International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064

Survey on Various IP Spoofing Detection Techniques

Ann Mary Jacob[1], Saritha S[2]

[1]Rajagiri School of Engineering & Technology, Kochi, India
[2]Rajagiri School of Engineering & Technology, Kochi, India

Abstract: ***Cyber crimes are becoming increasingly sophisticated and have more severe economic impacts. Each attacker goal can be divided into four main classes: Interruption, interception, modification and fabrication. Based on the attacker goals there are mainly two types of attack, active attack and passive attack. Active attacks are those in which attacker can modify information, interruption services and aim to gain unauthorized access to the network systems. During passive attack, the attacker simply monitors the transmission between the two parties and capture information that is send and receive. For this many traditional network devices such as Intrusion Detection System (IDS), firewalls and security scanners are available. However these techniques will not be able to detect the IP spoofing attacks. And also the spoofing attacks are man-in-the-middle attack. Hence there should be some mechanism by which such attacks can be detected. Through this paper we aim to make a comparative study on various mechanisms by which IP spoofing attack can be detected and specify the different available techniques to prevent the IP spoofing attack. First a penetration test method is presented to detect IP spoofing through the design flaws. Second paper, Defense Against Spoofed IP Traffic Using Hop-Count Filtering, says how IP spoofing can be detected using hop count value. The third paper, A protection Method against Unauthorized Access and Address Spoofing for Open Network Access Systems, which proposed a system for IP spoofing detection has been studied. Finally a comparison of these three methods has been made. The forth paper , Enhanced ARP: Preventing ARP Poisoning-Based Man-in-the-Middle Attacks ,defines how to enhance the ARP to detect and prevent man-in-the-middle attack. Through our study we concluded that the system proposed in A protection Method against Unauthorized Access and Address Spoofing for Open Network Access Systems is more efficient and less complex that the other two techniques.***

Keywords: Destination IP address, Hop count filtering, IP spoofing, Man-in-the-middle attack, Penetration test, source IP address

1. Introduction

Computer security has been a serious issue since the starting of internet. As the technology increases the rate of this security issues also increased. There are different ways to ensure security in internet. Most of these techniques are confined to securing the system from a particular type of intrusion. Hence as new systems are developed to protect against a specific attack, intruder comes up with a new intrusion method. Some of the intruder methods include spamming, spoofing, Phishing, cookies. Spamming refers to the junk mails send to the email. Normally spams are not dangerous. Spoofing is pretending to be someone else. Phising is a technique that is used to obtain username or password through an unauthorized way. Cookies are documents which store the history of browsing. Infact cookies serve to be helpful most of the times; however this document can be stolen by an intruder to gain access to unauthorized data. Also these attacks are done by a third party system .Hence all these attacks can be categorized into man-in-the-middle attack.

Through this paper we are trying to study various techniques for detecting IP spoofing attack and make a comparison based on the study. The concept of IP spoofing was first come into picture in the 1980's. In the April 1989 article entitled: Security Problems in the TCP/IP Protocol Suite, author S. M Bellovin of AT & T Bell labs was among the first to identify IP Spoofing as a real risk to computer networks [1]. Word meaning of Spoofing is pretending to be something you are not. Hence in terms of intruder in internet, spoofing refers to using someone else IP address as source address before sending of a packet. When the packet is received at the destination, the receiver believes that the packet was send by a trusted one and hence will respond to the packet. This happens because most of the protocols in internet rely on the source address for authentication. Also spoofing the source IP address is not a tough task. Therefore an intruder can easily cause an IP spoofing attack.

2. Background

Internet Protocol (IP) is used for sending of packets across internet.IP header consists of source IP address filed and destination IP address field. These two fields are mainly used for forwarding of a packet to the correct destination and for authentication. The source IP address in the header field is used for providing authentication and for replying. Spoofing the IP address means to replace the actual source IP address with another IP address, usually a trusted IP address. This packet on reaching the destination, it checks for the source IP address. Since the source IP adress is seen to be a trusted one it accepts the packet, even though it was sent by an untrusted party. In fig 1. It shows the IP header fields along with the source IP address field where spoofing occurs mostly.

<table>
<tr><td>Ver</td><td>1hl</td><td>Type of service</td><td colspan="2">Total length</td></tr>
<tr><td colspan="3">Identification</td><td>Flag</td><td>Fragment Offset</td></tr>
<tr><td>Time-to-live</td><td colspan="2">Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="5">Source IP address(Spoofed)</td></tr>
<tr><td colspan="5">Destination IP address</td></tr>
<tr><td colspan="4">Options</td><td>Padding</td></tr>
</table>

Figure 1: IP header format

An example for the IP spoofing is specified as below. Suppose that an intruder whose IP address is 192.168.30.12 needs to send a packet to a website with IP address 192.168.30.4.If the intruder knows an IP address which is a trusted one to 192.168.30.4,say 192.168.31.2 then 192.168.30.12 before sending the packet will change IP header field in such a way that the source IP address now is 192.168.31.2 instead of 192.168.0.12.This receiver on seeing the source IP address 192.168.31.2,it identifies that the packet is send from a trusted one.

There are various researches going on to detect the IP spoofing attack. Some of the techniques include penetration test, using hop count, using packet filters etc.Here in this paper, and we aim to compare these different techniques used for detecting IP spoofing attack.

3. Aiming at Higher Network Security through Extensive Penetration Tests

Penetration test means a way by which a teste performs all the ways by which an intruder may attack the system and check for vulnerabilities. Hence penetration test is a systematic process of testing a network to determine possible vulnerabilities. Penetration test mainly consists of four stages: planning, discovery, exploitation and reporting. It is during the planning phase that the tester makes a decision on what is to be tested. During the discovery phase the tester gains as much as information as possible about the network. Using the information obtained during the discovery phase the tester exploits the network in the exploitation phase. Finally a report is made. Here during the planning phase tester planned launch a testing mechanism to find out the chance of IP spoofing attack in the network. Here a network in which two subnet works for of victims and other of attackers is considered. To the victim sub network are connected a server pc, admin pc and a victim host. The attacker which resides on the other network will not be able to receive any packets other than those with destination IP address as that of its. Even though it cannot receive any packets which are not addressed to it, it will be able to identify that the host sends SNMP packets to the admin host every 5 minutes. SNMP is a UDP based protocol, all UDP based protocol, all UDP based protocol suffer from source address spoofing attack. So the tester tries to carry out an attack to see if there is a chance for IP spoofing attack. So the attacker at first generates a SNMP packet which has the request to copy the routers configuration on to a TFTP server. For this it will spoof the IP address of SNMP packet with the admin's IP address. The router on seeing the IP address as a trusted IP address it will copy the configuration. The intruder now has the access to the configuration file will make necessary changes and copy it back to the router. Hence by carrying out the penetration test during the exploitation phase it was found that IP spoofing is possible since the network uses UDP based protocol. Now the network security policy needs to be reevaluated to ensure security against the spoofing attack.

4. Defense against Spoofed IP Traffic Using Hop-Count Filtering

Another technique for detecting the IP spoofed packets is by using hop count value. Hop count value denotes the number of hops the packet visit before reaching the destination. The hop count value is determined using the routing infrastructure and hence cannot be spoofed. This feature can be used to identify if the packet has been spoofed. The hop count value cannot be obtained directly from the IP header. Rather this value is stored indirectly in the TTL (Time to live) field. Hence using the hop count an algorithm is proposed in this paper [3].According to this paper.

For each packet that arrives;

Extract the final TTL and infer the initial TTL value from it. Subtract the initial value from the final value and make a comparison with the stored hop-count value (IP2HC mapping table).IP2HC mapping table is a table maintained for storing the hop count value along with the IP address. Normally inorder to reduce the complexity it maintains a hash table for this. If it does not match, it can be concluded that IP spoofing have done and hence the packet need to be rejected. According to modern OSes mainly; Windows, Linux and various other ubuntu based OSes, the initial TTL value can be 30, 32, 60, 64, 128, 255[4].Thus from the final TTL value one can easily identify the initial TTL value except a bit confusion on the values 30 or 32 and 60 or 64.ie The initial TTL value will be a number greater than the final value. As for example if the final TTL value is 100 it can be easily identified that the initial value is 128.For those with confusion that is 30 or 32 and 60 or 64, both the cases will be considered. By clustering address prefixes based on hop-counts, one can build accurate IP2HC mapping tables and maximize the effectiveness of HCF without storing the hop-count for each IP address. Based on the BGP routing table information, a network-aware clustering technique [5] is there to identify the hop count for various IP addresses. Hence using this technique each of the packets that reaches the destination is monitored and compare the hop count value with the stored hop count. It any mismatch occurs it simply discards the packet.

5. A Protection Method Against Unauthorized Access and Address Spoofing for Open Network Access Systems

Through this paper, a system is proposed to provide access control facility. This system consists of a server for user authentication, an IP address assigning server, a frame filter and a set of LAN switches. The LAN switches have ports to which the user PCs is connected. The user PCs can connect to the network only through the ports of switch. The system is configured in such a manner that whenever a PC gets connected to the network through the switch, it has only access to the IP address assigning server. Hence when a PC get connected to the switch, the IP address assigning server assigns IP address for the PC. Then the PC is allowed to connect to the authentication server which authenticates the host. Once the authentication is over the filter copies all the information regarding the host to it and then it allows the PC

to get connected to outside network. Thus whenever a packet comes in, the filter checks the details before forwarding it to the destination. Thus the filter checks for source MAC address, destination MAC address, source IP address and destination IP address. These cross checking ensures that it will detect any spoofing that might have done. If it finds a spoofing have happened it will simply discard the packet.

6. Enhanced Arp: Preventing Arp Poisoning-Based Man-In-The-Middle Attacks

Address Resolution Protocol (ARP) are used to map the IP address to the corresponding MAC address. But there is a chance that a man-in-the-middle attack can occur which modifies the information in the ARP cache. Through this paper, an enhanced ARP is proposed to prevent the malious attack by a third party. Along with the ARP cache it also maintains a table which will store the information about all the alive hosts. The concept used here is that if a node, say node A, knows the correct IP/MAC address mapping of another node, say node B, then if node A retains this information as long as the node B is active, then the man-in-the-middle attack will not occur. Thus each node will maintain IP address, MAC address, a time value for each alive host. This time value denotes the time for which the information is to be retained. Normally this time value is set as 60minutes.After the 60 minutes the ARP will again sent request for the MAC address. If there occurs a conflict between the stored value and the value obtained from ARP reply, there can be to cases:

1. The host stored in the table is no longer alive
2. There was a man-in-the-middle attack

Hence inorder to confirm among the two cases, ARP will send multiple(50) unicast requests to the host in the table at random intervals with an average of 10 msec. If it receives atleast one reply it will conclude that an attack has occurred and hence will retain the data in the table and drop the one obtained by ARP reply. Suppose that the ARP reply was obtained during the ARP unicast request, it will come to an assumption that the host in the table is no longer active and therefore update the table with the new value.

7. Analysis

Three different techniques to detect IP spoofing attack have been studied. All the three papers specify three different ways to detect IP spoofing attack. Based on the study an analysis is done to identify the pros and cons of the three techniques.

Table 1: Result Comparison

Methods	Aiming at higher network security through extensive Penetration tests	Defense Against Spoofed IP Traffic Using Hop-Count Filtering	A protection Method against Unauthorized Access and Address Spoofing for Open Network Access Systems	Enhanced ARP: Preventing ARP Poisoning-Based Man-in-the-Middle Attacks
Complexity	Consists of four phases: Planning Discovery Exploitation Reporting	Requires to find the hop count value to each of the trustful IP address initially.	Requires to have an additional configuration set up with authentication center, IP address assigning center and a filter.	Not much complicated. Overhead occurs only during those cases in which to send 50 ARP requests.
Efficiency	This method needs to be carried out continuously.	This method is not a perfect one.But still it can discard most of the IP spoofed packets.	This method proves to be an efficient method as it checks the MAC address also.	Highly efficient for preventing the man-in-the-middle attack.

8. Suggestions

IP spoofing attack is an effective technique used by intruders in which they use the unique IP address replacement technique to gain access to a system in an unauthorized manner. Hence IP spoofing can be considered as a technique of fooling a party and hence gain the authorization. Above we have seen three different technique by which to detect IP spoofed packets. Now here are some suggestions by which IP spoofing attack can be prevented.

Method 1:
One of the major reason why the spoofing attack occurs is because the authentication is done just based on the source IP address. There should be some technique in which IP address is not the only criteria by which authentication are to be made.

Method 2:

In the first paper it was seen that spoofing can take place due to the design flaws of UDP. However TCP provides a more effective mechanism .This is because TCP establishes a connection between sender and receiver through a three way handshake mechanism. This three way handshaking mechanism can avoid spoofing because if the source address was spoofed the receiver on sending the acknowledgement to the sender the trusted host whose IP address was used for spoofing will respond with an error message. This will help to prevent IP spoofing.

Method 3:

Disable the ping commands. Even though ping commands are used rarely it can be used to trigger a DOS attack by flooding the victim with ICMP packets.

9. Conclusion

Security is a vital component of every network design. When planning, developing and deploying a network one should understand the importance of a strong security policy. A security policy defines what people can and can't do with network components and resources. There are different types of attack on internet, passive attack, active attack, Distributed Attack, Insider Attack, Phishing Attack, spoofing attack etc. All these attack have their own characteristics and hence the tester should be very vigilant about the attacker. Even though IDS and firewall are very successful method that ensures network security it does not produce better results in certain cases. Through this paper we can analyze different techniques through which to detect ma-in-the-middle attack and spoofing attack. A comparison of the four methods is made based on complexity and efficiency.

Reference

[1] http://seminarprojects.com/Thread-IP-spoofing-seminar-report#ixzz2BsndgFKr.
[2] Bechtsoudis and N. Sklavos," Aiming at Higher Network Security Through Extensive Penetration Tests", IEEE Latin America Transactions, Vol. 10, No. 3, April 2012.
[3] Haining Wang, Cheng Jin, and Kang G. Shin," Defense Against Spoofed IP Traffic Using Hop-Count Filtering", IEEE/Acm Transactions On Networking, Vol. 15, No. 1, February 2007.
[4] The Swiss Education and Research Network, Default TTL values in TCP/IP. 2002 [Online]. Available: http://secfr.nerim.net/docs/fingerprint/en/ttl_default.html.
[5] B. Krishnamurthy and J. Wang, "On network-aware clustering of web clients," in Proc. ACM SIGCOMM, 2000, pp. 97–110.
[6] Ishibashi, H., Yamai, N., Abe, K. and Matsuura, T., "A protection method against unauthorized access and address spoofing for open network access systems", IEEE Pacific Rim Conference on Communication and Signal Processing, 2001.
[7] Seung Yeob Nam, Dongwon Kim, and Jeongeun Kim," Enhanced ARP: Preventing ARP Poisoning-Based
[8] Man-in-the-Middle Attacks", IEEE Communications Letters, Vol. 14, No. 2, February 2010.