IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 3, March 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 11, Issue 3, March 2022 ||

| DOI:10.15680/IJIRSET.2022.1102067 |

Different Methods of IP Spoofing Attacks, Packet Detection and Prevention

Mr. Rushikesh Ratan Palve [1], Prof. Pingle Suvarna Digambarrao [2]

PG Student, Dept. of Computer Science and Engineering, PES College of Engineering Aurangabad (MS), India[1]

Associate Professor, Dept. of Computer Science and Engineering, PES College of Engineering Aurangabad (MS), India [2]

ABSTRACT: The phrase IP address spoofing or IP spoofing in computer networking refers to the fabrication of Internet Protocol (IP) packets with a forged source IP address, also known as spoofing, with the goal of concealing the sender's identity or impersonating another computing system. Attackers can avoid exposing their real locations, boost the effect of their attacks, or conduct reflection-based attacks by using addresses that are assigned to others or not assigned at all. This paper discusses various ways for detecting and preventing IP spoofing attacks.

KEYWORDS: Internet Protocol (IP), Packets, attackers, IP spoofing, Computer Networking.

I. INTRODUCTION

IP SPOOFING, or attackers initiating attacks using falsified source IP addresses, has long been recognized as a critical Internet security issue. Attackers can avoid exposing their real locations, boost the effect of their attacks, or conduct reflection-based attacks by using addresses that are assigned to others or not assigned at all. IP spoofing is used in a number of well-known attacks, including SYN flooding, SMURF, DNS amplification, and so on. A DNS amplification attack has been detected, which has seriously harmed the service of a Top Level Domain (TLD) name server. Despite widespread belief that DoS assaults are launched via botnets and that spoofing is no longer important, the ARBOR research presented at the NANOG 50th meeting reveals that spoofing is still important in observed DoS attacks. Spoofing activities are still common, according to backscatter messages intercepted by the UCSD Network Telescopes [1].

Capturing the sources of IP spoofing traffic on the Internet, on the other hand, is difficult. The study of tracing the source of spoofing traffic is classified as IP traceback. There are at least two major obstacles to constructing an IP traceback system on the Internet. The first is the cost of implementing a routing system with a traceback capability. Existing traceback solutions, especially in high-performance networks, are either not generally supported by current commodity routers (packet marking) [2] or will impose significant overhead to the routers (Internet Control Message Protocol (ICMP) generation [3], packet logging [4]).

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 11, Issue 3, March 2022 ||

| DOI:10.15680/IJIRSET.2022.1102067 |

II. SPOOFING ATTACKS

Figure 1 shows few variations on the types of attacks that successfully employ IP spoofing.

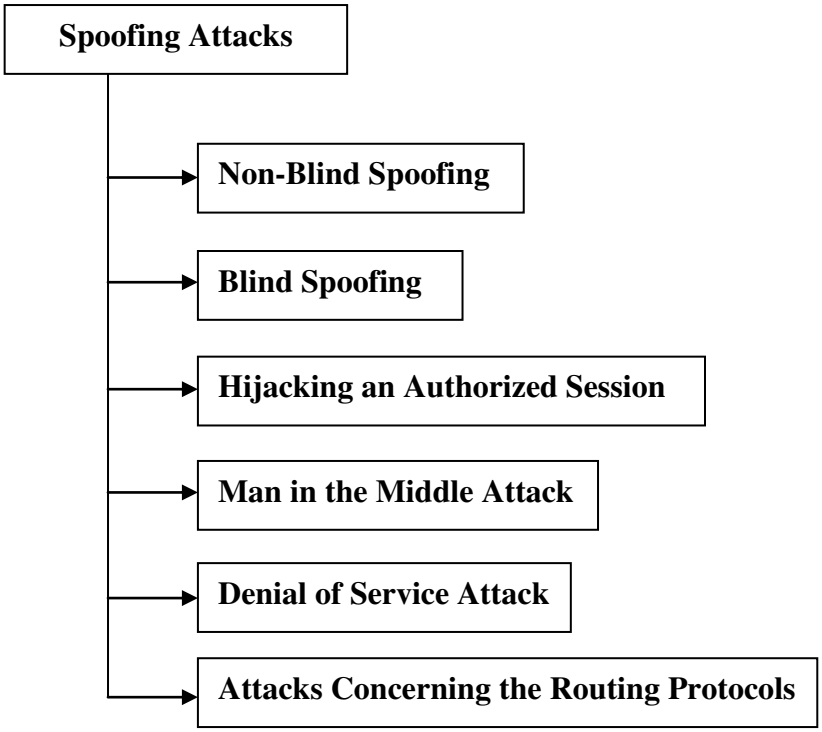

Figure 1 Variationstypes of attacks

- **Non-Blind Spoofing**

When the attacker and the victim are on the same subnet, this form of attack is possible. It is possible to calculate the sequence and acknowledgement numbers, which eliminates the potential difficulties of doing so accurately.

- **Blind Spoofing**

This attack could come from the outside if the sequence and acknowledgement numbers aren't accessible. In order to sample sequence numbers, attackers frequently send numerous packets to the target machine, which was possible in the past.

- **Hijacking an Authorized Session**

An attacker with the ability to produce accurate sequence numbers can send a reset message to one of the parties in a session, indicating that the session has ended. After putting one of the parties offline, the attacker can connect to the party that is still online and perform a malicious act on it using the IP address of that party.

- **Man in the Middle Attack**

Both types of spoofing are examples of the man in the middle (MITM) attack, which is a common security breach. A malicious party intercepts a valid communication between two friendly parties in these attacks.

- **Denial of Service Attack**

In a TCP system, the connection setup phase consists of a three-way handshake. Special bit combinations in the "flags" fields are used to perform this handshake. If host A wants to connect to host B through TCP, it sends a packet with the SYN flag set. Host B responds with a message with the TCP header flags SYN and ACK set. The initial handshake is completed when Host A sends back a packet with the ACK flag set.

- **Attacks Concerning the Routing Protocols**

To "inject" routes into a host, a host can send faked RIP packets. This is simple to set up; all that is required is IP/UDP spoofing. Passwords are required for upgrading routes on a LAN with RIPv2, although plaintext passwords are utilised.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 11, Issue 3, March 2022 ||

| DOI:10.15680/IJIRSET.2022.1102067 |

III. PACKET DETECTION

The IP address of the sender host is included in packets sent using the IP protocol [5]. This source address is used by the recipient to send replies to the sender. The protocol, however, does not verify the accuracy of this address. The IP protocol does not include a way for verifying the source of a packet. This means that an attacker can change the source address to whatever he wants. This is a well-known issue that has been extensively discussed [6][7][8]. Active host-based methods, passive host-based methods, and administrative methods are the types of detection methods that require router support.

a. Routing Methods

Routers (or IP level switches) can identify packets that should not have been received by a certain interface since they know which IP addresses originate with which network interface. A border router or gateway, for example, will know whether addresses are internal or external to the network. The packet source is most likely faked if the router gets IP packets with external IP addresses on an internal interface or IP packets with an internal IP address on an external interface. ISPs and other network operators have been asked to filter packets using the above-described manner in the aftermath of recent denial-of-service assaults utilising faked attack packets. Ingress filtering defends the company from outside threats by filtering inbound packets.

b. Non-routing methods

A number of active and passive methods exist for computers receiving a packet to identify if it has been faked. The term "active" refers to the host's requirement to do some network activity in order to confirm that the packet was sent from the claimed source. Active methods can be used to validate circumstances when the passive approach suggests the packet was faked.

IV. IP SPOOFING PREVENTION METHODS

a. Lossy Compression

Lossy compression, in computer language, is a data encryption method that removes some data in order to achieve its aim, with the effect that decompressing the data returns content that is different from the original, but similar enough to be useful in certain ways. Multimedia data, audio, video, images, and other types of data are routinely compressed using lossy compression. Text and data files, such as bank records, text articles, and so on, require lossless compression. In many circumstances, creating a master lossless file that can then be used to create compressed files for various purposes is helpful.

b. Lossless Compression

Lossless data compression is a type of data compression technology that allows you to retrieve the exact original material from compressed ZIP files. Lossless data compression differs from lossy data compression, which allows only an approximation of the original data to be re-fetched in return for higher compression rates. Many applications use lossless data compression. It's utilised in the popular ZIP file format and the UNIX kernel utility gzip, for example. It's also frequently employed as part of lossy data compression algorithms.

V. CONCLUSION

This paper discusses IP spoofing as a way of gaining illegal access to a network, as well as several IP spoofing detection and mitigation techniques. The attacker's goal is to establish a connection that will allow them to get root access to the host, allowing them to create a backdoor into the target system.

REFERENCES

[1] Guang Yao, Jun Bi and Athanasios V. Vasilakos, “Passive IP Traceback: Disclosing the Locations of IP Spoofersfrom Path Backscatter”, IEEE Transactions On Information Forensics And Security, Vol. 10, No. 3, March 2015.
[2] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, “Practical network support for IP traceback,” in Proc. Conf. Appl., Technol., Archit., Protocols Comput. Commun. (SIGCOMM), 2000, pp. 295–306.
[3] S. Bellovin, “ICMP Traceback Messages”, http://tools.ietf.org/html/draft-ietf-itrace-04, accessed Feb. 2003.
[4] A. C. Snoeren et al., “Hash-based IP traceback,” SIGCOMM Comput. Commun. Rev., vol. 31, no. 4, pp. 3–14, Aug. 2001.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 11, Issue 3, March 2022 ||

| DOI:10.15680/IJIRSET.2022.1102067 |

[5] Daemon9. IP Spoofing Demystified. Phrack MagazineReview, Vol 7, No. 48, June 1996, pp. 48-14.
[6] Computer Incident Advisory Committee (CIAC) (1995).Advisory Notice F-08 Internet Spoofing and HijackedSession Attacks.
[7] Donkers, A. (1998, July). Are you really Who You SayYou Are? System Administrator, Vol 7, No. 7, 69-71.
[8] D. Schnackenberg, K. Djahandari., and D. Sterne.Infrastructure for Intrusion Detection and Response.Proc. of the DARPA Information SurvivabilityConference and Exposition (DISCEX '00), 2000.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details