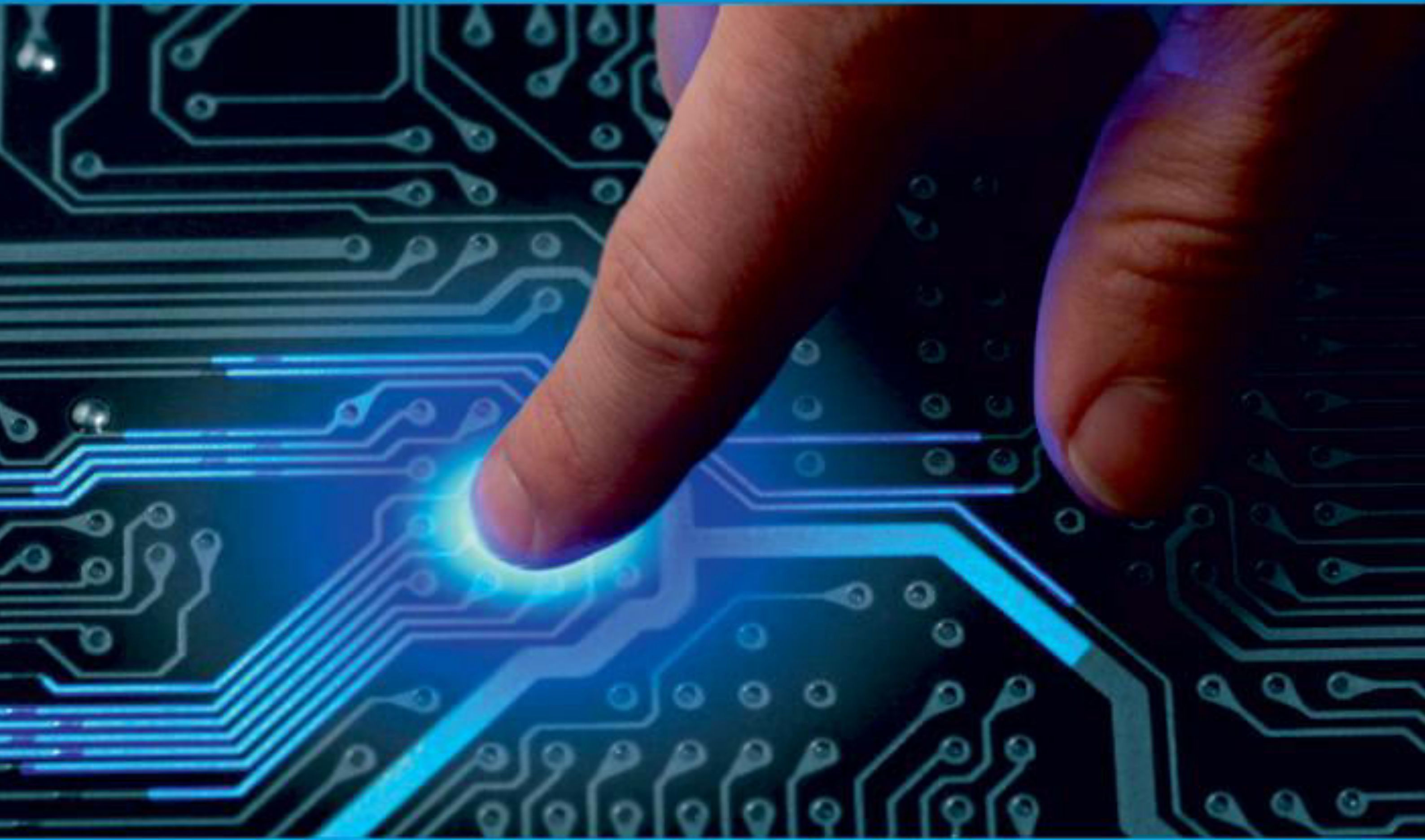
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 9, September 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

☎ 9940 572 462 6381 907 438 ✉ ijircce@gmail.com @ www.ijircce.com

Methods of IP Spoofing and Detection

Vivin Adhitya A M[1], Savita Sheelavant[2]

Student, RV College of Engineering®, Bengaluru, India[1]

Assistant Professor, RV College of Engineering®, Bengaluru, India[2]

ABSTRACT: In computer networking, the term IP address spoofing or IP spoofing refers to the creation of Internet Protocol (IP) packets with a forged source IP address, called spoofing, with the purpose of concealing the identity of the sender or impersonating another computing system. However, not much attention has been paid to the security weaknesses of the TCP/IP protocol by the general public. This study contains an overview of IP address and IP Spoofing various types of IP Spoofing, how they attack on communication systems. This study also describes some methods for detection and prevention methods of IP spoofing and also describes impacts on communication systems by IP Spoofing. This study describes the use of IP spoofing as a method of attacking a network in order to gain unauthorized access and some detection and prevention methods of IP spoofing. The goal of the attack is to establish a connection that will allow the attacker to gain root access to the host, allowing the creation of a backdoor entry path into the target system. Hence the proposed methods will be very helpful to detect and stop IP spoofing and give a secured communication system.

KEYWORDS: IP Spoofing, communication systems

I. INTRODUCTION

The basic protocol for sending data over the Internet network and many other computer networks is the Internet Protocol ("IP"). The header of each IP packet contains, among other things, the numerical source and destination address of the packet. The source address is normally the address that the packet was sent from. By forging the header so it contains a different address, an attacker can make it appear that the packet was sent by a different machine. The machine that receives spoofed packets will send a response back to the forged source address, which means that this technique is mainly used when the attacker does not care about the response or the attacker has some way of guessing the response.

Criminals have long employed the tactic of masking their true identity, from disguises to aliases to caller-id blocking. It should come as no surprise then, that criminals who conduct their nefarious activities on networks and computers should employ such techniques. IP spoofing is one of the most common forms of on-line camouflage. In IP spoofing, an attacker gains unauthorized access to a computer or a network by making it appear that a malicious message has come from a trusted machine by spoofing the IP address of that machine. In certain cases, it might be possible for the attacker to see or redirect the response to his own machine. The most usual case is when the attacker is spoofing an address on the same LAN or WAN. Hence the attackers have unauthorized access over computers. In this paper, we will examine the concepts of IP spoofing: why it is possible, how it works, how it can be detected and how to defend against it.

II. LITERATURE SURVEY

Analyses various techniques employed to verify the actual origin of a packet, this was done in order to identify a spoofed IP address in the event of a Distributed Denial of Service attack. They also proposed passive and active host-based Operating System fingerprinting that authenticates the actual source of an arriving packet by detecting its OS in a Fog Computing platform/environment [1].

This paper describes the use of IP spoofing as a method of attacking a network in order to gain unauthorized access and some detection and prevention methods of IP spoofing. The goal of the attack is to establish a connection that will allow the attacker to gain root access to the host, allowing the creation of a backdoor entry path into the target system. We think that our proposed methods will be very helpful to detect and stop IP spoofing and give a secured communication system. [2].

The Spoofing Attack is dangerous and complex to networks and clouds; an attacker fakes a legitimate user address and launches his attack. Those who control the cloud have a big role to play in preventing and detecting these attacks. This research focuses on enhancing an algorithm called HCF (Hop Count Filtering Algorithm) helps to get rid of the weaknesses of this algorithm. [3].

IP spoofing has often been exploited by Distributed Denial of Service (DDoS) attacks to: 1) conceal flooding sources and dilute localities in flooding traffic, and 2) coax legitimate hosts into becoming reflectors, redirecting and amplifying flooding traffic. Thus, the ability to filter spoofed IP packets near victim servers is essential to their own protection and prevention of becoming involuntary DoS reflectors. Our scheme is based on a firewall that can distinguish the attack packets (containing spoofed source addresses) from the packets sent by legitimate users, and thus filters out most of the attack packets before they reach the victim. They estimate that an implementation of this scheme would require the cooperation of only about 20% of the Internet routers in the marking process. The scheme allows the firewall system to configure itself based on the normal traffic of a Web server, so that the occurrence of an attack can be quickly and precisely detected. By this cryptographic approach, they aim at combining both the existing approaches namely, Victim Based and Router Based approaches against IP spoofing thereby enhancing the speed of detection and prevention of IP spoofing. [4].

This paper is also based on detecting IP spoofing techniques, it explains packet marking, hop by hop tracing, reactive and logging. Packet marking is further in two ways deterministic packet marking (DPM) & Probability packet marking (PPM). Firewalls are also used to prevent the unauthorized user entering the network In packet marking method trace back data is inserted in the packet which has to be traced. In deterministic packet marking, 16 bit of id in the header and 1 bit of flag information are marked on the source router. From this market information we can retrieve the traced information. IN hop by hop approach, if hop by hop program detects any unauthorized packet it sends it to the upstream router and it repeats until it reaches the last spoofed packet. Logging is the most effective method, in this method, the logging information of internet traffic packets throughout the internet is used and then mining operations are performed to detect the spoofed packet. [5].

Distributed Denial of Service (DDoS) attack has been identified as the biggest security threat to service availability in Cloud Computing. It prevents legitimate Cloud Users from accessing the pool of resources provided by Cloud Providers by flooding and consuming network bandwidth to exhaust servers and computing resources. A major attribute of a DDoS attack is spoofing of IP addresses that hides the identity of the attacker. This paper discusses different methods for detecting spoofed IP packets in Cloud Computing and proposes Host-Based Operating System (OS) fingerprinting that uses both passive and active methods to match the Operating System of incoming packet from its database. Additionally, how the proposed technique can be implemented was demonstrated in the Cloud Computing environment.[6].

Heavily used intra-domain protocols (like IP, ARP) do not have protection mechanisms against malicious activities by network clients. As a result IP and ARP spoofing are used by attackers to launch Man In The Middle (MITM), Denial of Service (DoS) and other attacks. These attacks are severe threats to the organizations. Detecting and preventing IP-ARP spoofing will enhance the security to great extent. This paper presents a simple and light-weight mechanism for detection and prevention of IP-ARP spoofing attacks. Experimental results are also provided to support the proposal. [7].

Based on the outcome of the Literature survey, Network security firewalls are level to IP spoofing attacks on organizational data and individual user data. The IP spoofing attack is still a challenging problem. Robust solutions are required to secure the data from IP spoofing attacks. Using routers enables us to determine every IP address' origin point on the network. Additionally, they also help us find out about the network interface from which the IP address is hailing. As a result, they help avoid all those packets not meant to be received by a particular interface. At the outset, there exist a host of ways, both passive and active, using which one can determine whether the packet received is spoofed in nature or not. Network monitoring tools, such as Net log, can be used to scan the packets' external interfaces in question. They also help detect IP spoofing by facilitating the comparisons of process accounting logs between systems present on the internal network.

III. DESCRIPTION

Every packet comprises an IP address header that possesses data about the IP address of the sender and the receiver and other relevant information about the packet under consideration. Usually, an IP spoofing attack occurs when the IP address of the source is altered to impersonate the IP address of another trusted or legitimate source. For instance, this source could be a computer or system that is part of a legitimate and credible network. Since the source appears to be authentic, the data ends up getting accepted. The cyber attacker can then use a variety of IP spoofing tools to change the IP address header. Once the address has been externally tampered with, there is no way for the receiver to identify and gauge it. It is primarily because IP spoofing in network security predominantly takes place at the network level. In computer networking, the term IP address spoofing or IP spoofing refers to the creation of Internet Protocol (IP) packets with a forged source IP address, called spoofing, with the purpose of concealing the identity of the sender or impersonating another computing system.

In a spoofing attack, the intruder sends messages 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 so that it appears that the packets are coming from the trusted system. In essence, the attacker is fooling (spoofing) the distant computer into believing that they are a legitimate member of the network.The goal of the attack is to establish a connection that will allow the attacker to gain root access to the host, allowing the creation of a backdoor entry path into the target system. 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: This type of attack takes place when the attacker is on the same subnet as the victim. The sequence and acknowledgement numbers can be calculated, eliminating the potential difficulty of calculating them accurately. The biggest threat of spoofing would be session hijacking. This is accomplished by corrupting the DataStream of an established connection, then re-establishing it based on correct sequence and acknowledgement numbers with the attack machine. Using spoofing, the attacker interferes with a connection that sends packets along the subnet.

Blind Spoofing: This attack may take place from outside where sequence and acknowledgement numbers are unreachable. Attackers usually send several packets to the target machine in order to sample sequence numbers, which is doable in older days. Usually, the attacker does not have access to the reply, and abuse trust relationships between hosts. For example: Host C sends an IP datagram with the address of some other host (Host A) as the source address to Host B. Attacked host (B) replies to the legitimate host (A)

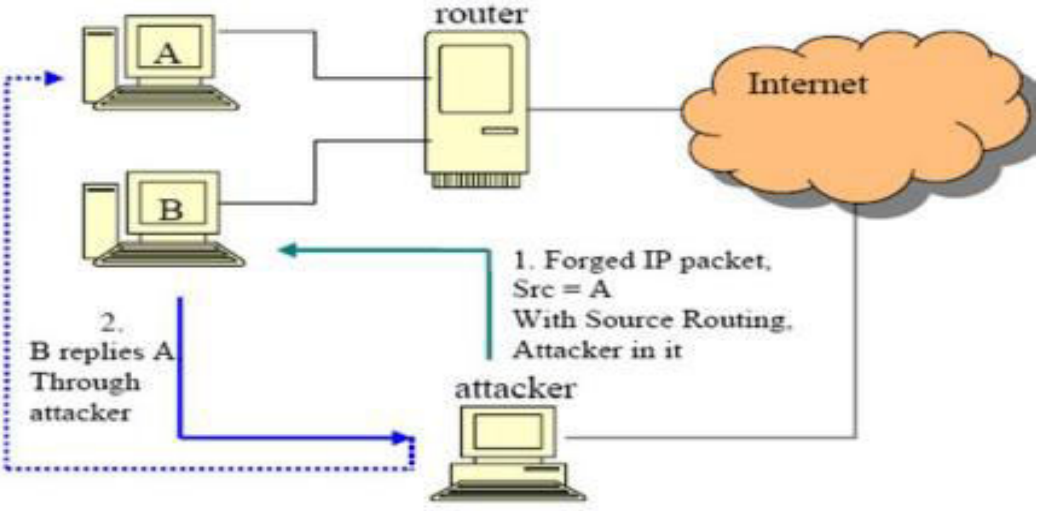


Figure 1.1 Block Diagram of IP Spoofing

Hijacking an Authorized Session: An attacker who can generate correct sequence numbers can send a reset message to one party in a session informing that party that the session has ended. After taking one of the parties' offline, the attacker can use the IP address of that party to connect to the party still online and perform a malicious act on it. The attacker can thus use a trusted communication link to exploit any system vulnerability. Keep in mind that the party that is still online will send the replies back to the legitimate host, which can send a reset to it indicating the invalid session, but by that time the attacker might have already performed the intended actions. Such actions can range from sniffing a packet to presenting a shell from the online host to the attacker's machine.

Man in the Middle Attack: Both types of spoofing are forms of a common security violation known as a man in the middle (MITM) attack. In these attacks, a malicious party intercepts a legitimate communication between two friendly parties. The malicious host then controls the flow of communication and can eliminate or alter the information sent by one of the original participants without the knowledge of either the original sender or the recipient. In this way, an attacker can fool a victim into disclosing confidential information by “spoofing” the identity of the original sender, who is presumably trusted by the recipient.

Denial of Service Attack: The connection setup phase in a TCP system consists of a three-way handshake. This handshake is done by using special bit combinations in the "flags" fields. If host A wants to establish a TCP connection with host B, it sends a packet with a SYN flag set. Host B replies with a packet that has SYN and ACK flags set in the TCP header. Host A sends back a packet with an ACK flag set, finishing the initial handshake. Then hosts A and B can communicate with each other.

IV. TECHNICAL SIGNIFICANCE

Having a well-developed security posture is essential to any business. Organizations should not assume the security of their customers' data and instead must take proactive steps to ensure it throughout the development process. Veracode provides powerful cloud-based tools, including static and dynamic security analysis, to detect vulnerabilities and security flaws before attackers can take advantage of them. One common threat to be wary of is spoofing, where an attacker fakes an IP address or other identifier to gain access to sensitive data and otherwise secure systems.

The following are some commonly used IP spoofing tools

Netcommander: This is the most user-friendly ARP tool for IP spoofing.

Sylkie: This tool makes use of the neighbor discovery protocol to spoof IPv6 addresses.

Aranea: Aranea is a clean and fast spoofing tool that cyber attackers often use to stage spoofing attacks on a network.

Isr Tunnel: Isr Tunnel makes use of source-routed packets to spoof connections.

StopCut, Find Mac Address pro, SecurityGateway for Exchange / SMTP, PacketCreator, Responder Pro are some commonly used IP spoofing prevention tools along with some techniques like

- Avoiding usage of the source address authentication by implementing cryptographic authentication system-wide.

- Configuring the network to reject packets from the Net that claim to originate from a local address.

- Implement egress and ingress filtering. This will monitor all incoming and outgoing information and will block any unauthorized traffic.

- Use encryption when sending any private information over the Internet. This will change any information you share into a code that hackers will not be able to understand.

- Use an ACL (access control list) to block any unauthorized or private IP addresses.

• Configure the router to reject unauthorized users that are claiming to be in your local network, when they are actually coming from outside your network. 9. Add an authenticated password-based key exchange to prevent IP spoofing. Two more users on the same network can use this key to access information. Without this, access is denied.

V. APPLICATIONS

IP address spoofing involving the use of a trusted IP address can be used by network intruders to overcome network security measures, such as authentication based on IP addresses. This type of attack is most effective where trust relationships exist between machines. In performance testing of websites, hundreds or even thousands of virtual users may be created, each executing a test script against the website under test, in order to simulate what will happen when the system goes "live" and a large number of users log in simultaneously. Since each user will normally have its own IP address, commercial testing products (such as HP LoadRunner, WebLOAD, and others) can use IP spoofing, allowing each user its own "return address" as well.

VI. CONCLUSION

The real-time risks of IP spoofing are rather grave and tend to have irreversible consequences in most situations. However, it is not a menace that can't be dealt with effectively. Adequate encryption, authentication, and cyber security measures must exist in place to prevent this exploitation of a trust-based relationship between two systems on a network. The most commonly adopted practices for preventing and controlling spoofing attacks like making use of an authentication system based upon the trading of keys such as Ipsec, blocking private IP addresses by using ACL on downstream interfaces, subjecting both inbound and outbound traffic to filtering, migrating the web application to IPv6 subsequently helps prevent spoofing through its implementation of authentication and encryption steps should be implemented in order to prevent such attacks from taking place

REFERENCES

[1] A. E. Agoni and M. Dlodlo, "IP Spoofing Detection for Preventing DDoS Attack in Fog Computing," 2018 Global Wireless Summit (GWS), Chiang Rai, Thailand, 2018, pp. 43-46, doi: 10.1109/GWS.2018.8686626.

[2] "Proposed Methods of IP Spoofing Detection & Prevention", Sharmin Rashid, Subhra Prosun Paul, International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064 2013

[3] Basim, Huda & Khaleel, Turkan. (2018). "An Improved Strategy for Detection and Prevention IP Spoofing Attack", International Journal of Computer Applications. 182. 975-8887. 10.5120/ijca2018917667.

[4]Ravi M., Narasimman S., Kumar G.K.A., Karthikeyan D. (2010) "A Cryptographic Approach to Defend against IP Spoofing.", Das V.V. et al. (eds) Information Processing and Management. BAIP 2010. Communications in Computer and Information Science, vol 70. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978- 3-642-12214-9_47

[5] Lavanya, Maderi & Sahoo, Prasanta & Scholar, P. (2016). "IP spoofing and its Detection Technique". International Journal of Scientific and Research Publications, Volume 7, Issue 11, November 2017 ISSN 2250-3153

[6] Opeyemi.A. Osanaiye, Mqhele Dlodlo, "IP Spoofing Detection for Preventing DDoS Attacks in Cloud Computing", EUROCON 2015 - International Conference on Computer as a Tool (EUROCON) IEEE, pp. 1-6, 2015

[7] S. G. Bhirud and V. Katkar, "Light weight approach for IP-ARP spoofing detection and prevention," 2011 Second Asian Himalayas International Conference on Internet (AH-ICI), Kathmundu, Nepal, 2011, pp. 1-5, doi: 10.1109/AHICI.2011.6113951.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 7.542

doi crossref

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

📱 9940 572 462 ✆ 6381 907 438 ✉ ijircce@gmail.com

Scan to save the contact details

www.ijircce.com