KEY ELEMENTS

OF

COMPUTER NETWORK

Authors:

Mr. Chetan N. Rathod [M.C.A., M.Phil.]

VIVEKANAND COLLEGE FOR ADVANCED COMPUTER & INFORMATION SCIENCE, SURAT

Mr. Sagar V.Fegade [M.C.A.]

M.L.PARMAR COLLEGE OF COMPUTER SCIENCE & I.T, SURAT

Ms. Bhumika K. Charnanand [M.C.A., M.Phil.]

PRABHU B.C.A. COLLEGE, UMRA, SURAT

Unit - 5

Network Security: Introductory concept and terminology

5.1 Various Types of Securities

Threat

- Anything that prevents users from accessing the required resources for performing their task is known as threat.
- Threat not includes only hacking of the server but it also include bad configuration.
- Threats can be classified into two groups.
  - **A.** internal treat
  - **B.** External treat

A . Internal threat

- Internal threat is long practice done by user in network resulting in inefficient Working of the network.
- The common internal threats are unauthorized access data destruction, administrative access, and system crash or hardware failure.

i. Unauthorized Access

- When the users access the network resources where he is not granted access, it is known unauthorized access.
- It may not cause any harm to the data but the user should not access those data.
- For example, the user is reading employee personal file.

ii. Data destruction

- Data destruction can be erasing or corrupting data accidentally.
- Users are authorized to access certain data but they are not authorized to make any changes to that data.
- For example, an employee has access product database where we can change only the product deception.
- These types of threat are dangerous because users are not informing about extent to which they can modify the data.

iii. Administrative Access

- The network operating systems come with various administrative tools and functionality. By giving administrative or root access to a user, can create problem.
- For example, giving right to a user to detect and add files in an important folder therefore, it is necessary to protect administrative function and programs from access and misuse by users.

iv. System crash or hardware failure

- The main cause of computer failure can be hard drive crash or power failure.

v. Virus

- The most efficient and fastest method of transferring computer virus among system is through the network.
- Most of the user focuses on the virus attacks from the internal, but the large number of virus enter the system to floppy disk, CD and USB.

❖ Protection from internal threat

- To protect network from internal threat administrator need to implement password, permissions, and polices on the user account.

1. Password

- A user account with a valid password would provide entry into a system, even if the user has limited permissions.
- If a user locks his password, the network administrator should set a new password and the user should be allowed to change if the next time he logs on.
- Biometric devices like finger prints used as replacement to password.

2. User Account Control

- Access to the user account should be restricted and he account should have a permission to access the necessary resources.

3. Polices

- It is essential or necessary to implement various polices to control user to access the resources or to prohibit them to do a certain task.
- For example, the administrator does not want the user to install software on their computer. This polices are generally applied a user account, a computer and depend upon the type ….work operating system is used.

4. Fault tolerance

- Fault tolerance is used to covering data if data is lost due to disk crash, RAID technology is used to fault tolerance.
- In RAID if the one of the hard disk crash, the data recover from the other hard disk.

B. External treat

- The external threat can exist into two forms:

  1. The attack can handled skillfully your user to gain access to the network; this process is known as social engineering.

  2. The hacker hack the remote location can use technical weakness of your network to gain access.

1. Social engineering

- The majority of the attack come under social engineering where the person manipulating the people within the organization to gain access to the network from outside.
- The people use other people to gain unauthorized information. The information can be a network login, credit card number or any other useful information that an organization may not want that an outside to know.

2. Hacking

- In hacking, the hacker gain access to the network by means of internet worms and other internet hacking tools.
- The main gain of hacker is to try a get area of public and private networks.
- The hackers basically fall into categories that is:
  - **I.** Inspector
  - **II.** Interceptor
  - **III.** Controller
  - **IV.** Flooder

i. Inspector

- The inspector is a hacker through just enter your serving system just like a normal user.
- The person looks for drawback in your internet access, permission, password and other method for gaining access to the network.
- The aims of this type of hacker are to look for a specific data.

ii. Interceptor

- The interceptor does not try to hack into the system. The type of hacker just monitors your network traffic looking to take interest for information.
- The interceptor often collects a password for later attack on the network.

iii. Controller

- Controller wants to control of the system. The most common aspect is taking control of the SMTP server and using it for spamming.

iv. Flooder

- Flooding attack is accomplishable over flow the network with too many requests so that its stops function.
- This type of attack is performing lost on website and mail server.

❖ **Protection from external threat**

1. Firewall

- Firewall is a system that backs all unwanted and unauthorized access of the system resources.
- It protects the private network from the people outside the network.

2. Encryption

- Encryption means the package unreadable. Encryption means that the sender transforms original information to another form and sends the resulting unimalligible message out over the network.

3. Physical protection

- It is essential to protect your server, so it is necessary to lock the server to prevent physical address by any authorized person.
- The network administrator should never leave logged in. we should log off the server or add a password protected screensaver when the server is not in use.

4. Public key

- Most strong encryption uses and a symmetric key methodology which uses two keys public key and private key.

5.2 Security with Certificates

- A security certificate is a small data file used as an Internet security technique through which the identity, authenticity and reliability of a website or Web application is established.
- A security certificate is used as a means to provide the security level of a website to general visitors, Internet service providers (ISPs) and Web servers.

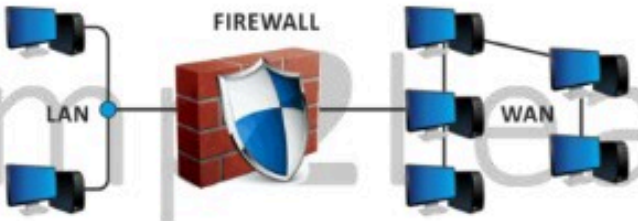
- A security certificate is also known as a digital certificate and as a Secure Socket Layer (SSL) certificate.
- A security certificate is allotted to a website or Web application by a third-party certification authority (CA).
- Typically, the CA evaluates the security framework of the website requesting the security certificate. Once the security, legitimacy and authenticity of the website are confirmed, a security certificate is provided.
- This security certificate is embedded within the website and is provided to Web servers, Web browsers, firewall and security applications, and ISPs when the website is requested.
- A security certificate is required to be updated on an annual basis or within a predefined time period.
- If a security certificate has expired, a user will see a notification in his browser stating that the security certificate is expired and the user is visiting the website at his own risk.

5.3 Firewalls

A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.

Accept : allow the traffic
Reject : block the traffic but reply with an "unreachable error"
Drop : block the traffic with no reply

A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.



5.1 FIREWALL

Before Firewalls, network security was performed by Access Control Lists (ACLs) residing on routers. ACLs are rules that determine whether network access should be granted or denied to specific IP address. But ACLs cannot determine the nature of the packet it is blocking. Also, ACL alone does not have the capacity to keep threats out of the network. Hence, the Firewall was introduced. Connectivity to the Internet is no longer optional for organizations. However, accessing the Internet provides benefits to the organization; it also enables the outside world to interact with the internal

network of the organization. This creates a threat to the organization. In order to secure the internal network from unauthorized traffic, we need a Firewall.

How Firewall Works?

Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic. For example, Rules are defined as any employee from HR department cannot access the data from code server and at the same time another rule is defined like system administrator can access the data from both HR and technical department. Rules can be defined on the firewall based on the necessity and security policies of the organization.

From the perspective of a server, network traffic can be either outgoing or incoming. Firewall maintains a distinct set of rules for both the cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass. Still, setting a rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication.

Incoming traffic is treated differently. Most traffic which reaches on the firewall is one of these three major Transport Layer protocols- TCP, UDP or ICMP. All these types have a source address and destination address. Also, TCP and UDP have port numbers. ICMP uses type code instead of port number which identifies purpose of that packet.

Default policy: It is very difficult to explicitly cover every possible rule on the firewall. For this reason, the firewall must always have a default policy. Default policy only consists of action (accept, reject or drop).

Suppose no rule is defined about SSH connection to the server on the firewall. So, it will follow the default policy. If default policy on the firewall is set to *accept*, then any computer outside of your office can establish an SSH connection to the server. Therefore, setting default policy as *drop* (or reject) is always a good practice.

Generation of Firewall

Firewalls can be categorized based on its generation.

1. First Generation- Packet Filtering Firewall :

Packet filtering firewall is used to control network access by monitoring outgoing and incoming packet and allowing them to pass or stop based on source and destination IP address, protocols and ports. It analyses traffic at the transport protocol.

Packet firewalls treat each packet in isolation. They have no ability to tell whether a packet is part of an existing stream of traffic. Only It can allow or deny the packets based on unique packet headers. Packet filtering firewall maintains a filtering table which decides whether the packet will be forwarded or discarded. From the given filtering table, the packets will be Filtered according to following rules:.

	SOURCE IP	DEST.IP	SOURCE PORT	DEST.PORT	ACTION
1	192.168.21.0	--	--	--	deny
2	--	--	--	23	deny
3	--	192.168.21.3	--	--	deny
4	--	192.168.21.0	--	>1023	allow

Sample Packet Filter Firewall Rule

1. Incoming packets from network 192.168.21.0 are blocked.
2. Incoming packets destined for internal TELNET server (port 23) are blocked.
3. Incoming packets destined for host 192.168.21.3 are blocked.
4. All well-known services to the network 192.168.21.0 are allowed.

2. Second Generation- Stateful Inspection Firewall :

Stateful firewalls (performs Stateful Packet Inspection) are able to determine the connection state of packet, unlike Packet filtering firewall, which makes it more efficient. It keeps track of the state of networks connection travelling across it, such as TCP streams. So the filtering decisions would not only be based on defined rules, but also on packet's history in the state table.

3. Third Generation- Application Layer Firewall :

Application layer firewall can inspect and filter the packets on any OSI layer, up to the application layer. It has the ability to block specific content, also recognize when certain application and protocols (like HTTP, FTP) are being misused.

In other words, Application layer firewalls are hosts that run proxy servers. A proxy firewall prevents the direct connection between either side of the firewall, each packet has to pass through the proxy. It can allow or block the traffic based on predefined rules.

Note: Application layer firewalls can also be used as Network Address Translator(NAT).

Next Generation Firewalls (NGFW) :

Next Generation Firewalls are being deployed these days to stop modern security breaches like advance malware attacks and application-layer attacks. NGFW consists of Deep Packet Inspection, Application Inspection, SSL/SSH inspection and many functionalities to protect the network from these modern threats.

Types of Firewall

Firewalls are generally of two types: Host-based and Network-based.

Host- based Firewalls :

Host-based firewall is installed on each network node which controls each incoming and outgoing packet. It is a software application or suite of applications, comes as a part of the operating system. Host-based firewalls are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from attacks and unauthorized access.

Network-based Firewalls:

Network firewall function on network level. In other words, these firewalls filter all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on the firewall. A Network firewall might have two or more network interface cards (NICs). A network-based firewall is usually a dedicated system with proprietary software installed both types of firewall have their own advantages.