge of either the original sender or the recipient.

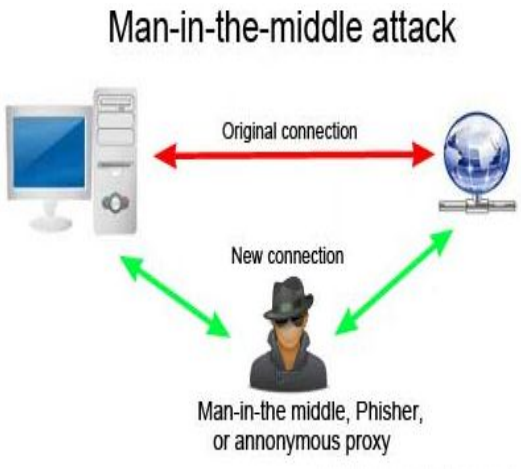

Fig 4: Man-in-the Middle Attack

Denial of Service Attack

Denial of service is the main attack which uses IP spoofing and are the most difficult to defend against. In this attack the attacker only tries to consume the bandwidth and resource of a server. The attacker does not care about the response, so they need not worry about properly completing handshakes and transactions. In this attack an attacker only wishes to flood the victim's machine with as many packets as possible in a short amount of time in order to make the victim's machine inaccessible to valid users. The attacker uses random-source IP addresses to send packets to the target machine to make tracing and stopping the DoS as difficult as possible.

Fig 5: Denial of Service (DoS) Attack

III.DEFENSES AGAINST IP SPOOFING

There are a few precautions that can be taken to prevent IP Spoofing attacks on the network:

A. Filtering packets at the Router

Implementing ingress and egress filtering on your routers is the best defense against the IP spoofing attack. Ingress filtering is the process of blocking packets from outside the network with a source address inside the network. Egress filtering is the blocking of packets from inside the network with a source address that is not inside. You will also need to implement an ACL (access control list) that blocks private IP addresses on your downstream interface. On the upstream interface you should restrict source addresses outside of your valid range, which will prevent someone on your network from sending spoofed traffic to the Internet.

B. Encryption and Authentication

Implementing encryption and authentication will also reduce spoofing threats. Both of these features are included in IPv6, which will eliminate current spoofing threats. Host IP based authentication must not be used based on the IP address. It is recommended to design network protocols and services so that they do not rely on the IP source address for authentication.

IV.CONCLUSION

IP spoofing is really easy because there are many tools available which allow users to edit packets and send packets from the IP. So performing IP spoofing is really simple, which leads to some big hacking operations. Although many servers have secure mechanisms to prevent spoofed packets, all those mechanisms are limited. Most of the networks still does not consider this attack. So their authentication based on IP address fails. Server administrators and network administrators must consider this attack while designing the security rules for their servers and networks. By considering some points, it's easy to identify the forged packet with fake IP addresses .With the above proper defensive measures, it can be traced and avoided.

REFERENCES

[1] P. Ramesh Babu, D.Lalitha Bhaskari, CH.Satyanarayana,"A Comprehensive Analysis of Spoofing" (IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 1, No.6, December 2010.

[2] Vimal Upadhyay. Rajeev kumar." DETECTING AND PREVENTING IP SPOOFED ATTACK BY HASHED ENCRYPTION" International Journal of Enterprise Computing and Business Systems ISSN (Online) : 2230-8849 http://www.ijecbs.com Vol. 1 Issue 2 July 2011.

[3] Haining Wang, Member, IEEE, Cheng Jin, and Kang G. Shin, Fellow, IEEE, "Defense Against Spoofed IP Traffic Using Hop-Count Filtering", IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 15, NO. 1, FEBRUARY 2007.

[4] N. Arumugam, C. Venkatesh ,"A Trivial Scheme for Detecting and Preventing Fake IP Access of Network Server Using IPHP Filter", European Journal of Scientific Research, ISSN 1450-216X Vol.53 No.2 (2011), pp.258-268.

[5] Yao Chen, Shantanu Das, Pulak Dhar, Abdulmotaleb El Saddik, and Amiya Nayak, "Detecting and Preventing IP-spoofed Distributed DoS Attacks," International Journal of Network Security, Vol.7, No.1, PP.70–81, July 2008.

[6] Tanase, Matthew "IP Spoofing: An Introduction".(March 11, 2003). Symantec. Retrieved September 25, 2015.

[7] J. Bellardo and S. Savage, 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions, Proc.USENIX Security Symp., pp. 15-28, 2003.

[8] Wagner, R. (2001) Address Resolution Protocol Spoofing and Man in the Middle Attacks. SANS Institute .Error! Hyperlink reference not valid..

[9] A. Perrig, D.Song, and A.Yaar, StackPi: A New Defense Mechanism against IP Spoofing and DDoS Attacks, Technical Report CMU-CS-02-208, CMU Technical Report, February 2003.

[10] International Journal of Network Security, Vol. 7, No. 1, PP. 70–81, July 2008 (Received Aug. 9, 2006; revised and accepted Nov. 8, 2006) Yao Chen1, Shantanu Das1, Pulak Dhar2, Abdulmotaleb El Saddik1, and Amiya Nayak1.

[11] StackPi: New Packet Marking and Filtering Mechanisms for DDoS and IP Spoofing Defense Abraham Yaar Adrian Perrig Dawn SongCarnegie Mellon University{ayaar, perrig, dawnsong}@cmu.edu 2006.

[12] "IP Address Spoofing and Hijacked Session Attacks";1/23/95 http://ciac.llnl.gov/ciac/bulletins/f-08.shtm