ASSIGNMENT - 1
Network Programming(CSB 351)
Ayush Singh
171210017

Q1. How does firewall help to secure a PC ?

Ans. Firewall is used to monitor and control incoming and outgoing traffic based on predefined rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources in order to block malicious traffic like viruses and hackers. Firewalls guard traffic at a computer's entry point, called ports, which is where information is exchanged with external devices.

Firewall can be software(Host Based) or hardware(Network Based). It is recommended to have both. A software firewall is a program installed on each computer and regulates traffic through port numbers and applications, while a physical firewall is a piece of equipment installed between your network and gateway.

Types of FIREWALL :

Packet Filtering Firewall : Examine packets and prohibit them from passing through if they don't match an established security rule set. This type of firewall checks the packet's source and destination IP addresses. If packets match those of an "allowed" rule on the firewall, then it is trusted to enter the network. It works on network layer and transport layer.

Application (Proxy) Firewall : Works on network traffic at the application level. Unlike basic firewalls, the proxy acts as an intermediary between two end systems. The client must send a request to the firewall, where it is then evaluated against a set of security rules and then permitted or blocked. Most notably, proxy firewalls monitor traffic for layer 7 protocols such as HTTP and FTP, and use both stateful and deep packet inspection to detect malicious traffic.

Types of attack and prevention by FIREWALL:

IP address Spoofing:

In this kind of attack, an intruder from the outside tries to send a packet towards the internal corporate network with the source IP address set equal to one of the IP address of internal users.

Prevention:

Firewall can defeat this attack if it discards all the packets that arrive at the incoming side of the firewall, with source IP equal to one of the internal IPs.

Source Routing Attacks:

In this kind of attack, the attacker specifies the route to be taken by the packet with a hope to fool the firewall.

Prevention:

Firewall can defeat this attack if it discards all the packets that use the option of source routing aka path addressing.

Tiny Fragment Attacks:

Many times, the size of the IP packet is greater than the maximum size allowed by the underlying network such as Ethernet, Token Ring etc. In such cases, the packet

needs to be fragmented, so that it can be carried further. The attacker uses this characteristic of TCP/IP protocol. In this kind of attack, the attacker intentionally creates fragments of the original packet and send it to fool the firewall.

Prevention:
Firewall can defeat this attack if it discards all the packets which use the TCP protocol and is fragmented. *Dynamic Packet Filters* allow incoming TCP packets only if they are responses to the outgoing TCP packets.

Q2. Discuss steps or precautions you will take to secure a PC as a system admin.
Ans. Computer security includes measures taken to ensure the integrity of files stored on a computer or server as well as measures taken to prevent unauthorized access to stored data, by securing the physical perimeter of the computer equipment, authentication of users or computer accounts accessing the data, and providing a secure method of data transmission.
Steps taken to implement :

Access Control : The selective restriction of access to a place or other resource while access management describes the process. The act of *accessing* may mean consuming, entering, or using.

Physical Security : Protecting property and people from damage or harm (such as from theft, espionage, or terrorist attacks). It includes security measures designed to deny unauthorized access to facilities, (such as a computer room), equipment (such as your computer), and resources (like the data storage devices, and data, in your computer). If a computer gets stolen, then the data goes with it. In addition to theft, physical access to a computer allows for ongoing espionage, like the installment of a hardware keylogger device, and so on.

Data Security : Protecting data, such as a database, from destructive forces and the unwanted actions of unauthorized users.

Information Privacy : Relationship between collection and dissemination of data, technology, the public expectation of privacy , and the legal and political issues surrounding them. Privacy concerns exist wherever other sensitive information is collected and stored – in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues.

Network Security : Provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator.

Internet Privacy : Involves the right or mandate of personal privacy concerning the storing, repurposing, provision to third parties, and displaying of information pertaining to oneself via the Internet. Privacy can entail either Personally Identifying Information (PII) or non-PII information such as a site visitor's behavior on a website. PII refers to any information that can be used to identify an individual. For example, age and physical address alone could identify who an individual is without explicitly disclosing their name, as these two factors relate to a specific person.

Location Access : Access is provided only on the basis of location.

World Wide Web Security : Dealing with the vulnerabilities of users who visit websites. Cybercrime on the Web can include identity theft, fraud, espionage and intelligence gathering. For criminals, the Web has become the preferred way to spread malware.