A

Seminar report

On

Ip Spoofing

Submitted in partial fulfillment of the requirement for the award of degree
Of Computer Science

SUBMITTED TO:

www.studymafia.org

SUBMITTED BY:

www.studymafia.org

Preface

I have made this report file on the topic **"IP spoofing".** I have tried my best to elucidate all the relevant detail to the topic to be included in the report. While in the beginning I have tried to give a general view about this topic.

My efforts and wholehearted co-corporation of each and everyone has ended on a successful note. I express my sincere gratitude to ……..who assisting me throughout the prepration of this topic. I thank him for providing me the reinforcement, confidence and most importantly the track for the topic whenever I needed it.

Acknowledgement

I would like to thank respected Mr…….. and Mr. ……..for giving me such a wonderful opportunity to expand my knowledge for my own branch and giving me guidelines to present a seminar report. It helped me a lot to realize of what we study for.

Secondly, I would like to thank my parents who patiently helped me as i went through my work and helped to modify and eliminate some of the irrelevant or un-necessary stuffs.

Thirdly, I would like to thank my friends who helped me to make my work more organized and well-stacked till the end.

Next, I would thank Microsoft for developing such a wonderful tool like MS Word. It helped my work a lot to remain error-free.

Last but clearly not the least, I would thank The Almighty for giving me strength to complete my report on time.

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.

What is IP Spoofing

- An IP (Internet Protocol) address is the address that reveals the identity of your Internet service provider and your personal Internet connection. The address can be viewed during Internet browsing and in all of your correspondences that you send.
- IP spoofing hides your IP address by creating IP packets that contain bogus IP addresses in an effort to impersonate other connections and hide your identity when you send information. IP spoofing is a common method that is used by spammers and scammers to mislead others on the origin of the information they send.

How IP Spoofing Works

The Internet Protocol or IP is used for sending and receiving data over the Internet and computers that are connected to a network. Each packet of information that is sent is identified by the IP address which reveals the source of the information.

When IP spoofing is used the information that is revealed on the source of the data is not the real source of the information. Instead the source contains a bogus IP address that makes the information packet look like it was sent by the person with that IP address. If you try to respond to the information, it will be sent to a bogus IP address unless the hacker decides to redirect the information to a real IP address.

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.

Brief History of IP Spoofing

The concept of IP spoofing was initially discussed in academic circles in the 1980's.
In the April 1989 article entitled: “Security Problems in the TCP/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.

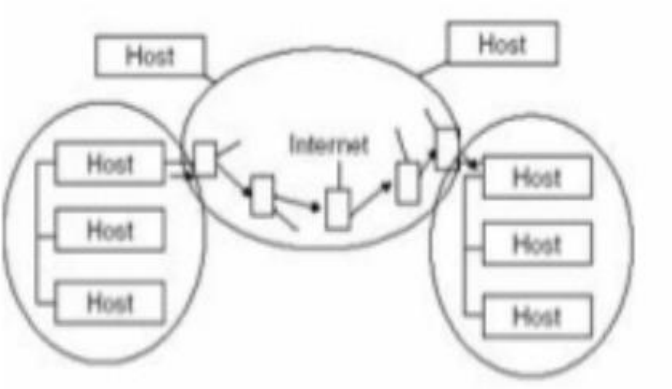
Bellovin describes how Robert Morris, creator of the now infamous Internet Worm, figured out how TCP created sequence numbers and forged a TCP packet sequence. This TCP packet included the destination address of his “victim”
and using an IP spoofing attack Morris was able to obtain root access to his targeted system without a User ID or password.

Another infamous attack, Kevin Mitnick's Christmas Day crack of Tsutomu Shimomura's machine, employed the IP spoofing and TCP sequence prediction techniques. While the popularity of such cracks has decreased due to the demise of the services they exploited, spoofing can still be used and needs to be addressed by all security administrators.

A common misconception is that "IP spoofing" can be used to hide your IP address while surfing the Internet, chatting on-line, sending e-mail, and so forth. This is generally not true. Forging the source IP address causes the responses to be misdirected, meaning you cannot create a normal network connection. However, IP spoofing is an integral part of many network attacks that do not need to see responses (blind spoofing).

3. Why IP Spoofing is Easy

- Problem with the Routers. IP routing is hop by hop. Every IP packet is routed separately. The route of an IP packet is decided by all the routers the packet goes through.
- Routers look at Destination addresses only.
- Authentication based on Source addresses only.
- To change source address field in IP header field is easy [1]



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.

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.

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 re-establishing 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.

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.

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.

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.

ADVANTAGES

Multiple Servers :

Sometimes you want to change where packets heading into your network will go. Frequently this is because you have only one IP address, but you want people to be able to get into the boxes behind the one with the `real' IP address.

Transparent Proxying :

Sometimes you want to pretend that each packet which passes through your Linux box is destined for a program on the Linux box itself.

This is used to make transparent proxies: a proxy is a program which stands between your network and the outside world, shuffling communication between the two.

The transparent part is because your network won't even know it's talking to a proxy, unless of course, the proxy doesn't work.

DISADVANTAGES

Blind to Replies

A drawback to ip source address spoofing is that reply packet will go back to the spoofed ip address rather than to the attacker.

This is fine for many type of attack packet. However in the scanning attack as we will see next the attacker may need to see replies .in such cases, the attacker can not use ip address spoofing.

Serial attack platforms :

However, the attacker can still maintain anonymity by taking over a chain of attack hosts. The attacker attacks the target victim using a point host-the last host in the attack chain.

Even if authorities learn the point host's identity .They might not be able to track the attack through the chain of attack hosts all the way back to the attackers base host.

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.

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.

Reference

- www.google.com
- www.wikipedia.com
- www.studymafia.org