A Comparative Analysis on IP Spoofing Detection & Prevention on Route Based Information

[1]Parul

[1]College of Computing Science and Technology, TMU Moradabad

E-mail- **parul0295@gmail.com**

***Abstract*—IP spoofing is used in one of the most difficult attack to defend against – Denial of Service (DoS) attack. DOS attack is evolving due to increase of diverse network application. The IP packet header information is efficiently handled by routers, hence proposing a technique the uses the router specific features will be best suited for real time processing. In this paper we introduce a technique which uses the router specific information to identify the IP spoofing based attack and mitigate it using that information. This paper is on — "Proposed methods of IP Spoofing Detection & Prevention". This paper contains an overview of IP address and IP Spoofing and its background. It also shortly discusses various types of IP Spoofing, how they attack on communication system. This paper spoofing and also describes impacts on communication system by IP Spoofing.**

***Keywords*— Dos attack, IP Spoofing, IP address, Information, Trust, Filtering.**

I. INTRODUCTION

Criminals have long employed the tactic of masking their true identity, from disguises to aliases to caller-id blocking. The basic protocol for sending data over the Internet network and many other computer networks is the Internet Protocol ("IP"). Spoofing can take on many forms in the computer world, all of which involve some type false representation of information. There are a variety of methods and types of spoofing. We would like to introduce and explain following

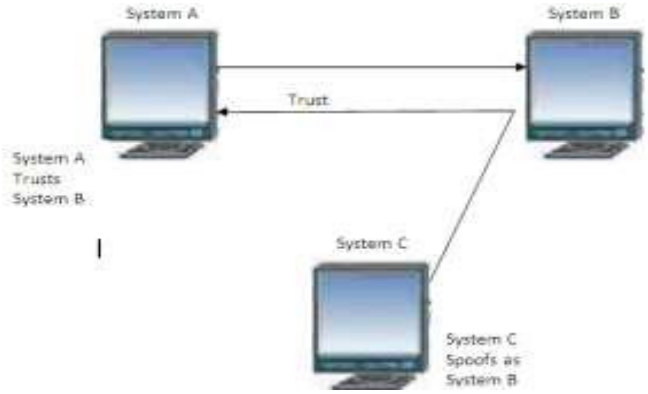
A. Types in this paper:

- IP Spoofing
- ARP Spoofing
- E-Mail Spoofing
- Web Spoofing
- DNS Spoofing

II. IP SPOOFING

IP spoofing is used to gain unauthorized access to a computer. The attacker forwards packets to a computer with a source address indicating that the packet is coming from a trusted port or system. Attackers must go through some complicated steps to accomplish the task [1]. They must:

- Obtain a target.
- Obtain an IP address of a trusted machine.
- Disable communication of the trusted machine (e.g. SYN flooding).
- Sample a communication between the target and trusted hosts.
- Guess the sequence numbers of the trusted machine.
- Modify the packet headers so that it appears that the packets are coming from the trusted host.
- Attempt connection to an address authenticated service or port.
- If successful, the attacker will plant some kind of backdoor access for future reference.



III. ARP SPOOFING

ARP stands for Address Resolution Protocol. ARP is used to map IP addresses to hardware addresses. A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP. When an incoming packet sent to a host machine on a network arrives at a router, it asks the ARP program to find a MAC address that matches the IP address. The ARP program looks in the ARP cache and, if it finds the address, provides it so that the packet can be converted to the right packet length and ARP updates the ARP cache for future reference and then sends the packet address to the MAC that replied.

IV. E-MAIL ADDRESS SPOOFING

E-mail spoofing can be used for malicious purposes such as spreading viruses, trawling for sensitive business data and other industrial espionage activities. If you receive a snail mail letter, you look to the return address in the top left corner as an indicator of where it originated. E-mail messages contain return addresses, too – but they can likewise be deliberately misleading, or "spoofed." Senders do this for various reasons, including:

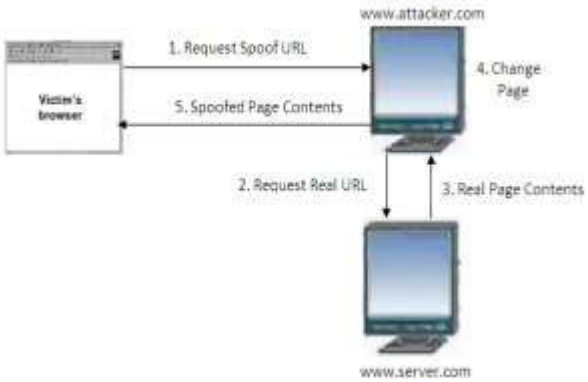
- The e-mail is spam and the sender doesn't want to be subjected to anti-spam laws
- The e-mail constitutes a violation of some other law (for example, it is threatening or harassing).
- The e-mail contains a virus or Trojan and the sender believes you are more likely to open it if it appears to be from someone you know.
- The e-mail requests information that you might be willing to give to the person the sender is pretending to be (for example, a sender might pose as your company's system administrator and ask for your network password), as part of a "social engineering" attack.
- The sender is attempting to cause trouble for someone by pretending to be that person (for example, to make it look as though a political rival or personal enemy said something he/she didn't in an e-mail message).

.

V. WEB SPOOFING

Web Spoofing is an attac Web Spoofing works on both Internet Explorer and Netscape and is not necessarily prevented by secure connections. This is due the way that the SSL protocol uses certificates to authenticate websites. The attacker can observe and modify all web pages and form submissions, even when the browser is indicating that there is a secure connection. The attack can be implemented using JavaScript and Web server plug-ins, and works in two parts. First, the attacker causes a browser window to be created on the victim's machine, with some of the normal status and menu information replaced by identical-looking components supplied by the attacker.

Current browsers do not completely prevent Web Spoofing, and there seems to be little movement in the direction of addressing this problem. I believe that there can be no fully secure electronic commerce on the Web until the Spoofing vulnerability has been addressed.



VI. DNS SPOOFING

A DNS spoofing attack can be defined as the successful insertion of incorrect resolution information by a host that has no authority to provide that information.

According to the most recent "Domain Health Survey" (Feb 2003), a third of all DNS servers on the Internet are vulnerable to spoofingsh Operating normally, a customer can expect to *query*

their DNS server to discover the IP address of the named host they wish to connect to. The following diagram reflects this process.

Fig 1: The Normal DNS Motion Process

A. The customer queries the DNS server – "What is the IP address of www.bank.com?"

B. The DNS responds to the customer query with "The IP address of www.bank.com is 150.10.1.21"

C. The Customer then connects to the host at 150.10.1.21-- expecting it to be www.bank.com. However, with a successful DNS spoofing attack, the process has been altered. The following diagram reflects this process.

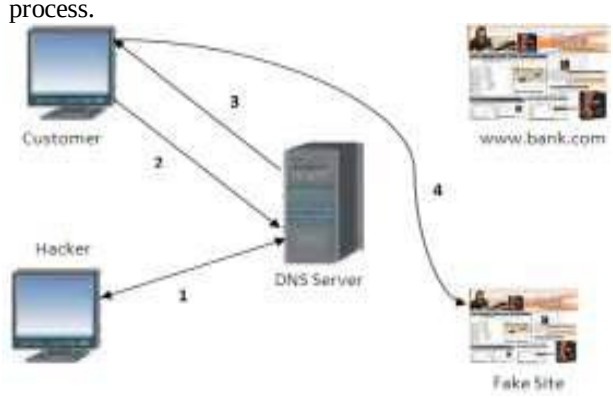


Fig 2: The DNS motion process having fallen victim to a DNS spoofing attack

A. The attacker targets the DNS service used by the customer and adds/alters the entry for www.mybank.com – changing the

B. stored IP address from 150.10.1.21 to the attacker's fake site IP address (200.1.1.10).

C. 2. The customer queries the DNS server "What is the IP address of www.bank.com"

D. 3. The DNS responds to the customer query with "The IP address of www.bank.com is 200.1.1.10" – not the real IP address.

E. 4. The Customer then connects to the host at 200.1.1.10 – expecting it to be www.bank.com, but in fact reaching the attackers fake site.

VII. Spoofed Packet Detection

Packets sent using the IP protocol include the IP address of the sending host. The recipient directs replies to the sender using this source address. Detection methods can be classified as those requiring router support, active host-based methods, passive host based methods, and administrative methods. Administrative methods are the most commonly used methods today. When an attack is observed, security personnel at the attacked site contact the security personnel at the supposed attack site and ask for corroboration.

This section describes a number of such methods.

VII [1]. Routing Methods

Because routers (or IP level switches) can know which IP addresses originate with which network interface, it is possible for them to identify packets that should not have been received by a particular interface. Filtering inbound packets, known as ingress filtering, protects the organization from outside attacks. Similarly, filtering outbound packets prevents internal computers from being involved in spoofing attacks.

Table #1: Special IP Addresses

Private Networks (RFC 1918) --	
10.0.0.0/8	
172.16.0.0/12	
192.168.0.0/16	
Special / IANA Reserved --	
0.0.0.0/8	- Historical Broadcast
127.0.0.0/8	- Loopback
169.254.0.0/16	- Link Local Networks
192.0.2.0/24	- TEST-NET
240.0.0.0/5	- Class E Reserved
248.0.0.0/5	- Unallocated
255.255.255.255/32	- Broadcast

Table 1: Special IP addresses

VII [2]. Non-routing methods

Computers receiving a packet can determine if the packet is spoofed by a number of active and passive ways. We use the term active to mean the host must perform some network action to verify that the packet was sent from the claimed source. Passive methods require no such action; however anactive method may be used to validate cases where the passive method indicates the packet was spoofed. There are some other methods for detecting spoofed packets:

A. If we monitor packets using network-monitoring software such as netlog, look for a packet on our external interface that has both its source and destination IP addresses in your local domain. If we find one, you are currently under attack.
B. 2. Another way to detect IP spoofing is to compare the process accounting logs between systems on our internal network. If the IP spoofing attack has succeeded on one of our systems, we may get a log entry on the victim machine showing a remote access; on the apparent source machine, there will be no corresponding entry for initiating that remote access.

There are some configuration and services that are vulnerable to IP spoofing:

- RPC (Remote Procedure Call services)
- Any service that uses IP address authentication
- The X Window System
- The R services suite (rlogin, rsh, etc.)

Some Softwares that are caused for IP Spoofing:

- Mac Spoofing
- Macaroni Screen Saver Bundle
- SpoofMAC
- sTerm
- MAC Change

VIII. IP Spoofing Prevention Methods

Compression

Basically compression classified into two types-

VIII [1] Lossy Compression

In Computer terminology, lossy compression is a data encryption method which eliminates some of the data, in order to achieve its goal, with the result that decompressing the data yields content that is different from the original, though similar enough to be useful in some way. Lossy compression is most commonly used to compress multimedia data, audio, video, image, etc. lossless compression is required for text and data files, such as bank records, text articles, etc. In many cases it is advantageous to make a master lossless file which can then be used to produce compressed files for different purposes.

VIII [2] Lossless Compression

Lossless data compression is a kind of data compression algorithms that allows the exact original data to be fetched from the compressed ZIP data. The term lossless is in contrast to lossy data compression, which only allows an approximation of the original data to be re fetched, in exchange for better compression rates. Lossless data compression is used in many applications. For example, it is used in the popular ZIP file format and in the kernel OS UNIX tool gzip. It is also often used as a component within lossy data compression technologies.

IX. Software to Stop IP Spoofing

We can use some software's to stop IP Spoofing:

- StopCut
- Find Mac Address pro
- SecurityGateway for Exchange / SMTP
- PacketCreator
- Responder Pro

X. Conclusion

This paper describes the use of IP spoofing as a method of attacking a network in order to gain unauthorized access and some detection and prevention methods of IP spoofing. 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. We think that our proposed methods will be very helpful to detect and stop IP spoofing and give a secured communication system.

XI. References

[1] Leila Fatmasari Rahman, Rui Zhou. **IP Address Spoofing,** (December 16, 1997). CERT Advisory CA-1997-28. IP Denial-of-Service Attacks. CERT/CC.

[2] Computer Incident Advisory Committee (CIAC) (1995).Advisory Notice F-08 Internet Spoofing and HijackedSession Attacks.

[3]www.wikipedia.com

[4] http://www.puc.net/email_spoofing.htm

[5] A. Bermlerand H. Levy. "Spoofing prevention Method," INFOCOM'05, 2005.

[6] Daemon, Route, Infinity, "IP Spoofing Demystified", Phrack Magazine;
1996;