IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

IP SPOOFING

Sagar Prajapati, Priyanka Rana, Kaushal Gor
MCA Student, MCA Student, Professor
MCA Department, Parul University of Engineering and Technology, Vadodara, India.

Abstract- 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. IP Spoofing is attack that takes place in Network. It is used to gain unauthorized access to computer by spoofing the IP Address from the IP (Internet Protocol) Packet Header. The study will also help to get knowledge of IP & Spoofing using it. As the attack can be harmful to any one, so the concepts of preventing from IP Spoofing attack is explained here. With the direct comparison to the alternative's prevention technique, we can deeply understand how prevention can be done.

Keywords –IP Spoofing, IPv4, IPv6, IP Attacks

1. INTRODUCTION

Growing Internet and services are also leading in cyber-attacks, IP Spoofing is attack which takes place in network. the main purpose of IP Spoofing attack is to hide the true identity of the attacker.[2] The Internet Protocol(IP) is the main protocol used to route information across the Internet. the role of IP is to provide best service for the delivery of information to its destination. [1] IP Spoofing forge the IP Address from the IP header and the packet with the forged IP address is send to the victim. Router is responsible for routing, whenever packet is arrived at router it checks the destination address and send the packet according to the destination address. source IP address is not checked by the router that whether it is proper or not & it is simply send towards the destination.[2] IP Spoofing is used by the popular attacker such as DoS(denial of service), Hijacking an Authorized Session & Man in Middle attacks.

1.1 INTRODUCTION to IP

The Spoofing is done using IP(Internet Protocol) which is primary need for transmitting data from source to destination. IP acts as the address for the delivery packet.so we need to understand first what are IPs ant its version. The basic protocol for sending data over the Internet network and many other computer networks is the Internet Protocol ("IP"). There are two types of IP address version are used IPv4 & IPv6.

1.2 IPv4

The Internet Protocol Version 4 is the core protocol of standards-based internetworking method in the Internet and other packet switched networks. This was the first version used ARPANET in 1983. IPv4 uses a 32-bit address in which we can store 2^{32} unique host address, in these blocks of address are reserved for special networking purpose. This are most often written in dot-decimal notation, which consists of octets of the address used individually in decimal numbers and separated by dots. IPv4 address are divided into two parts, one the network identifier which is the most significant octet of address and other part is host identifier which is also known as rest filed.

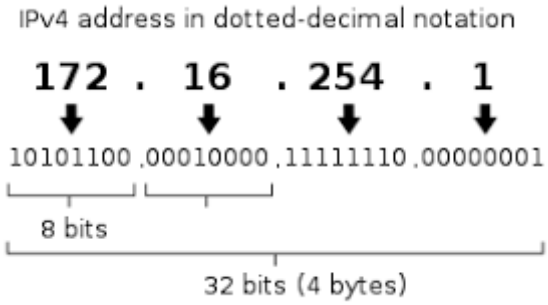

Fig 1: IPv4 Address [14]

1.3 IPv6

Internet Protocol version 6 is the most recent version of Internet Protocols which provides an identification and location system for computers on the networks and routes traffic across the Internet.IPv6 use 128-bit address which can contain 2^{128} unique host address inside it. As the Data is transmitted in form of packet over the internet, so that IPv6 specifies a new packet format which is designed to minimize the packet header processing by the routes. It also supports automatic and renumbering address configuration.

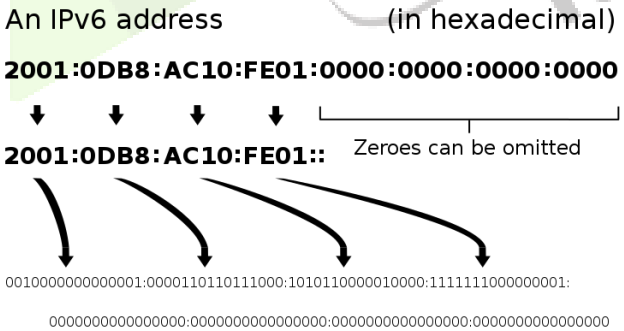

Fig 2: IPv6 Address [15]

This are two only protocols which are used in IP Spoofing in any type of attack.

2. APPLICATION AREA

2.1 PURPOSE OF SPOOFING

If the sender on any network has some malicious intention and he/she does not want to identified. Most of the system maintain logs of internet activities, so if attacker want to hide their identity then in that case, they need to change the source address.[1] The host in the network who is receiving the spoofed packets responds to the spoofed address, so at that time the attacker receives no reply back from the victim host, only the victim continues to respond. If the spoofed address belongs to a host on the same subnet as the attacker in that case the attacker can detect & get the reply in some scenario, an attacker might want to inspect the response from the target victim, else in other cases the attackers might not care of getting responds at all. [1]

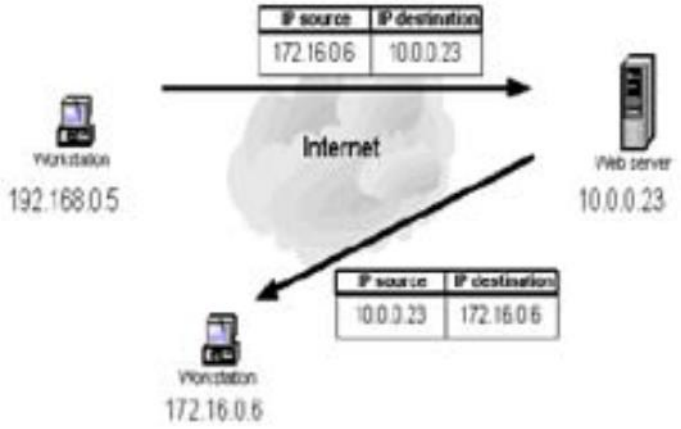

Fig 4: Spoofing [4]

2.2 DENIAL OF SERVICE ATTACK

IP Spoofing is mostly used in one of the most executed attack -Denial of Service Attacks which is very difficult to defend.[4] The connection setup in network consists of a Three-Way handshake, this three-way handshake must be completed in order to establish a connection. As the attack are concerned only of consuming bandwidth & resources, they don't worry about properly completing of handshake and transaction. They moto is to only flood the victim with as many packets as possible in short period of time. As to continuing the effect of the attacks, spoofed IP address from the source is used, which make it more difficult to stop & trace the DOS attack.[4]

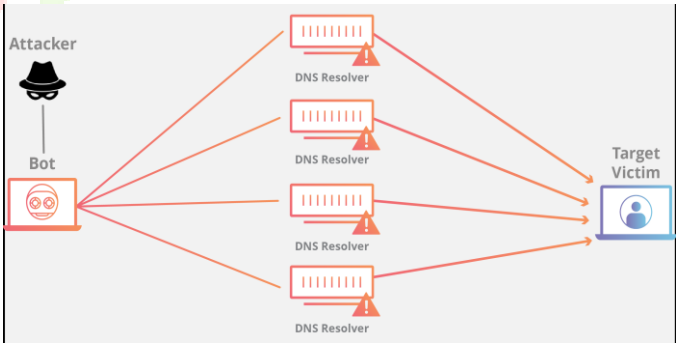

Fig 5: Denial of service attack.[19]

2.3 HIJACKING AN AUTHORIZED SESSION

In a network, if the attacker can generate correct sequence number then he can send a message for reset to one of the parties in a session of the network, informing the party session has ended.[4] After taking one of the parties offline, the attacker can use the IP address of that party to connect to that network in session, which makes it still show online and give a chance to perform malicious act over it. The attacker can thus use a trusted communication link to exploits the system vulnerability. The session hijacking attack compromises the session token by stealing or predicting a valid session token gain unauthorized access to the web server.[12]

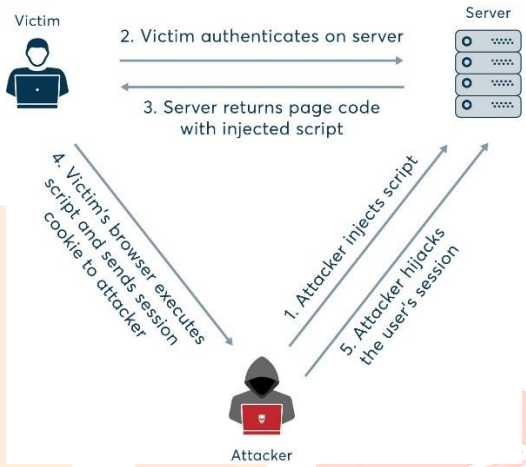

Fig 6: Hijacking an Authorized Session.[20]

2.4 MAN IN MIDDLE ATTACK

In this attack, a malicious party intercept a legitimate communication between two friendly party. The malicious host then controls the flow of communication and can alter the information sent by one of the original participants without the knowledge of either the original sender or the recipients. 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.[4].

Fig 7: Man in Middle Attack.[21]

2.5 BLIND SPOOFING

In this attack, an attacker outside the area of the local network transmits multiple packets to his intended target to get back a series of sequence numbers. Which are used to bring together all the packets in the order in which they were intended.[16] The attacker is blind so don't know that about the way in which transmissions take place on this network, so he needs to induce the machine into responding to his own requests so he can analyze the sequence numbers. By knowing the sequence number, the attacker can hide his identity by injecting data into the stream of packets without having to have authenticated himself when the connection was first established.[16] Current operating systems use random sequence number generation method, so it's more difficult for attacker to predict the correct sequence number.

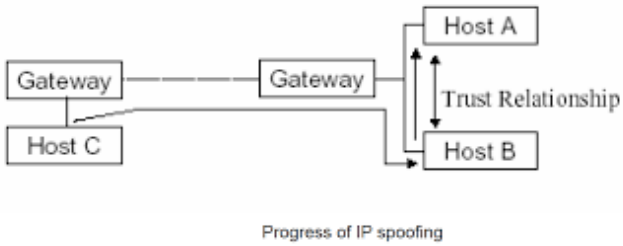

Fig 8: Blind Spoofing. [16]

3. PREVENTION AND DETECTION TECHNIQUES.

3.1 HOP COUNT TECHNIQUE

In any attack, the attacker can spoof the source IP address, the hop along the travelling path(router to router) cannot be spoofed.[6] This technique learn & check the IP to HC(hop count) mapping and stores the mapping in an IP2HC table. As the packet arrives, it is compared to the HC stored for this IP. If the HC values matches, then the packet is legitimate otherwise discarded. After calculating the HC overlap between each IP and every other IP, we calculate the average of the HC overlap based in IPs in the same AS(Automated System) and the same country, IPs in the same country with different AS and IPs in different countries with different AS. IPs in different countries and AS seen very different in terms of HC. There is no average less than 19% chance that two IPs would have the same HC value as seen by a random destination. A random destination IP has a high probability of viewing two IPs in same AS as similar in terms of HC. This HC overlap or similarly decreases as the IPs are chosen in same country.[6] At the end of filtering phase the packet is considered legitimate if HC belong to the HC-list created in the learning phase otherwise it is considered as an Attack. All the traffic in and out of any organization usually travels through periphery routes followed by firewall for inspection. This detection algorithm can be placed in between router & firewall.

3.2 TECHNIQUE FOR ANALYZING MAC ADDRESSES AND SOURCE IP ADDRESSES

In this method, the received data packet on the port are determined with its source MAC address. This source MAC address is compared with MAC-address table entries which are stored previously.[7] A determined source MAC is then checked weather the address is new or not. If the data packets source MAC address is found to be previously stored in the table, then the source IP address and MAC address pair are compared with the IP/MAC address already stored in the table. If the pair for the received data packet is found in the table then the received data packet is passed through the port. Else the data packet with wrong IP/MAC address pair is blocked, which is not stored in the table. As the new MAC address data arrives then the source IP address for the packet is compared with maximum no. of stored IP address. If the maximum number of the source IP addresses are not present on the port, then a learn source IP routine is performed.[7] After learning, a reverse IP check is performed to confirm the source IP address. If the reverse IP check is successful then the table is updated with the new IP/MAC address pair and the packet is passed. Else if it found that the reverse check is not successful then the received data packet is blocked/dropped.

3.3 BGP ANTI-SPOOFING EXTENSION(BASE)

Marking and Filtering approach using BGP(Border Gateway Protocol) update messages, so the marking value inscribed in a packet should exist as the source's entry in each node's filtering table, otherwise the packet is been dropped. The base mechanisms prevent an attacker from predicting the marking value. Since a one-way chain is used to computing marking value, such a cryptographic marking mechanism render a filter's marking values unpredictable by an attacker.[8] Valid marking values are not visible to an attacker, even in the process of marking and filtering by BASE flows toward the victim. A BASE router communicates with other BASE routers by the use of BGP update messages. One BGP update message invokes distributed filter, propagating through all legacy BGP router, reaching all BASE routers. This mechanism works transparently with the legacy BGP speaker by using optional transitive attributes, in which the information stored in transitive attributes is forwarded even through non-BASE routers. In case of BASE, no location can spoof a packet travelling from source to destination. As the valid mark is coming from source, so the attacker in between cannot send spoofed packet using the source's address.[8] Enhanced protection power of BASE comes from the use of packet marking to allow non-adjacent BASE-enabled Ass to verify the validity of the source address of travelling packets.

3.4 AUTHENTICATION BASED PREVENTION TECHNIQUE

This technique works when an attacker is attacking on IPv6 edge network with a forged source address. The host certifies its ownership of a certain IP address via showing the security gateway its secret session key which is shared with the security gateway. The authentication algorithm includes two mechanisms [12]. The source address validation. the anti-reply mechanisms. the host generates a signature by using the hash function(Such as MD5, SHA-1) with the session key and contain some data in it as input. The anti-reply mechanisms combine the sequence number method and the timestamp method.[12] The security gateway checks the signature for validate the source address, since the secret session key itself is not transferred in the plain text form, this makes impossible to attacker to modify or forge another host packet.

3.5 HOST BASED METHOD USING HANDSHAKE

An attacker who sends specified packet is unable to see the replies and in response a receiving host send acknowledgement that must change the TCP window size or try to retransmits and observes that the source responds correctly or not. If the source does not change window size or not retransmits packets, then recipient host may treat the packets as Spoofed.[9] In SYN Cookies, sending host does not allow resources to connect until 3-way TCP handshake is completed. First sending host send SYN+ACK with packets with encoded initial sequence number(cookies) which includes hash of TCP header received from the receiving host SYN packets, a timestamp and client maximum size. A SYN cookie using secure hash by encoding initial sequence number in 3-way TCP handshaking and when it receives the receiving host response the sending host checks the sequence number and creates the necessary state if the receiving host sequence number is cookie value plus one. As such attacker are not able to guess the cookie values.[9]

3.6 ADVANCE BIT SECURITY(ABS) TECHNIQUES

When a new node wants to join the link local network, it generates an IPv6 address as a tentative IP address the target host selects the first 64 bit of IP address. Using Blake2b algorithm hashes the selected bits and inserts them into the ABS field of NS(Neighbor Solicitation) message format.[13] The target host send the NS to the SNMA(solicited-node multicast group) address based on the last 24-bit of the tentative IP address. All existing hosts on the same IPv6 link that have the same SNMA address receive the message. After receiving NS message, the existing hosts first check for the ABS field, if it is not existing then discard the message, otherwise receiver run a query if it matches with its own first 64bit hashes values. If it does not match with received 64-bit hash values, then the host discard the message, otherwise if matches found subsequently it recalls hash values of its own IP from cache and send a NA message as a reply with next 32-bits and last 32-bits. Upon receiving the NA message, the target host first checks for ABS field, if it is not found then discard it, otherwise check for both next 32-bits and last 32-bits that sent from one of existing hosts.[13] If matches not found then it is considered that the generated IP address is unique. Otherwise, the target host will generate another IP address and repeat the whole algorithm from beginning. And if the host is not found a unique IP within three tries then it will stop the whole generating process.

3.7 VIRTUAL ANTI-SPOOFING EDGE(VASE)

VASE uses sampling and no-demand filter configuration to reduce unnecessary overhead in peace. It provides agile IP spoofing filtering capability. A novel filter generation mechanism is designed to identify spoofing packet. To avoid performing validation on each packet, filtering is not always performed on packet, instead of that sampling is perform on routers and the controller which is used to collect sample from router is called VASE server.[11] To identify spoofing from the sampled packets, VASE server generates filtering rules based on flow path computation. If a sample is matched by filtering rule, adaptive rules will be configured on the corresponding interfaces. In a network with certain scale, the number of interfaces managed by VASE server can be enormous. In order to make the solution scalable, a perimeter concept is introduced. The routers chosen to filter spoofing traffic can form one or more perimeters separating the inside routers from the other part of the network. Inside the perimeters, sampling and filtering are only performed at the interfaces where the perimeter connects with the other part of the network and the interface attached by the stub network.[11] The perimeter concept is essential: however large the VASE coverage is, the number of interfaces to manage is only the sum of the amount of stub networks in the perimeter and the number of links intersecting the perimeter. Through setting the VASE server to be accessible only from the management addresses of routers, the VASE server can be prevented from attack from malicious nodes, even with spoofing source IP address.[11]

3.8 PASSIVE IP TRACEBACK TECHNIQUE

IP traceback techniques are designed to disclose the real origin of IP traffic or track the path It is long known attackers may use forged source IP address to conceal their real locations. PIT can use to find the spoofing packet without any deployment requirement, PIT is actually composed by a set of mechanisms. The basic mechanism, which is based on topology and routing information.[22]

- Basic Tracking Mechanism:
  - Whenever a path backscatter message whose source is router and the original destination is captured, the most direct inference is that the packet from attacker to original destination should bypass.
  - If the topology and routes of the network are known, this mechanism can be used to effectively determine the suspect set.
  - an ISP can make this model to locate attacker in its managed network.
  - the one who performs tracing does not know the routing choices of the other networks, which are non-public information.

- Tracking Without Topology & Routing Knowledge:
  - The path backscatter messages whose original hop count is 0 or 1 such messages are generated 1 or 2 hops from the attacker. possibly they are arrived from the gateway of the attacker.
  - The path backscatter messages whose type is 'Redirect. Such messages must be from attacker gateway.[22]
  - The path backscatter messages whose original destination is a private address or unallocated address. Such messages are typically generated by the first DFZ(Default Free Zone) router on the path from the attacker to the original destination.

3.9 STACK PI(STACK PATH IDENTIFIER)

A packet which is traveling through router on the path towards its destination, the router determines and mark a bit in the packet IP identification filed. The deterministic marking guarantee that the packets travelling along the same path will have same marking. Stack Pi allows the victim and routers on the attack path to take a proactive role in defending against DDOS attack by using the Stack Pi mark to filter out attack packets on per packet basis.[10] The victim can build statistics overtime regarding Stack Pi mark to IP address. If an attacker spoofs an IP address, it is likely that the Stack Pi mark in the spoofed packet will not match the Stack Pi mark corresponding to the legitimate IP address in the database, thus enabling the victim to tag packets with possibly spoofed source IP addresses. Stack Pi is not only effective against large scale DDoS attacks, but also effective against other IP spoofing attacks such as TCP hijacking and multicast source spoofing attacks.[10]

4. References

[1]. J. Jacobsen,ole@cisco.com,"the internet protocol journal" vol-10,no.4.
[2]. ISSN No: 2319-5606 Journal of Engineering Computers & Applied Sciences(JECAS) Volume 4, No.1, January 2015.
[3]. College of Computing Science and Technology, TMU Moradabad.
[4]. Sharmin Rashid, Subhra Prosun Paul,World University of Bangladesh, Dhanmondi, Dhaka, Bangladesh.
[5]. Ayman Mukaddam,Imad Elhajj,Ayman Kayssi,Ali Chehab,Electrical and Computer Engineering Department American University of Beirut,Beirut 1107 2020, Lebanon.
[6]. US007979903B2,Philip Kwan,Foundry Networks, LLC, San Jose, CA(US).
[7]. Heejo Lee, Minjin Kwon,Dept. of Computer Science and Engineering Korea University Seoul, South KOREA Geoffrey Hasker, Adrian Perrig,CyLab / CMU Pittsburgh, USA.
[8]. Guang Yao, Jun Bi,Athanasios V. Vasilakos, Senior Member, IEEE,IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 3, MARCH 2015.
[9]. M. Tariq Banday,Reyaz Ahmad,university of kashmir,10.13140/RG.2.1.1142.9848.
[10]. Adrian Perrig,Dawn Song,Abraham Yaar,School of Computer Science Carnegie Mellon University Pittsburgh, PA 15213.
[11]. Guang Yao, Jun Bi, Senior Member, IEEE, and Athanasios V. Vasilakos, Senior Member, IEEE IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 3, MARCH 2015.
[12]. Lizhong Xie, Jun Bi, and Jianpin Wu,Network Research Center, Tsinghua University,Beijing, 100084, China.

[13]. Md. Mustafejur Rahman, Md. Mostafizur Rahman, Saif Ibne Reza, Sumonto Sarker, and Md. Mehedi Islam,EJERS, European Journal of Engineering Research and Science Vol. 4, No. 12, December 2019.

[14]. https://en.wikipedia.org/wiki/File:Ipv4_address.svg.

[15]. https://en.wikipedia.org/wiki/File:Ipv6_address.svg.

[16]. https://www.globallogic.com/wp-content/uploads/2019/12/Why-do-Hackers-IP-Spoof-and-How-to-Prevent-It.pdf

[17]. https://sites.google.com/site/ragavikannan911/home/types-of-attacks/bfbrfh.png?attredirects=0

[18]. https://en.wikipedia.org/wiki/File:IP_spoofing_en.svg

[19]. https://www.cloudflare.com/img/learning/ddos/what-is-a-ddos-attack/ntp-amplification-botnet-ddos-attack.png

[20]. https://dpsvdv74uwwos.cloudfront.net/statics/img/blogposts/illustration-of-session-hijacking-using-xss.png

[21]. https://blog.trendmicro.com/trendlabs-security-intelligence/files/2015/02/MITM-attack-diagram-2.jpg

[22]. www.owasp.org/www-community/attacks/Session_hijacking_attack

[23]. https://www.websense.com/content/support/library/web/v84/wcg_help/configure_ip_spoofing.aspx