ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 1, March 2013

Network Attacks and Their Countermeasures

Ajit Kotkar[1], Alok Nalawade[2], Siddhesh Gawas[3], Aniket Patwardhan[4]

Student, Department of IT, RMCET, Devrukh, India[1,2,3,4]

ABSTRACT: For the first few decades of their existence, computer networks were primarily used by university researchers for sending e-mail and by corporate employees for sharing printers and other resources. Under these conditions, security did not get a lot of attention. But now, as millions of people are using networks for their daily use such as banking, shopping, and filing their tax returns, network security is looming on the horizon as a potentially massive problem. Because all their daily activities are data sensitive means data should not be altered. The requirements of information security within an organisation have undergone two major changes in the last several decades. Before the widespread use of data processing equipment, the security of information felt to be valuable to an organization was provided primarily by physical and administrative means .With the introduction of computer network attacks and their respective countermeasures can help us in securing our data and system from hackers. This paper provides you with brief introduction of attacks on network are various layers and their countermeasures.

Keywords*:* Host, Pretend, Source, Destination, Client, Server.

I. INTRODUCTION

As we know networking is large and very complex topic to understand. We are covering brief introduction required to understand networking attacks and their countermeasures. Basically network means collection of many devices such computers, switches. Routers etc

The two basic components of network are host and server. Here host can be server, client machine, router or any switch in network. But to enforce security in network we should consider above two components very first. Network does the work of transferring data to or from above components.

Transfer of data takes place only when both parties are agreed upon common protocol which is used in communication. Protocol is nothing but set of rules that should be followed by every party in communication. And every protocol has their layers in which data gets transferred or processed. For example OSI model has 7 layers architecture. Every protocol works on specific layers. Each protocol stack may have certain flaws in their architecture; an attacker may exploit those weaknesses in protocol stack to misuse of network. Attacker attacks on particular protocol in layer.

Basic network and its components are shown in below Fig.1. Figure shows two servers are connected to the router And the PCs are connected to the network through Ethernet Switch so they can communicate with servers.

Server - In the client/server programming model, a server is a program that awaits and fulfils requests from client programs in the same or other computers.

Client - A client is the requesting program or user in a client/server relationship. For example, the user of a Web browser is effectively making client requests for pages from servers all over the Web.

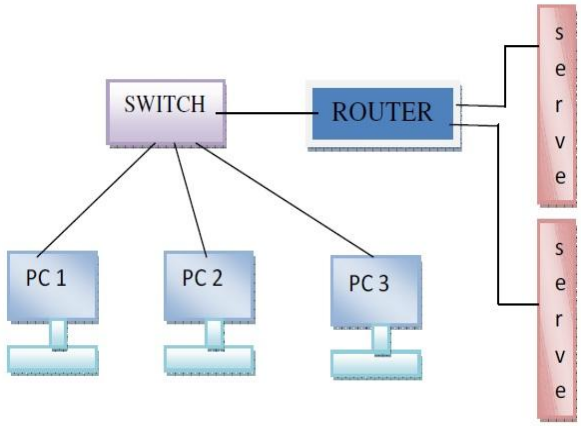

Fig.1 Basic Networking.

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 1, March 2013

II. ATTACKS AND THEIR COUNTERMEASURES

A. *Mac flooding*

1) *Theory:* In computer networking, MAC flooding is a technique employed to compromise the security of network switches. Essentially, MAC flooding inundates the network switch with data packets that disrupt the usual sender to recipient flow of data that is common with MAC addresses. Switches maintain a MAC (sometimes called as CAM) Table that maps individual MAC addresses on the network to the physical ports on the switch. This allows the switch to direct data out of the physical port where the recipient is located, as opposed to indiscriminately broadcasting the data out of all ports as a hub does. The advantage of this method is that data is bridged exclusively to the network segment containing the computer that the data is specifically destined for. In a typical MAC flooding attack, a switch is fed many Ethernet frames, each containing different source MAC addresses, by the attacker. The intention is to consume the limited memory set aside in the switch to store the MAC address table. This cause switches to enter into failopen state, in which switch will acts as hub. Attacker then can use packet sniffer to capture sensitive data. Some advance switch such as Cisco offers you protection against this attack.

2) *Countermeasures:* To prevent MAC flooding one of the following features should be configure in switch.
Port security: Post security should be configured which limits number of MAC addresses that can be learned on ports connected to end stations.
Implementations of IEEE 802.1X suites: It often allow packet filtering rules to be installed explicitly by an AAA server based on dynamically learned information about clients, including the MAC address.

B. *Session hijacking*

1) *Theory:* It is like taking over secure or unsecure web user session by gaining session ID. Once user's session ID is accessed, the attacker can pretend as original user and does anything that user is authorized to do on that network. As sown in Fig. 2. In case of web communication server send some data to user called as "COOKIE". Cookie is the place where attacker gets session ID of user. This cookie is sent back by user to server when he accesses web for authentication. Attacker gets this cookie and sends to server and pretends as original user.

2) *Methods of session Hijacking :* The methods are listed below,
IP spoofing*:* Attacker uses this method when he wants to send malicious content to target machine and don't wish to get identified. Victim assumes that packet is from trusted host and it accepts packet, response back to source computer. Attacker must guess proper sequence number and if this step gets successful attacker can establish connection with victim's machine.
Session side hijacking*:* Here attacker use packet sniffing tools to get session cookie file .Web sites uses SSL encryption for login pages to prevent attackers to get password but there might be chances of no encryption for rest of communication. Attacker exploits this weakness and get cookie of original sender.
Cross-Site Scripting : User makes one hyperlink with lots of malicious data attached to link. When user visit website and click on hyperlink attacker can send malicious contents to user computer and user will be totally unaware of this.

3) *Diagram*

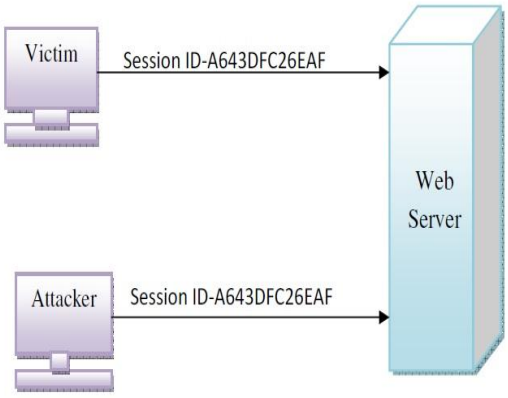

Fig.2 Session Hijacking.

4) *Countermeasures :* There are several types of countermeasures which are listed below:
Encryption: Banks and e-commerce services should use this technique because it prevents sniffing style attacks. Some user services make additional checks against identity of the user.
String as Session key: This prevents attacker to guess valid session key through Brute Force attack.

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 1, March 2013

Regenerating of Session ID after a Successful Login: This method prevents session fixation, because attacker does not know the Session ID of the user after he has logged in.

C. IP Spoofing

1) *Theory:* IP spoofing enables attacker to gain access to computer on which he does not have access to. Attacker makes fool by sending messages pretending he is trusted host. IP is the basic protocol to communicate over internet and we know IP header has source and destination address of a packet .When transferring of packet attacker change source address and put his address as source IP address and pretend he is original sender as shown in Fig. 3. Destination host will start sending packet to attacker. This technique is used when attacker does not care about responses.
2) *Diagram :*

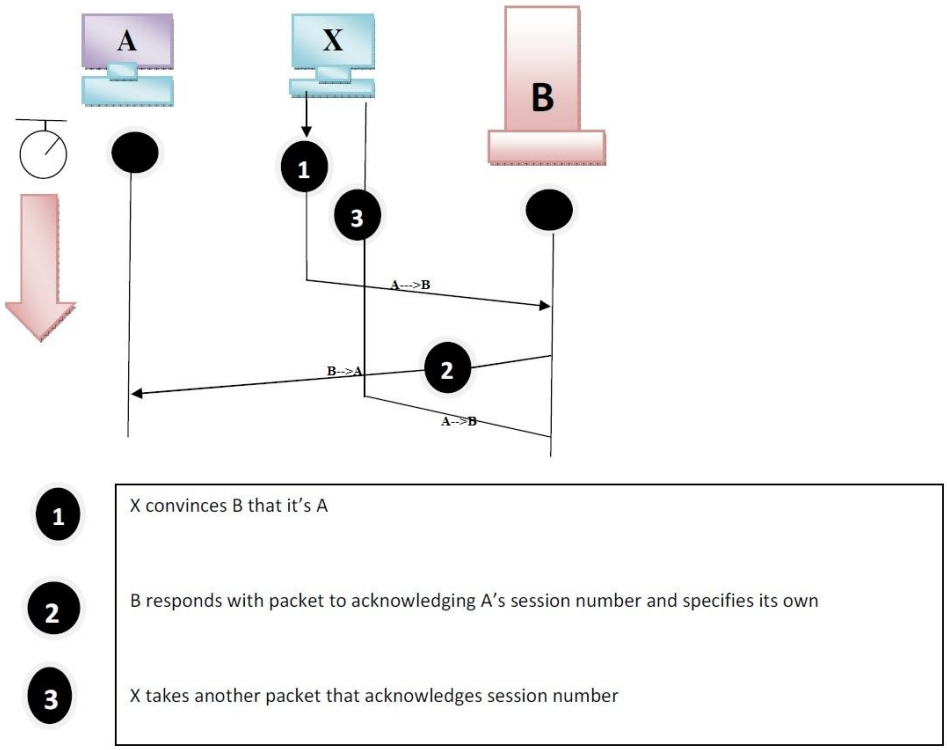

Fig. 3 IP spoofing.

3) *Countermeasures :* The countermeasures are given below
Encryption and Authentication: This technique is implemented in IP V6 that eliminates current spoofing threats. There should be proper authentication process in place.
Router filtering: Spoofing can be defence at router level by implementing ingress and egress filtering. Access Control List should be maintaining to allow only trusted IP to interact with your network.

C. Denial of Service Attack.

1) Theory: The function of a denial of service attack is fundamentally to flood its target machine with so much traffic that it prevents it from being accessible to any other requests or providing services. The target machine is kept so busy responding to the traffic it is receiving from its attacker that it has insufficient resources to respond to legitimate traffic on the network. A distributed denial of service (D-DOS) attack adds a many-to-one dimension to these forms of attacks. This form of denial of service generally involves a machine containing a master program and several machines which have been enslaved as zombie machines. They are referred to as zombies as these machines which are originally the victim of a denial of service attack unwittingly become an attacker. These zombies or daemons reside on the victim's machine until they are instructed by the master machine to attack another target. This makes it almost impossible to track down the real attacker as the attack is coming from zombie machines which have no knowledge of the origin of the attack.

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 1, March 2013

2) Diagram :

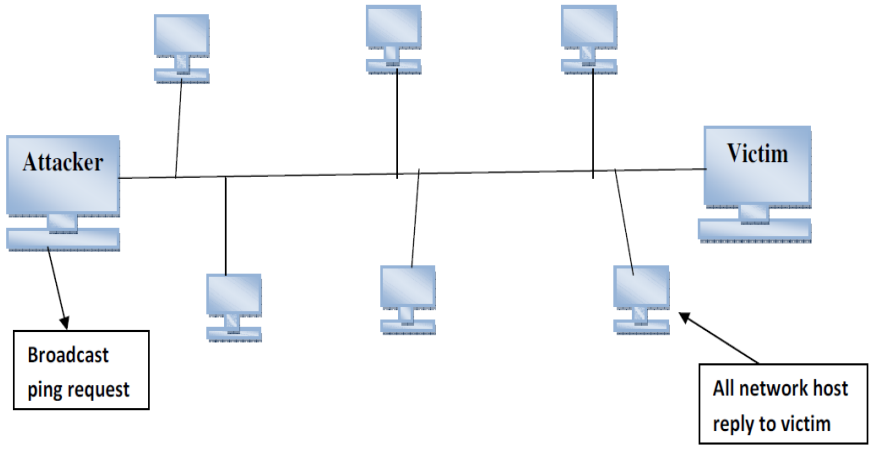

Fig. 4 DOS attack.

3) Countermeasures: The DOS [3] attack has following countermeasures ,
Smurf Attack*:* This form of an attack involves sending Internet Control Message Protocol (ICMP) or ping requests to multiple Internet Protocol (IP) broadcast addresses. All of these messages have a spoofed source address of the intended victim. The hosts receiving the ICMP echo request upon accepting it reply with an echo to the source address, which in this case is the target of the attack. The weight of this attack is therefore effectively multiplied by the number of responding hosts. If the attack took place on a multi-broadcast network there could potentially be hundreds of machines to reply to each packet sent.

UDP Flood: A UDP flood, also known as a fragile, is a cousin to the Smurf attack. This is based on UDP echo and character generator (chargen). It uses a forged UDP packet to connect the echo service on one machine to the chargen on another. These two machines then uses up all available bandwidth, sending characters back and forth between themselves.

SYN Flood: A SYN flood exploits the TCP standard 3-way handshake protocol. The attacker initiates a connect request to the server and then ignores the acknowledgement (ACK). This forces the server to wait for the ACK from the attacker, wasting time and resources. A server can at any given time only process a fixed number of requests and so this form of attack can effectively block all legitimate traffic.

III. CONCLUSION

In this paper, we have addressed most common network attacks and their common and simple countermeasures. We have discussed security threats on network. We have started from MAC layer vulnerabilities to Application layer vulnerabilities. Then we discussed what an ethical hacker can do with our network if network is weak. We have given some tricks to defence against most common attacks.

ACKNOWLEDGMENT

It is an opportunity of immense pleasure for us to present the paper "Network Attacks and Their Countermeasures" expressing our heart left gratitude to all those who have generously offered their valuable suggestions towards the completion of the paper. The credit goes to our Prof. Yadav A.B. (RMCET, Ambav, Ratnagiri) whose positive attitude; moral support and encouragement lead to the success of the paper.

REFERENCES

1. Andrew S.Tanenbaum, 'Computer Networks', 2005, Fourth Edition, Pearson Education.
2. Yogesh Kothari, 'System Security Information Security', 2012, Nandu publication.
3. Deven N. Shah, 'IFORMATION SECURITY', First Edition, Wiley India.
4. Peterson,Davie, 'Computer Network',2007,Fourth Edition, Morgan Kaufmann Publishers.
5. Forouzan, 'Data communication and networking forouzan', Fourth Edition, McGraw-Hill.

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 1, March 2013

Mr. Ajit D Kotkar is pursuing his BE in Information Technology, RMCET, Mumbai University. He is a member of ISTE. His area of interest is networking and Security.

Mr. Alok T Nalawade is pursuing his BE in Information Technology, RMCET, Mumbai University. He is a member of ISTE. His area of interest is networking.

Mr. Siddhesh G. Gawas is pursuing his BE in Information Technology, RMCET, Mumbai University. He is a member of ISTE. His area of interest is networking.

Mr. Aniket A. Patawardhan is pursuing his BE in Information Technology, RMCET, Mumbai University. He is a member of ISTE. His area of interest is networking and Security.