UNIT-4

• INTRUDERS

Unauthorized intrusion into a computer system / network is one of the most serious threats to computer security. Three classes of intruders are:

1. **Masquerader**

   An user who is not authorized to use the computer and who penetrates a systems access controls to exploit the system.

2. **Misfeasor**

   A legitimate user who accesses data, programs or resources for which such access is not authorized or who is authorized for such access but misuse his/her privelages.

3. **Clandestine User**

   An individual who siezes supervisory control of the system and uses this control to access others controls.

The objective of the intruder is to gain access to a system or to increase the range of priveleges accessible on a system. Intruders acquires information that should have been protected.

• INTRUSION DETECTION

Intrusion detection is based on the assumption that the behaviour of the intruder differs from that of a legitimate user in ways that can be quantified.

Approaches to Intrusion Detection

1. **Statistical anomaly detection**: It involves collection of data related to behaviour of legitimate users over a period of time. Statistical tests are applied to observe behaviour of users to find out illegitimate users.

2. **Rule Based Detection**: Defines a set of rules that can be used to decide that a given behaviour is that of an intruder. Rules are developed to detect deviation from previous usage patterns.

• INTRUSION DETECTION SYSTEM

An Intrusion detection system monitors network traffic and monitors for suspicious activities and alerts the system or network administrator. Its main function are to identify malicious activity, log information about this activity, ~~attempt to block / stop~~ it and report it.

1. **Network Intrusion Detection System** (NIDS)

NIDS are placed at a strategic points within the network to monitor traffic to and from all devices on the network. It would scan all the inbound and outbound traffic.

2. **Host Intrusion Detection System** (HIDS)

HIDS run on individual hosts or devices on the network. It monitors the inbound and outbound packets from the device only and will alert the user / administrator if suspicious activity is detected.

It takes snapshot of the existing system file and matches it to previous snapshot. If modified, an alert is sent to administrator

3. **Signature Based**

A signature Based IDS will monitor packets on the network and compare them against a database of signatures or attributes from known malicious threats.

Passive IDS — simply detects and alerts the administrator.
It is upto administrator to take action to block the activity.

Reactive IDS — It will not only detect suspicious activity and alert the administrator but will take pre-defined actions to respond to threat.

- **HONEYPOTS**

Honeypots are decoy systems that are designed to lure a potential attacker away from critical systems. These are designed to:

1. Divert an attacker from accessing critical systems.
2. Collect information about the attacker's activity.
3. Encourage the attacker to stay on system long enough for administrators to respond.

These systems are fabricated with information that appear valuable but a legitimate user of the system wouldn't access. Thus any access to the honeypot is a suspect.
The system is aided with sensitive monitors and event loggers that detect these accesses and collect information about the attacker's activity.
Administrators have time to log and track the attacker without exposing productive systems.

- **INTRUSION PREVENTION SYSTEM (IPS).**

Intrusion prevention systems (IPS) also known as intrusion detection and prevention systems (IDPS), are network security / threat prevention technology that monitors network traffic and system activities for malicious activities.
The main function of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block / stop it and report it.

IPS are considered as extensions of intrusion detection systems because they both monitor traffic / system for malicious activities.
The main differences are, unlike IDS, IPS are placed in-line and are able to actively prevent / block intrusions that are detected.

IPS often sits behind the firewall and provides complementary layer of security. IPS can take actions such as

1. Sending an alarm to adminstrator
2. Dropping malicious packets
3. Blocking traffic from the source address
4. Resetting the connection

Types of IPS are:

1. Network Based Intrusion Prevention Systems (NIPS)

It monitors the entire network for suspicious traffic by analyzing protocol activity.

2. Wireless Intrusion Prevention Systems (WIPS)

It monitors a wireless network for suspicious traffic by analyzing wireless networking protocol.

3. Network Behaviour Analysis (NBA).

It examines network traffic to identify threats that generate unusual traffic flows, such as DDos attacks, certain forms of malware and policy variations.

4. Host Based Intrusion Prevention Systems (HIPS).

It is an installed software package that ~~generate~~ monitors a single host for suspicious activity by analyzing events occuring within the host.

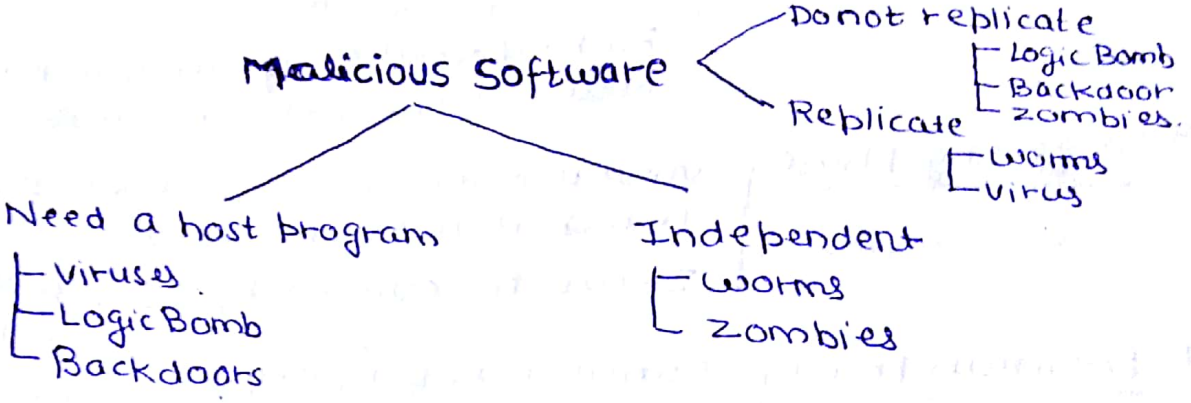
Dection Methods

1. Signature Based
2. Statistical anomaly-based detection
3. Stateful protocal analysis detection

- MALICIOUS SOFTWARE is a software that is intentionally included or inserted in a system for a harmful purpose.

- VIRUS is a piece of software that can 'infect' other programs by modifying them; the modification includes a copy of virus program which can then go on and infect other programs.
  (attach itself to another program & executes secretly when host runs)

- WORM is a program that can replicate itself and send copies from computer to computer across network connections. The worm may be activated to replicate & propgate again. In addition to propgation, they perform some unwanted function.



- BACKDOOR is a secret entry point into a program that allows someone to gain access without going through usual ~~attivit~~ security access procedures.
  Programmers have used backdoors legitimately to debug & test programs.

- LOGIC BOMB is the code embedded in some legitimate program that is set to 'explodes' when certain coditions are met. (e.g a particular day of week, partiular application running)
  Once triggered, bomb may alter or delete data or files, cause a machine halt or do some other damage.

- ZOMBIE is a program that secretly takes over another Internet attached computer and then uses the computer to launch attacks that are difficult to trace to the zombie's creator.
  These are used in DOS attacks. The zombies are planted on hundred of computers and then used to attack the targeted web site.

- TORZON HORSES is an apparently useful program that contains hidden code that when invoked performs some unwanted or harmful function.

They can be used to accomplish functions indirectly that an unauthorized user could not accomplish directly

- LIFECYCLE OF VIRUS

1. Dormant Phase
   - The virus is idle.
   - It will eventually be activated by some event.
   - Not all viruses have this stage.
2. Propgation Phase
   - Virus places identical copy of itself into other programs
   - Each infected program will now contain clone of the virus, which itself will propgate
3. Triggering Phase
   - Virus is activated to perform function for which it was intended.
   - It can be caused by variety of events.
4. Execution Phase
   - Function is performed.
   - Function may be harmless, such as message on the screen or damaging such as destruction of data files.

- TYPES OF VIRUSES

1. Parasitic Virus : It attach itself to executable files and replicates
2. Memory-resident : Lodges in main memory as a part of resident System program. Infects every program that executes.
3. Boot sector : Infects master boot record and spreads when a system is booted from the disk containing virus.
4. Stealth : A form of virus that is designed to hide itself from detection by antivirus software.
5. Polymorphic : creates a copies during replication that are functionally equivalent but have different bit patterns.
6. Metamorphic : It rewrites itself completly at each iteration making it diffuet to detect.

• VIRUS STRUCTURE

1. A virus can be prepended / postpended to an executable program, or can be embedded in some other fashion.
2. Key to operation - when infected program is invoked, it will first execute the virus code and then executes original code of program.

In infected program begins with virus code & work as follow:

1. 1st line of code is a jump to main virus program.
2. 2nd line is a special marker that is used by virus to determine whether the program is already infected or not.
3. When program is invoked → control transfers to main virus program, which first seeks uninfected executable file and infects them
4. Next, virus may perform some damaging action.
5. Finally the virus transfers control to the original program.

The user is unlikely to notice any difference between the execution of infected and uninfected program.

```
Program V
{ gotomain; // transfers control
              to virus program
  1234567;
subroutine infect-executable.
 {
   }
subroutine do-damage.
 {
   }
main.
{ infect-executable;
  do-damage;
  gotonext;
 }
}
```

• VIRUS COUNTERMEASURES

1. Detection - once the infection has occurred, determine that it has occurred and locate the virus
2. Identification - Identify the specific virus that has infected the program.
3. Removal - Remove all traces of the virus from the infected program and restore it to its orginal state. Remove the virus from all infected systems so that the disease cannot spread further.

If removal is not possible, then discard the infected program and reload a clean backup version.

Four generations of Antivirus

1. 1st Generation - simple scanner requires virus signature to identify virus. These are limited to detection of known viruses.
2. 2nd Generation - uses heuristic scanner which uses heuristic rules to search for virus infection. They look for fragments of code that are often associated with viruses.

   Integrity checking - a checksum can be appended to each program.
3. 3rd Generation - memory resident programs that identify a virus by its action rather than its structure in an infected program. A small set of ~~Gest~~ actions that indicate an infection needs to be identified.
4. 4th Generation : are packages consisting of variety of antivirus techniques used in conjunction. Includes scanning and activity trap components. Includes access control capability which limits the ability of viruses to penetrate a system & then limits the ability of a virus to update files to pass an infection.

• FIREWALL

A firewall forms a barrier through which the traffic going in each direction must pass.

It is designed to operate as a filter at the level of IP packets or may operate at higher layer protocol

A Firewall security policy dictates which traffic is authorized to pass ~~or fr~~ in each direction.

• Firewall Characteristics

1. All traffic from inside to outside and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network expect via the firewall.
2. Only authorized traffic, as defined by security policy will be allowed to pass.
3. The firewall itself is immune to penetration. This implies that use of trusted system with a secure operating system.

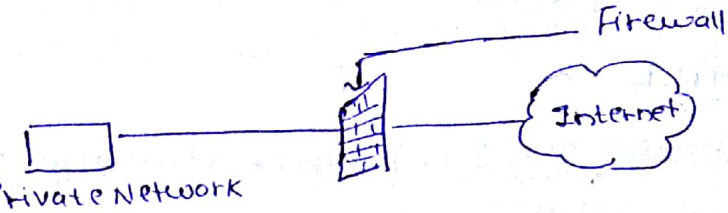
• Techniques Used By Firewalls

1. Service control - Determines the type of Internet services that can be accessed. Firewall filters traffic on basis of IP address and TCP port no. (may provide proxy software).
2. Direction control - Determines the direction in which particular service requests may be initiated and allowed to flow through the firewall.
3. User control - controls access to a service according to which the user is attempting to access it.
4. Behaviour control - controls how particular services are used. e.g Firewall may filter e-mail to eliminate spam.

• LIMITATIONS OF FIREWALLS

1. cannot protect against attacks that bypass the firewall.
2. Does not protect against internal threats (disgruntled employee).
3. cannot protect against the transfer of virus-infected programs. impossible for firewall to scan all incoming files, emails for viruses

• TYPES OF FIREWALLS



(1) PACKET-FILTERING

A packet filtering router applies set of rules to each incoming and outgoing IP packet and the forwards or discards the packet

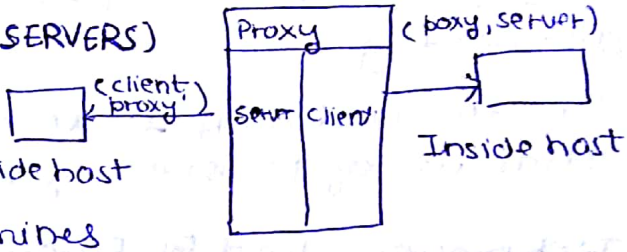
It allows or block packets based on criteria such as source or destination IP addresses, protocol, source or destination port no and various other parameters within IP header. Packet filter rule:

Selection Criteria: condition & pattern matching for decision making

Action Field: Specifies action to be taken if IP packet meets the criteria. (Block/Allow)

It works well for small networks but when applied to larger network can become very complex and difficult to configure.

(2) APPLICATION-LEVEL GATEWAY (PROXY SERVERS)



It deals with network traffic by passing all packets through a separate 'proxy' application that examines data at an application level.

A proxy firewall doesn't allow direct connection b/w a trusted server or client and an untrusted host.

They intercept incoming and outgoing packets, run proxies that copy and forward information across gateway. Proxies examines and filters individual packets before forwarding them.

(3) CIRCUIT-LEVEL GATEWAY

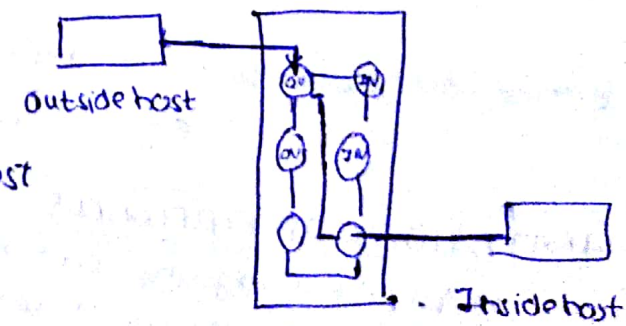
It is an intermediate solution b/w packet filter & application gateway.

It runs at transport layer and hence can act as proxy for applications.

It does not permit end-to-end TCP connection across ~~net~~ gateway. It sets up two TCP connections ~~and relays~~

- one b/w itself and TCP user on inner host
- b/w itself and TCP user on outer host

Then, it relays TCP segments from one network to the other without examining contents.



- **TRUSTED SERVICES**

A trusted system is a computer and operating system that can be verified to implement a given security policy

The focus of trusted system is access control. A policy is implemented that dictates what objects may be accessed by what subjects