WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

IP spoofing attack Detection and Prevention of different network using various techniques

Ms. Unde Suvarna P.[1], Prof. Avhad G.T. [2]

[1] Student, Vishwabharati college of Engineering, Ahmednagar Maharashtra,India
[2] Asst.Prof., Vishwabharati college of Engineering, Ahmednagar Maharashtra,India

ABSTRACT :

The main goal of writing this paper is to enable students about IP Spoofing; It is an attack that takes place in the network, the main purpose of an IP Spoofing attack is to hide the true identity of the attacker. Internet Protocol (IP) is the main protocol used to route information over the Internet. The role of IP is to provide the best service to deliver information to its destination. IP Spoofing spoofs the IP address from the IP header and a packet with the fake IP address is sent to the victim. The router is responsible for routing whenever a packet arrives at the router, it checks the destination address and forwards the packet according to the destination address. the source IP address is not checked by the router to see if it is correct or not and is simply sent to the destination. IP Spoofing is used by popular attacker like DoS (denial of service), Hijacking an Authorized Session & Man in Middle attacks.

Keywords – IP Spoofing, Filtering, Attacks, Information, Trust, IPv4, IPv6

INTRODUCTION :

IP spoofing is when a hacker changes the original IP address to hide the real source IP address. It can be used to attack: Individual, users, servers. Spoofing is done using Internet Protocol (IP), which is the primary need to transfer data from source to destination. The IP acts as the address for the delivery packet. So first we need to understand what IP addresses are and their versions. The basic protocol for sending data over the Internet and many other computer networks is the Internet Protocol ("IP"). Two types of IP address versions are used IPv4 and IPv6.

How does IP spoofing work?

IP spoofing can be done in many ways, most of which are quite simple. One way to do this is with a software program that overrides the TCP/IP settings of the network card (which can often be done with just the click of a button) and routes all connections through an intermediate host[9]. It is also possible to use routing protocols such as HSRP or VRRP to redirect all traffic from one broadcast domain to another without any user interaction – using a technique called IP masquerading. It works by modifying your computer's ARP table with information that causes other computers on the network to send all packets for addresses not in their own ARP caches back over the wire on a different interface than the one they came on. When a packet is received for an address that does not exist in the ARP table, it is sent back to the other interface as if it never happened, and you will continue to send packets to that address until the process fails or stops someone. It can also cause various problems and malfunctions in your network, so be careful when using this technique. IP spoofing is used in man-in-the-middle attacks and from the scenario above, it can be seen that the attacker (Ken) places himself between two communicating individuals (Daniel & Adeola), spoofing each address[5]. Each victim thus sends its network packets to the attacker and not directly to the intended destination. This research paper focuses on man-in-the-middle IP spoofing attacks caused by packet behavior anomalies that occur during packet transmission that could indicate the presence of a man-in-the-middle attack.

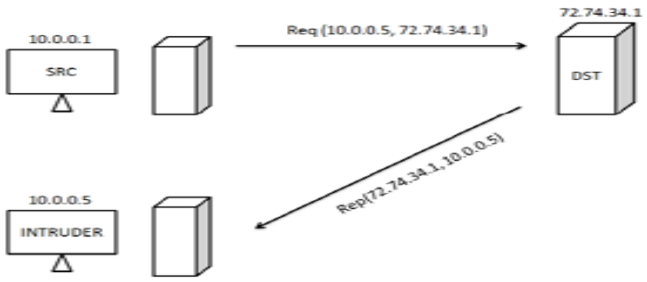

Figure 1. IP spoofing

A deep learning (Multilayer Perceptron Neural Network) process was proposed to classify and identify the IP spoofing MITM attack, which helps to make accurate future predictions based on past occurrences and specified attributes synonymous with the attack type. IP spoofing can be achieved by compromising end systems, i.e. source and target systems[7]. The intruder captures the IP of the source computer and assigns its IP to the packets sent to the destination machine so that the target machine believes that the intruder is the legitimate source machine that sent the request. The intruder's main goal is to create a duplicate connection between itself and the target. Normally when there is communication between two machines, say SRC machine and DST machine, where SRC is the source machine and DST is the destination machine.

Detection of IP Spoofing Attack

IP address spoofing or IP spoofing is the creation of Internet Protocol (IP) packets with a false source IP address to impersonate another computer system. The basic protocol for sending data over the Internet and many other computer networks is the Internet Protocol (IP). The protocol specifies that every IP packet must have a header that contains (among other things) the IP address of the sender package. Software-defined networking (SDN) technology is an approach to network management that enables dynamic, programmatically efficient network configuration to improve network performance. and monitoring, making it more cloud computing than traditional network management.
In existing source IP address spoofing or IP address spoofing attack, refers to attackers releasing packets with spoofed IP source addresses so they can hide their real ones identities and launch attacks such as reflecting network traffic overpower the victims of the hosts. Once you suffer an attack like that, it's hard for the victim to track down the perpetrator and identify them real identity that seriously threatens the internet actually a responsibility. From a technical point of view The threat of IP spoofing is derived from the design of the Internet packet forwarding in routers depends only on packets destination IP address, but neglects validation the source IP address of the packet to verify the authenticity of the sender. By exploiting this vulnerability, attackers can begin in earnest attacks against stated targets and in fact, most attacks are directly related to this SYN floods DDOS. It does not support bandwidth allocation between streams will be static, software-defined The protocol was not implemented, so the IP address was missing consumption occurs.

ARP (Address Resolution Protocol) is used for IP mapping. address to the corresponding MAC address. But it exists the likelihood that a man-in-the-middle attack can occur modifies the information in the ARP cache. Through this paper, an improved ARP is proposed to prevent malicious third party attack. Along with ARP cache as well maintains a table that will store information about everyone living hosts. The concept used here is that if a node, say node A, knows the correct IP/MAC address mapping another node, say node B, then if node A keeps this information if node B is active then man-inthe- medium attack does not occur. So does every node maintain IP address, MAC address, time value for each one living host. IP spoofing is used to gain unauthorized access to a computer. Attacker forwards packets to a computer with a source address that indicates the packet is coming from a trusted port or system. In order to accomplish the task, the attackers have to go through several complex steps. This is a completely blind attack, it takes a lot of experience and knowledge of what to expect from the target's reactions to successfully execute this attack.

IV. Spoofed IP Packet Detection Methods

A new approach to filtering fake IP packets, called Spoofing Prevention Method (SPM). This method allows routers closer to the packet's destination to verify the authenticity of the packet's source address. This is in contrast to standard ingress filtering, which is effective mostly on routers adjacent to the source and ineffective otherwise. In the proposed method, a unique time key is associated each ordered pair of source target networks. Each packet leaving the source network S is labeled with a key K(S;D), associated with (S;D), where D is the destination network. Upon arrival at the destination network, the key is verified and deleted. Thus, the method verifies the authenticity of packets carrying an address that belongs to network S. An efficient implementation of the method to ensure that routers are not overloaded is presented[11]. The main benefits of this method are the strong incentive it provides to network operators to implement it and the fact that the method is suitable for deployment as it benefits the networks that use the method, even if it is only implemented on part of the Internet. These two properties, which are not shared by alternative approaches, make it an attractive and viable solution to the packet spoofing problem [14].

1. Hop Count Technique

In any attack, the attacker can spoof the source IP address. The hop along the path (router to router) cannot be spoofed. This technique learns and checks the IP to HC (hop count) mapping and stores the mapping in the IP2HC table. As the packet arrives, it is compared to the HC stored for that IP. If the HC values match, then the packet is legitimate, otherwise it is dropped. After calculating the HC overlap between each IP and every other IP, we calculate the average HC overlap based on IPs in the same AS (automated system) and the same country, IPs in the same country with different ASs, and IPs in different countries with different ASs. IP addresses in different countries and AS are very different in terms of HC[11]. On average, there is no less than a 19% chance that two IP addresses will have the same HC value as seen by a random target.

2. Host Based Method Using Handshake

An attacker who sends the specified packet cannot see the replies and the receiving host sends an acknowledgment in response, which must resize the TCP window or attempt a retransmission to determine whether the source is responding correctly or not. If the source does not resize the window or retransmit the packets, the receiving host may consider the packets to be spoofed. In SYN Cookies, the sending host will not allow resource

connections until a three-way TCP handshake is complete. The first sending host sends a SYN+ACK with packets with an encoded initial sequence number (cookies) that contains a hash of the TCP header received from the receiving host's SYN packets, a timestamp, and the maximum client size. A SYN cookie using a secure hash by encoding the initial sequence number in a 3-way TCP handshaking, and upon receiving the receiving host's response, the sending host checks the sequence number and creates the necessary state if the receiving host's sequence number is the value of the cookie plus one. As such, the attacker is unable to guess the cookie values.

3. OS Fingerprint

The OS imprint is a modification of the internal packet for OS regulation, which is subsequently based on it. This is commonly marketed through system managers to detect outdated OS's on their network, discover and harden vulnerable OS's, and detect a malicious customer. Additionally, the fingerprint detection OS canister remains sedentary or vigorous. It gains the advantage that different operating system devices are different from the TCP/IP stack and use its unique signature[10].The OS footprint is extremely dependent on whether it is active or inactive. A strong footprint involves distributing a specially crafted probe packet to the exact source, while an indolent one obtains the header topography from the received packets. Utility dynamic fingerprints include SinFP, Xprobe, and Nmap, while inactive fingerprints include p0f (Inactive OS Fingerprint), OSF (iptables-targeted Inactive OS Fingerprint), in addition to Ettercap. we consider p0f and Nmap. Nmap is the predominant electrical network planning tool. It provides a mouth through the distribution of up to fifteen investigations that are completed ICMP, TCP, and UDP, to the sweep and host ports of the local board.

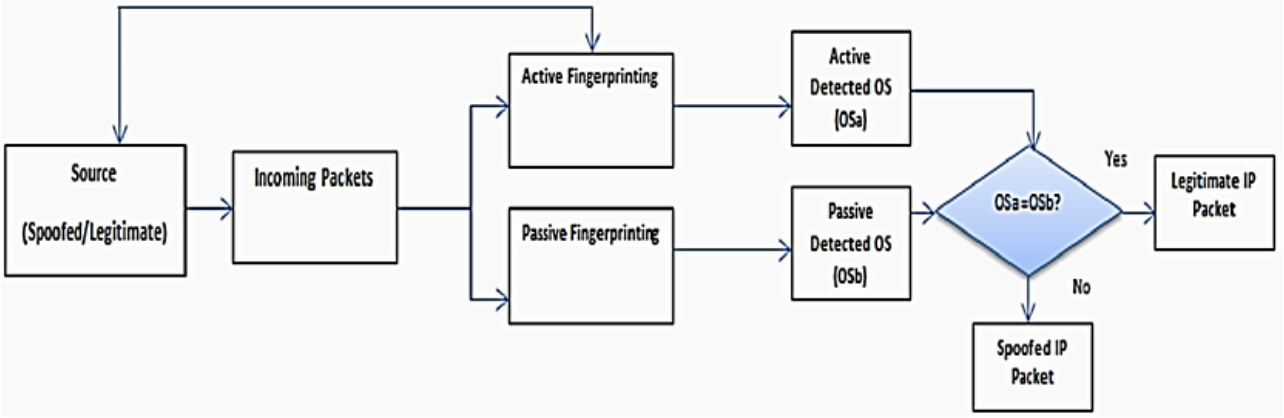

Figure 2. IP Spoofing Detection Block

V. CONCLUSION :

This paper mainly focuses to classify and identify also how to prevent IP Spoofing efficiently and reliably. The proposed system acquires IP traffic for verification and filters the packet that is identified as malicious. The application can be used to spoof any type of malicious packets with the main advantage of consuming fewer resources. It is an integrated tool containing a packet analyzer, active ports and LAN machines. The system is resistant to Distributed Denial of Service (DDoS), Replay and blind spoofing attacks. Upgrade an existing system with a new kit guidelines or methods for packet tracking is our future work. Future works can focus on the use of this machine learning alternative.

REFERENCES :

[1] O. A. Osanaiye, "Short Paper: IP spoofing detection for preventing DDoS attack in Cloud Computing," in 2015 18th International Conference on Intelligence in Next Generation Networks, 2015, pp. 139141:IEEE.

[2] D. Plonka, "FlowScan: A Network Traffic Flow Reporting and Visualization Tool," in LISA, 2000, pp.305-317.

[3] 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.

[4] "Intrusion Detection in 802.11 Networks: Empirical Evaluation of Threats and a Public Dataset," in IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 184-208, Firstquarter 2016, doi: 10.1109/COMST .2015.2402161.

[5] Daemon, Route, Infinity, “IP Spoofing Demystified”, Phrack Magazine;1996[6] A. Bermlerand H. Levy. “Spoofing prevention Method,” INFOCOM’05, 2005.

[7] Rashid S, Paul SP. Proposed Methods of IP Spoofing Detection & Prevention. IJSR. 2013 Aug; 2(8):438–44. ISSN: 2319-7064.

[8] Durai Raj M, Manimaran A. A study on security issues in cloud based e-learning. INDJST. 2015 Apr; 8(8):757–65. e-ISSN: 0974-5645.

[9] Stone R. Center Track: An IP overlay network for tracking DoS floods. Proceedings of USENIX Security Symposium; 2000 Jul. p. 199–212.

[10] Whalen, Sean; “An Introduction to ARP Spoofing”;packetstorm.securify.com/papers/protocols/ intro_to_arp_spoofing.pdf; 6/25/01.

[11] Felten, Balfanz, Dean, Wallach D.S., “Web Spoofing, An Internet Con Game”; http://bau2.uibk.ac.at/matic/spoofing.htm;

[12] Yu F, Lee D. Internet Attack Traceback Cross-validation and Pebble Tracing. Waltham, MA: IEEE; 2008. p. 378–83. ISSN: 978-1-4244.

[13] H. Wang, C. Jin, and K. G. Shin, "Defense against spoofed IP traffic using hop-count filtering," IEEE/ACM Transactions on networking, vol. 15, no. 1, pp. 40-53, 2007 .

[14] 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.

[15] IP address spoofing. Accessed 02.32 PM http://en.wikipedia.org/wiki/IP_address_spoofing.