IP Spoofing

Mohit Taneja[1], Anil Dhankhar[2], Nirmala Choudhary[3]
[1]Dept of MCA
[2]Assoc. Professor, Dept of MCA
[3]Asst. Professor, Dept of MCA
[1, 2, 3] RIET Jaipur

Abstract- *"IP spoofing is a method of attacking a network in order to gain unauthorized access. The attack is based on the fact that Internet communication between distant computers is routinely handled by routers which find the best route by examining the destination address, but generally ignore the origination address. The origination address is only used by the destination machine when it responds back to the source.*

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 to 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."

Keywords- IP Spoofing • Spoofing Attacks • Non-Blind Spoofing • Blind Spoofing • Man in the Middle Attack • Denial of Service Attack. IP Spoofing Steps • Why IP Spoofing is used • Applications of IP spoofing

I. INTRODUCTION

Criminals have long employed the tactic of masking their true identity, from disguises to aliases to caller-id blocking.

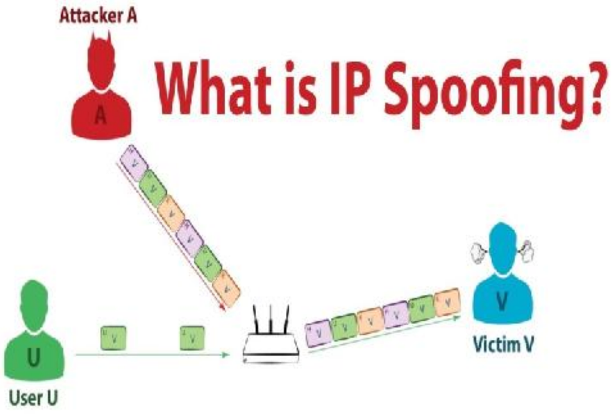
It should come as no surprise then, that criminals who conduct their nefarious activities on networks and computers should employ such techniques. IP spoofing is one of the most common forms of on-line camouflage.

In IP spoofing, an attacker gains unauthorized access to 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 the subsequent pages of this report, we will examine the concepts of IP spoofing: why it is possible, how it works, what it is used for and how to defend against it.

II. SPOOFING ATTACKS

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.



*A.*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 sniffed, eliminating the potential difficulty of calculating them accurately. The biggest threat of spoofing in this instance would be session hijacking. This is accomplished by corrupting the data stream of an established connection, then reestablishing it based on correct sequence and acknowledgement numbers with the attack machine. Using this technique, an attacker could effectively bypass any authentication measures taken place to build the connection.

B. Blind Spoofing

This is a more sophisticated attack, because the sequence and acknowledgement numbers are unreachable. In order to circumvent this, several packets are sent to the target machine in order to sample sequence numbers.

While not the case today, machines in the past used basic techniques for generating sequence numbers. It was relatively easy to discover the exact formula by studying packets and TCP sessions. Today, most OSs implement random sequence number generation, making it difficult to predict them accurately.

If, however, the sequence number was compromised, data could be sent to the target. Several years ago, many machines used host-based authentication services (i.e. Rlogin). A properly crafted attack could add the requisite data to a system (i.e. a new user account), blindly, enabling full access for the attacker who was impersonating a trusted host.

C. 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.

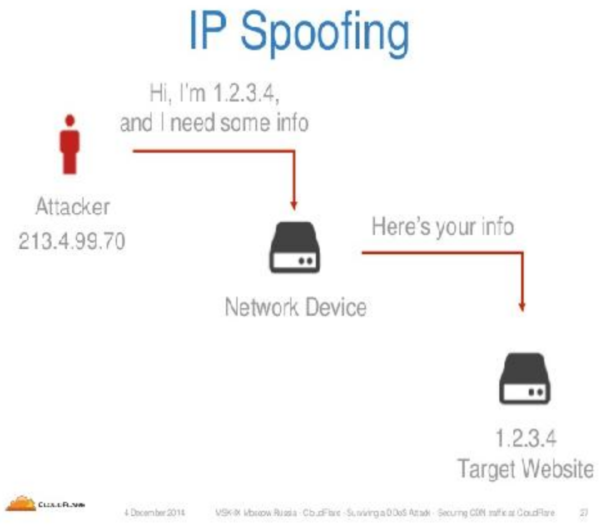
In this way, an attacker can fool a victim into disclosing confidential information by "spoofing" the identity of the original sender, who is presumably trusted by the recipient.

D. Denial of Service Attack

IP spoofing is almost always used in what is currently one of the most difficult attacks to defend against – denial of service attacks, or DOS. Since crackers are concerned only with consuming bandwidth and resources, they need not worry about properly completing handshakes and transactions.

Rather, they wish to flood the victim with as many packets as possible in a short amount of time. In order to prolong the effectiveness of the attack, they spoof source IP addresses to make tracing and stopping the DOS as difficult as possible.

When multiple compromised hosts are participating in the attack, all sending spoofed traffic; it is very challenging to quickly block traffic.



III. IP SPOOFING STEPS

- Selecting a target host (the victim)
- Identify a host that the target "trust"
- Disable the trusted host , sampled the target's TCP sequence
- The trusted host is impersonated and the ISN forged.
- Connection attempt to the service that only requires address-based authentication.
- If successfully connected, executes a simple command to leave a backdoor.

IV. WHY IP SPOOFING IS USED..?

IP spoofing is used to commit criminal activity online and to breach network security. Hackers use IP spoofing so they do not get caught spamming and to perpetrate denial of service attacks. These are attacks that involve massive amounts of information being sent to computers over a network in an effort to crash the entire network. The hacker does not get caught because the origin of the messages cannot be determined due to the bogus IP address.

IP spoofing is also used by hackers to breach network security measures by using a bogus IP address that mirrors one of the addresses on the network. This eliminates the need for the hacker to provide a user name and password to log onto the network.

V. APPLICATIONS OF IP SPOOFING

Many other attacks rely on IP spoofing mechanism to launch an attack, for example SMURF attack (also known as

ICMP flooding) is when an intruder sends a large number of ICMP echo requests (pings) to the broadcast address of the reflector subnet.

The source addresses of these packets are spoofed to be the address of the target victim. For each packet sent by the attacker, hosts on the reflector subnet respond to the target victim, thereby flooding the victim network and causing congestion that results in a denial of service (DOS).

Therefore, it is essential best practice to implement anti spoofing mechanisms to prevent IP spoofing wherever feasible.

Anti-spoofing control measures should be implemented at every point in the network where practical, but they are usually most effective at the borders among large address blocks or among domains of network administration.

VI. FUTURE SCOPE

If the suggestion as given in my paper will be implemented practically; it is the most chances to free our internet from IP Spoofed Attack and also chances to explore my idea in future to enhance the security in the field of Internet & Network too.

VII. CONCLUSION

IP spoofing is less of a threat today due to the patches to the Unix Operating system and the widespread use of random sequence receive numbering.

Many security experts are predicting a shift from IP spoofing attacks to application-related spoofing in which hackers can exploit a weakness in a particular service to send and information under false identities.

As Security professionals, we must remain current with the Operating Systems that we use in our day to day activities. A steady stream of changes and new challenges is assured as the hacker community continues to seek out vulnerabilities and weaknesses in our systems and our networks.

REFERENCES

[1] P. Ramesh Babu, D.LalithaBhaskari, CH.Satyanarayana,”A Comprehensive Analysis of Spoofing” (IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 1, No.6, December 2010.

[2] VimalUpadhyay. Rajeev kumar.” DETECTING AND PREVENTING IP SPOOFED ATTACK BY HASHED ENCRYPTION” International Journal of Enterprise Computing and Business Systems ISSN (Online) : 2230-8849 http://www.ijecbs.com Vol. 1 Issue 2 July 2011

[3] Haining Wang, Member, IEEE, Cheng Jin, and Kang G. Shin, Fellow, IEEE, “Defense Against Spoofed IP Traffic Using Hop-Count Filtering”, IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 15, NO. 1, FEBRUARY 2007.

[4] 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.

[5] Wagner, R. (2001) Address Resolution Protocol Spoofing and Man in the Middle Attacks. SANS Institute .Error! Hyperlink reference not valid..

[6] www.google.com

[7] www.wikipedia.com

[8] www.studymafia.org