A Study on Network Attacks: Firewall Basics

Prof. Kinjal Joshi[1], Elvin Varghese[2], Chandni Dave[3]
[1,2,3]Computer Engineering Department,
[1,2,3]A.D. Patel Institute of Technology (GTU), Karamsad.

Abstract:In today's time, all our important documents are on the virtual platform and so there is always a need to provide security to them. Lack of proper security mechanism can lead to the loss of classified data and sometimes to cyber thefts. Thus, there is a need for a firewall to protect the user from all these cyber breaches. Setting up a firewall needs the programmer to study about all the attacks that the firewall has to defend and so in this review paper we will study about different attacks that can happen on a firewall and the kind of threats they pose. A study on different kinds of attacks has been carried out to know what threats a user can face and this will help to know how a firewall can be set up efficiently.

Keywords:
Attacks, active, passive unauthorized access, spoofing, Dos attack, ping of death, smurf attack.

1. Introduction:

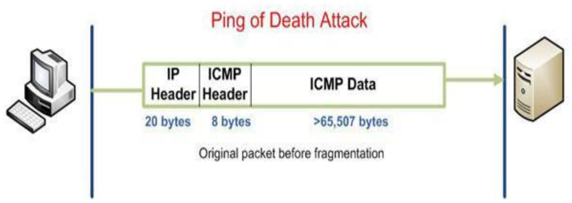
Attacks are mainly of two types, Active and Passive. The attacker tries to bypass into secured systems by introducing worms, viruses or Trojan horses in an Active attack. They include attempts to break protection features and steal or modify information. It results in the disclosure or dissemination of data files, DoS, or modification of data. In Passive attacks unprotected communications are monitored, weakly encrypted traffic is decrypted and traffic analysis is done. Passive attacks result in the disclosure of information to the attacker without the consent or knowledge of the user.

The attacks we are going to study here are: Dos attack that includes the ping of death attack; unauthorized access, spoofing attack and the smurf attack.

Known DoS attacks in the Internet generally conquer the target by exhausting its resources, which can be anything related to network computing and service performance, such as link bandwidth, TCP connection buffers, application/service buffer, CPU cycles, etc. Individual attackers can also exploit vulnerability, break into target servers, and then bring down services. Unauthorised access is the act of gaining access to a network, system, application or other resource without permission. A spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data, thereby gaining an illegitimate advantage. All these attacks will be studied in detail in this paper.

2. Dos Attack (ping of death)

Many attack techniques can be used for DoS purpose as long as they can disable service, or downgrade service performance by exhausting resources for providing services. As it is impossible to enumerate all the existing Dos attack techniques, we will be focusing only on the ping of death Dos attack that is used for the firewall. **[1]** The TCP/IP specification allows for a maximum packet size of 65,536 octets. The ping of death attack sends oversized ICMP datagrams (encapsulated in IP packets) to the victim. Some systems, upon receiving the oversized packet, will crash, freeze, or reboot, resulting in denial of service.

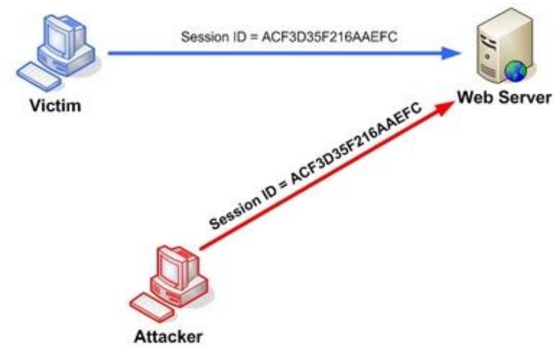


Some computer systems were never designed to properly handle a ping packet larger than the maximum packet size because it violates the Internet Protocol documented in RFC 791.[2] Like other large but well-formed packets, a ping of death is fragmented into groups of 8 octets before transmission. However, when the target computer reassembles the malformed packet, a buffer overflow can occur, causing a system crash and potentially allowing the injection of malicious code. In early implementations of TCP/IP, this bug is easy to exploit and can affect a wide variety of systems including Unix, Linux, Mac, Windows, and peripheral devices. As systems began filtering out pings of death through firewalls and other detection methods, a different kind of ping attack known as ping flooding later appeared, which floods the victim with so many ping requests that normal traffic fails to reach the system. This is the ping of death attack.

3. Unauthorized access

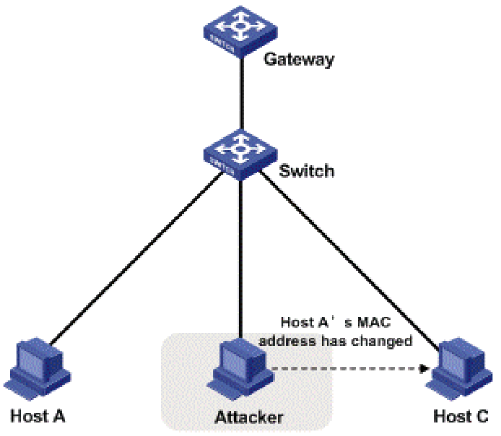
Unauthorised access is the act of gaining access to a network, system, application or other resource without permission. Unauthorised access could occur if a user attempts to access an area of a system they should not be accessing. Unauthorised access could be result of unmodified default access policies or lack of clearly defined access policy documentation.[3] If someone were to gain unauthorised access to your organisation's internal network, that person could cause damage in many ways, perhaps by accessing sensitive files from a host, by planting a virus, or by hindering network performance by flooding your network with illegitimate packets. To prevent unauthorized access, you can require users to be authenticated before they gain access into a network. When users attempt to access a service or host (such as a web site or file server) within the protected network, they must first enter certain data such as a username and password, and possibly additional identification information.

After successful authentication (depending on the method of authentication), users will be assigned specific privileges, allowing them to access specific network assets. In most cases, this type of authentication would be facilitated by using specific access protocols in conjunction with an authentication protocol, such as TACACS+ or RADIUS.



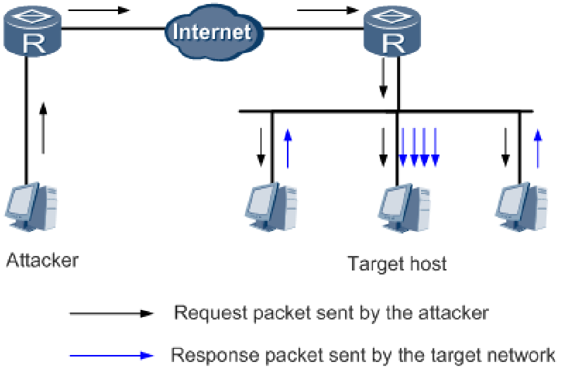
4. Spoofing Attack

[4]Many of the protocols in the TCP/IP suite do not provide mechanisms for authenticating the source or destination of a message. They are thus vulnerable to spoofing attacks when extra precautions are not taken by applications to verify the identity of the sending or receiving host. [5]Spoofing attacks which take advantage of TCP/IP suite protocols may be mitigated with the use of firewalls capable of deep packet inspection or by taking measures to verify the identity of the sender or recipient of a message. In computer networking, IP address spoofing or IP spoofing is the creation of Internet Protocol (IP) packets with a forged source IP address, with the purpose of concealing the identity of the sender or impersonating another computing system. IP spoofing can also be a method of attack used by network intruders to defeat network security measures, such as authentication based on IP addresses. This method of attack on a remote system can be extremely difficult, as it involves modifying thousands of packets at a time. This type of attack is most effective where trust relationships exist between machines. For example, it is common on some corporate networks to have internal systems trust each other, so that users can log in without a username or password provided they are connecting from another machine on the internal network (and so must already be logged in).



5. Smurf Attack

[6]Smurf attack overflows network traffic which is a kind of denial of service attack where with the help of spoofed broadcast ping messages flooding of target system is done. Generally smurf is used by attackers so that attack part cannot be operated. Smurfing can make use of Internet Protocol (IP) and Internet Control Message Protocol (ICMP). Basically network nodes and their administrators use ICMP for exchanging information regarding state of network. ICMP ping other nodes to check whether they are operating or not. A node which is operating basically sends an echo message when we send any ping message.


R
Internet
R
Attacker
Target host
Request packet sent by the attacker
Response packet sent by the target network

Smurf program forms a network packet seems to originate from another address that means spoofing an IP address. The packet basically has ICMP ping message addressing the IP broadcast address that means all IP addresses are within a given network. When ping messages will be sent responses come back to victim address. Due to flooding of number of pings and echoes inside a network it may cause hurdles for real traffic to pass through. The figure shows the working of a smurf attack.

6. Conclusion

The study of all the attacks mentioned above will help us to understand the working of these attacks better and as the working is understood their prevention becomes facile. The knowledge of the ways and means of how an attack happens lets us to design a firewall in such a way that offers complete protection in all sense. This study hence throws light on the needed information for setting up a firewall and providing protection against these attacks. Further study is in progress to find out more about the existing many complex attacks to design a firewall strong and more powerful against them.

7. References

1. Denial of Services, ComplexNetworks pdf

2. Erickson, Jon (2008). HACKING the art of exploitation (2nd ed.). San Francisco: NoStarch Press. p. 256. *ISBN 1-59327-144-1*.

3. Unauthorized Access Attack, MazeLabs

4. Tanase, Matthew (March 11, 2003). "IP Spoofing: An Introduction". Symantec. Retrieved September 25, 2015.

5. Gantz, John; Rochester, Jack B. (2005). Pirates of the Digital Millennium. Upper Saddle River, NJ 07458: Prentice Hall. ISBN 0-13-146315-2.

6. Sanjeev Kumar, “Smurf-based Distributed Denial of Service(DDOS), Attack Amplification in Internet”, Second International Conference on Internet Monitoring and Protection (ICIMP 2007) 0-7695-2911-9/07 2007 IEEE

7. M. Frantzen, F. Kerschbaum, E. Schultz, and S. Fahmy, “A framework for understanding vulnerabilities in firewalls using a dataflow model of firewall internals,”Computers and Security, vol. 20, no. 3, pp. 263–270, May 2001.

8. Froutan, Paul (June 24, 2004). "How to defend against DDoS attacks". Computerworld. Retrieved May 15, 2010.

9. Abante, Carl (March 2, 2013). "Relationship between Firewalls and Protection against DDoS". Ecommerce Wisdom. Retrieved 2013-05-24.

10. Fredrik Ullner (May 2007). "Denying distributed attacks". DC++: Just These Guys, Ya Know?. Retrieved 2007-08-22.