Unit :2

Introduction to Intruders

Intruders are the attackers who attempt to breach the security of a network. They attack the network in order to get unauthorized access. Intruders are of three types, namely, masquerader, misfeasor and clandestine user.

- **Masquerader – unauthorized user who penetrates a system exploiting a legitimate user's account *(outside)***
- **Misfeasor - legitimate user who makes unauthorized accesses or misuses his privileges *(inside)***
- **Clandestine user - seizes supervisory control to evade auditing and access controls or suppress audit collection *(inside|outside)***

Computer Intruders

Computer intrusions occur when someone tries to gain access to any part of your computer system. Computer intruders or hackers typically use automated computer programs when they try to compromise a computer's security. There are several ways an intruder can try to gain access to your computer. They can:

1. Access your computer to view, change, or delete information on your computer.
2. Crash or slow down your computer.
3. Access your private data by examining the files on your system.
4. Use your computer to access other computers on the Internet.

Intrusion Detection functions

An Intrusion Detection System (IDS) is an application to detect suspicious activity on network traffic. Also known as an Intrusion Prevention System, it is widely used to identify suspicious or unknown malware activities on a protected asset. It is not impossible for hackers to penetrate networks; therefore, intrusion detection system importance is paramount here. Traditional enterprise systems and organizations can benefit from IDS to improve their security controls and protect their network environment.

Functions of an Intrusion Detection System

IDS serves three main functions: detecting anomalies, reporting potential threats, and blocking traffic using two methods – Signature-based detection and Anomaly-based detection.

1. Signature-based IDS

With the rise in cyberattacks, it is wise to safeguard your personal or business network from malware, viruses, Trojans, etc. Signature-based detection is a popular technique to detect and identify suspicious software or malware attacks in your system.

2. Anomaly or Behavior-based IDS

Anomaly-based IDS is more effective than signature-based detection systems. Unlike signature-based, the anomaly-based detection system can monitor and analyze significant network traffic and data to detect anomalies. It does not rely on known signature attacks to identify potential threats but looks for behaviors that could be a threat or attack.

Malicious Software

Viruses, worms, Trojan horses and related computer threats are commonly confused with each other because they often cause similar damage. Viruses have been around longer than the others, and consequently the term “virus” is commonly but inaccurately used to refer to all of them. Here are some

characteristics:

Virus

A virus is a relatively small file that can copy itself into another file or program (its host). It can be transmitted only if its host file or program is transmitted. Some viruses are designed to change themselves slightly in order to make their detection and removal more difficult.

Trojan horse

A Trojan horse is a program that appears to be useful or entertaining, but it carries a hidden malicious function that is activated when the program is run. Some Trojan horses even masquerade as repair tools, claiming to remove threats from your computer but actually doing the opposite.

Worm

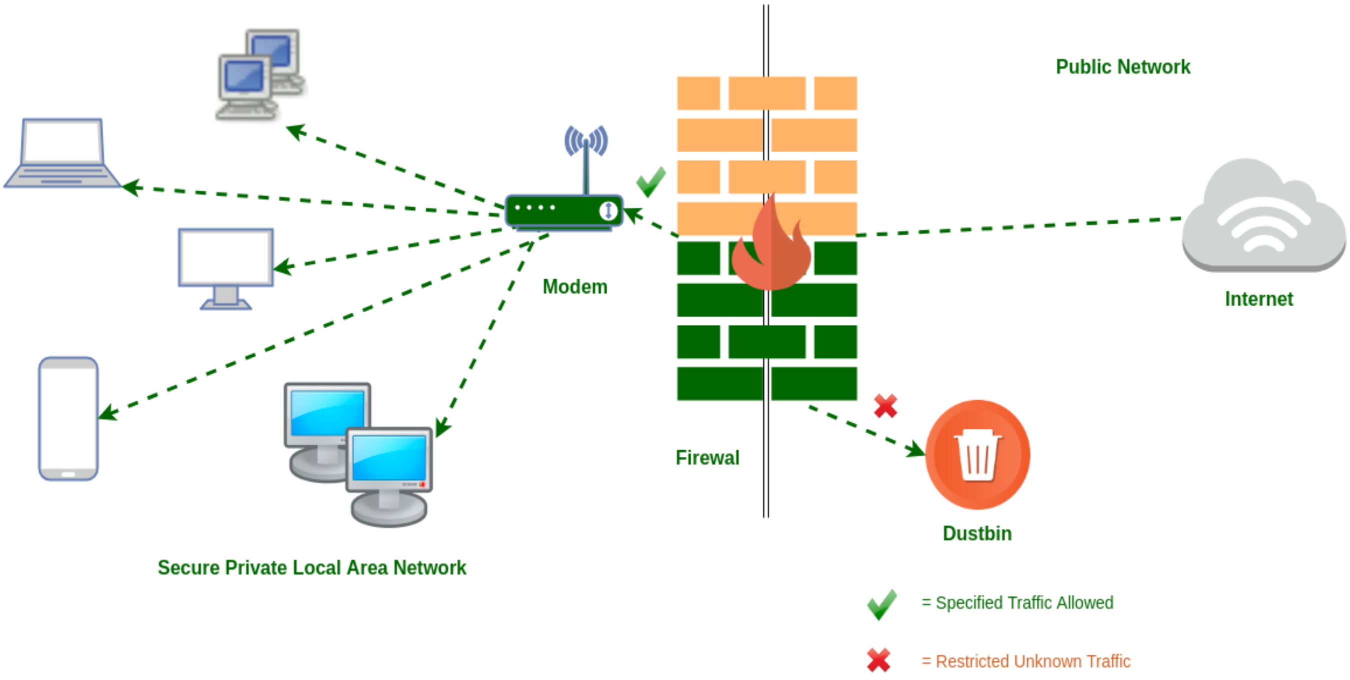
A worm is a program that can both copy and transmit itself. This type of threat is now more common and often more disruptive than many viruses.

Malicious script

These vary in the harm they can cause, and they can get into your computer or compromise your personal information by a number of means; e.g., when you click on a link inside an specially designed

Firewall

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.


Public Network
Modem
Internet
Firewal
Dustbin
Secure Private Local Area Network
✓ = Specified Traffic Allowed
✗ = Restricted Unknown Traffic

Characteristics of Firewall

1. **Physical Barrier:** A firewall does not allow any external traffic to enter a system or a network without its allowance. A firewall creates a choke point for all the external data trying to enter into the system or network and hence can easily block the access if needed.
2. **Multi-Purpose:** A firewall has many functions other than security purposes. It configures domain names and Internet Protocol (IP) addresses. It also
acts as a network address translator. It can act as a meter for internet usage.
3. **Flexible Security Policies:** Different local systems or networks need different security policies. A firewall can be modified according to the requirement of the user by changing its security policies.
4. **Security Platform:** It provides a platform from which any alert to the issue related to security or fixing issues can be accessed. All the queries related to security can be kept under check from one place in a system or network.

5. **Access Handler:** Determines which traffic needs to flow first according to priority or can change for a particular network or system. specific action requests may be initiated and allowed to flow through the firewall.

Limitations of Firewall

When it comes to network security, firewalls are considered the first line of defense. But the question is whether these firewalls are strong enough to make our devices safe from cyber-attacks.

The importance of using firewalls as a security system is obvious; however, firewalls have some limitations:

- Firewalls cannot stop users from accessing malicious websites, making it vulnerable to internal threats or attacks.
- Firewalls cannot protect against the transfer of virus-infected files or software.
- Firewalls cannot prevent misuse of passwords.
- Firewalls cannot protect if security rules are misconfigured.
- Firewalls cannot protect against non-technical security risks, such as social engineering.

- Firewalls cannot stop or prevent attackers with modems from dialing in to or out of the internal network.
- Firewalls cannot secure the system which is already infected.

Types of firewall

1. packet filtering firewall
2. circuit-level gateway
3. application-level gateway (aka proxy firewall)
4. stateful inspection firewall

1. Packet filtering firewall

Packet filtering firewalls operate inline at junction points where devices such as routers and switches do their work. However, these firewalls don't route packets; rather they compare each packet received to a set of established criteria, such as the allowed IP addresses, packet type, port number and other aspects of the packet protocol headers. Packets that are flagged as troublesome are, generally speaking, unceremoniously dropped -- that is, they are not forwarded and, thus, cease to exist.

Packet filtering firewall advantages

- A single device can filter traffic for the entire network
- Extremely fast and efficient in scanning traffic
- Inexpensive

Packet filtering firewall disadvantages

- Doesn't check the payload and can be easily spoofed
- Not an ideal option for every network
- Access control lists can be difficult to set up and manage

2. Circuit-level gateway

Using another relatively quick way to identify malicious content, circuit-level gateways monitor TCP handshakes and other network protocol session initiation messages across the network as they are established between the local and remote hosts to determine whether the session being initiated is legitimate -- whether the remote system is considered trusted. They don't inspect the packets themselves, however.

Circuit-level gateway advantages

- Only processes requested transactions; all other traffic is rejected
- Easy to set up and manage
- Low cost and minimal impact on end-user experience

Circuit-level gateway disadvantages

- No application layer monitoring
- Requires ongoing updates to keep rules current

3. Application-level gateway

This kind of device -- technically a proxy and sometimes referred to as a *proxy firewall* -- functions as the only entry point to and exit point from the network. Application-level gateways filter packets not only according to the service for which they are intended -- as specified by the destination port .

Application-level gateway advantages

- Provides fine-grained security controls that can, for example, allow access to a website but restrict which pages on that site the user can open
- Protects user anonymity

Application-level gateway disadvantages

- Can inhibit network performance
- Costlier than some other firewall options
- Doesn't work with all network protocols

4. Stateful inspection firewall

State-aware devices not only examine each packet, but also keep track of whether or not that packet is part of an established TCP or other network session. This offers more security than either packet filtering or circuit monitoring alone but exacts a greater toll on network performance.

Stateful inspection firewall advantages

- Does not need to open numerous ports to allow traffic in or out
- Delivers substantive logging capabilities

Stateful inspection firewall disadvantages

- Resource-intensive and interferes with the speed of network communications
- More expensive than other firewall options