Applied GIS

ISSN: 1832-5505
Vol-4 Issue-02 April 2016

Methods for Identifying and Preventing IP Spoofing

Authors 1Hitanshu Bagde, 2Satyam Nagpure, 3 Ravi Asati,

1, 2, 3 RGCER, Nagpur, Computer Science and Engineering
[3]

Abstract-- IP spoofing is a method of attack in which the attacker hides his or her true identity by masquerading as a legitimate host on the network in order to gain access to the system and ultimately take over the browser. Man in the Middle attacks, in which a malicious actor intercepts data being sent between two systems and makes unauthorized changes before sending it on, often use this approach. In this article, we will discuss the several methods that have been offered to counter IP spoofing attacks.

Keyword- IP spoofing, MITM attacks, route-based filters, and MAC address restrictions.

INTRODUCTION

Spoofing is the illegal disclosure of an IP address by an individual or organization. In a Man in the Middle attack, the offender tricks the devices into thinking they are interacting directly with one another by forging their data packets. If executed properly, this assault might be totally transparent to users, making it difficult to halt and detect. In technical terms, this attack is the consequence of packet sniffing and spoofing methods. You may have heard of this kind of assault called a "fire brigade," "eavesdropping," or "connection hijacking." This article examines the Man in the Middle assault and the numerous countermeasures used to lessen its severity.

IP SPOOFING

It's a method of attack in which the hacker poses as a legitimate but malicious host in order to gain access to a network and take control of the users' browsers. IP spoofing is also known as forging an IP address or tampering with a host file. By sending network traffic under a faked IP address that makes it seem to originate from a trustworthy host, the attacker gains unauthorized access to the computers. To spoof an IP address, the attacker must first determine the IP address of a trusted host and then alter the packet headers being delivered by the sender such that the receiving system believes the packets are coming from the trusted IP address. The term "IP spoofing" refers to a set of techniques used to impersonate a computer system in order to steal sensitive information. [8]

BLIND SPOOFING

In this type of attack, the perpetrator transfers number of packets to his targeted machine to receive a series of numbers which are used to assemble packets in the order in which they planned to read. After this the perpetrator launches malicious information unknown to the sender.

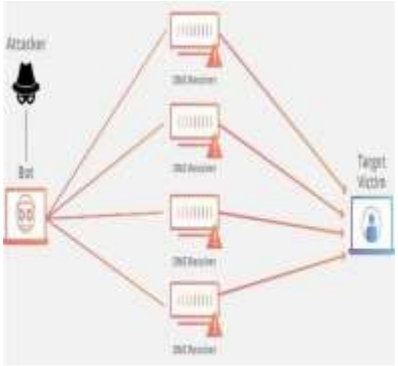


Fig.1: Blind Spoofing [3]

NON-BLIND SPOOFING

In Non –blind spoofing the perpetrator and the targeted machine reside on the same subnet. It is an easier attack than blind spoofing. Here, perpetrator becomes the trusted user of the targeted machine by the process of authentication. [3]

DENIAL OF SERVICES

In this attack, there is a direct hit on the large network administrations, where the server or the main access point is being hacked by the perpetrator and the information from it is spoofed without any prior permission. [3]

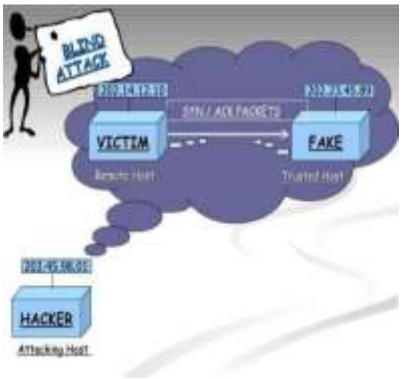
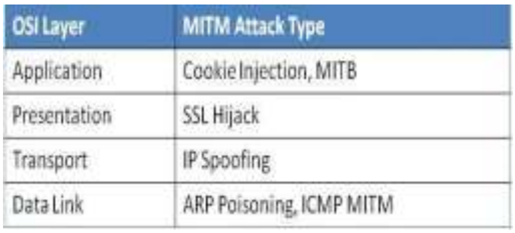


Fig.2: Denial of Service Attack [3]

MAN IN THE MIDDLE ATTACK

It is a type of attack that occurs when an perpetrator enclosure himself as a relay/proxy into a communication session between people or machines. This attack allows perpetrator to steal, transfer and receive data meant for someone else, or not meant to be sent at all, without either outside party knowing until it is too late. The main idea behind this attack is, to intercept packets, and to copy the stolen information for different purposes. [4]

The main objective of the perpetrator is to steal the session from his/her desired system, and hence the information is being transferred over Ethernet. It is known that TCP/IP works on three-way handshake (SYN, SYN-ACK, ACK). It forms a connection between two different network interface cards which then use the packet sequencing and data acknowledgements to transfer or receive data. The data in the ethernet flows from the physical layer all the way up to the application layer. Essential feature of this is that all the layers can participate in man in the middle attacks. [4]



OSI Layer	MITM Attack Type
Application	Cookie Injection, MITB
Presentation	SSL Hijack
Transport	IP Spoofing
Data Link	ARP Poisoning, ICMP MITM

Fig 3: Man in the middle attacks on various OSI layers. [4]

Since this attack can happen at more than one layers, the fatality of attack may become very high. Perpetrators can steal sessions formed at the lower OSI, to discard all the packets flowing. Also, there is an alternate method to capture a complete authentication session and decipher the user id and password information, which can be used by the perpetrator to play the victim and to cause damage at a great extent. Various man in the middle attack happens at several networking layers, which are: ARP poisoning, ICMP man in the middle, DNS man in the middle, DHCP man in the middle, Cookie Hijacking, Man in the browser, SSL man in the middle, and Wireless man in the middle attack. [4]

DEFENSE MECHANISM

In this paper, studied various techniques which have been proposed by different authors for protection against the IP Spoofing based attacks. One of them is Route-based Filtering.

ROUTE-BASED FILTERING

Route-based packet filtering consists of probabilistic packet marking and ICMP message-based trace-back. It shows that by utilizing routing information relevant to the BGP, distributed packet filtering is capable of achieving a synergistic filtering effect which prevents a significant amount of spoofed IP flows from reaching their destinations. Those spoofed IP Flows which can’t be stopped from penetrating are so less, however, such that their area of origin can be localized to within 5 sites carrying out effective IP traceback. Collectively, DPF renders 88% of possible malicious sites impotent, i.e., no spoofed IP flow coming from such sites can reach other target sites which promote DDoS attack prevention. This filtering effect can be reached by doing the filtering function at less than 20% of all Autonomous Systems (AS) on the Internet which makes incresaed deployment a possiblity. Lastly, we show that the distributed filtering effect relies on the power-law connectivity structure of Internet topology. [1]

A route-based filter associates a source address with the previous hop traversed by this source’s packets. RBF is altruistic defense and its authors recommended a vertex cover deployment. [1]

A route-based filter identifies spoofed packets by comparing each packet’s incoming interface against the expected interface relevant with the packet’s source IP in the incoming table that are present in it. Figure 4 explains a scenario where filtering router R has information about 3 sources in its incoming table: sources A and B reach over interface 2 and source C reaches over interface 1. For a while, we keep aside parts of a network which are illustrated in dashed lines. Source A gets compromised and transfers two spoofed packets towards destination D. In the first packet, A spoofs C’s IP address; this packet is identified by R as spoofed as it reaches on interface 2, whereas the expected interface is 1. In the second packet, A spoofs B’s IP address. R can’t identify that this packet is spoofed as its incoming interface is similar to the expected interface for B. This example explains a vital property of RBF: If the route from source S1 to destination D1 overlaps the route from source S2 to destination D2 (possibly D2 6= D1), S1 and S2 can spoof one another and avoid identification by RBF routers placed downstream from the overlap. [2]

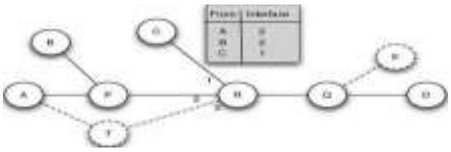


Fig 4: Illustration of Route-based Filtering [2]

Clearly, the location of filtering routers significantly will affect filtering effectiveness. For example, if router Q (from Figure 4) were selected for filter deployment instead of R, all three sources could spoof each other. If, on the other hand, P and R were both filters no spoofing would be possible between A, B and C. [2]

An alternative RBF design maps source IP-destination IP pairs in the incoming table with an expected interface. Park call this a maximal filter whereas RBF with source-only information is referred as a semi-maximal filter. Maximal filter storage carries a cost O(N2), where N is the number of potential sources and destinations, while a semi-maximal filter cost O(N). The effectiveness of maximal filters is only a but higher than that of semi-maximal filters, which is not enough to call for the high storage cost. Still, there may be cases where a semi-maximal filter would erroneously filter out legitimate traffic, when a maximal filter would not do so. Figure 4 explains this case, with dashed items included. Let source A arrive at destination D through P-R-Q and destination E through T-R-Q. This conjures two expected interfaces for A at R. If R is a semi-maximal filter and only collects one expected interface then some legitimate traffic will be filtered out as spoofed. If R is a maximal filter it would appropriately capture that A's packets come trhough interface 2 for destination D and through interface 3 for destination E, so this argument talks in favour of maximal filters. On the other hand, semi-maximal filter scan be extended to appropriately handle the above situation at a much lower storage cost — by allowing multiple expected interfaces. The price that we pay is lower filtering accuracy as multiple expected interfaces conjure more holes for the spoofed traffic to pass through. It is tough to calculate how often is the above routing scenario on the Internet. We limit our discussion to semi-maximal filters with a single expected interface however this design can be extended to support multiple interfaces if needed. [2]

MAC LIMITING

MAC Limiting puts a restriction on the number of MAC addresses that can be dynamically learnt on a single layer to access interface or on all the layer 2 access interfaces on the services gateway. MAC limit is applied to new MAC learning requests. It isn't true for static MAC addresses. Users can configure any number of static MAC addresses not depending upon MAC limiting and all of them are included to be added to forwarding database (FDB). It also improves the security of port by restricting number of MAC addresses which are learnt using VLAN. Flooding happens when the number of new MAC addresses that are learnt causes the Ethernet switching table to overflow, and previously learnt MAC addresses are removed from the table. The switch then comes back to flooding the previously-learnt MAC addresses, which can affect performance and cause security vulnerabilities. MAC limiting is configured on Layer 2 interfaces. The user can specify the maximum number of dynamic MAC addresses which are learnt on a single interface, all interfaces, or a specific interface depending on its membership within a VLAN. [5]

CONCLUSION

In this paper we have discussed about IP Spoofing and Spoofing based attacks. We have also, studied about the man in the middle attack how it is done on different layers. It is found that Route-based filtering limits the spoofing capability of an perpetrator compared to other defense mechanism. They also helped to localize different origins of attack packets. In conclusion, route-based filtering has the capacity to block the IP Spoofing attack.

REFERENCES

[1] Sneha S. Rana, "*A Survey of Defense Mechanisms Against IP Spoofing*", in IJCST, June,2012.

[2] Jelena Mirkovic, Nikola Jevtic and Peter Reiher, "*A Practical IP Spoofing Defense Through Route-Based Filtering*".

[3] Deeksha Vashishth, "*An Analytical Study of Network Security Threats Through IP Spoofing*" in ICAC,2017.

[4] www.valencynetworks.com, "*Cyber-attacks explained man in the middle attack*".

[5] www.junipernetworks.com, "*Understanding MAC Limiting*".

[6] A. Bremler-Barr, H.Levy, "*Spoofing Prevention Method*", In Proc. of INFOCOM, 2005.

[7] Hikmat Farhat, Zouk Mosbeh, "*A scalable method to protect from IP Spoofing*",2008 IEEE.

[8] www.interserver.com "*IP Spoofing and its techniques*".

[9] Hinna Hafeez, Tayyaba Khalil "*IP Spoofing and its Detection Techniques*" in IJSRP, Nov,2017.