# OS Assignment – 5

1. Explain various Program Threats and System Threats.
2. Describe various security classifications in computer systems.
3. Explain components of Linux operating system with a suitable diagram.
4. Write important features of Linux Operating System.
5. Explain Architecture of Linux Operating system with suitable diagram.

## Q1

#### Program Threats

An Operating system's processes and kernel perform their designated tasks as instructed. If a program makes these processes perform malicious tasks, then it is known as a Program Threat. Some well-known program threats are as follows:

* Trojan Horse − Such programs traps user login credentials and sends them to a malicious user who can later on login to computer and can access system resources.
* Trap Door − If a program performs an illegal action without knowledge of user then it is said to have a trap door.
* Logic Bomb − Logic bomb is a situation when a program misbehaves only when certain conditions are met otherwise it works as a genuine program. It is harder to detect.
* Virus − A virus is generally a small code embedded in a program that can replicate itself on a computer system. They are highly dangerous and can modify/delete user files and crash systems.

#### System Threats

System threats refers to the misuse of system services and network connections to put user in trouble. System threats can be used to launch program threats on a network. Some well-known system threats are as follows:

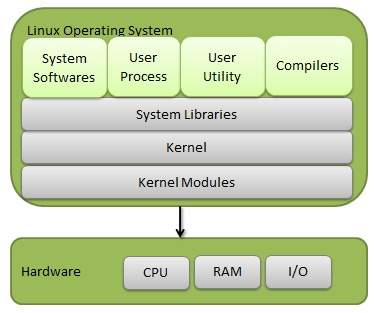
* Worm − Worm is a process which can choke down a system’s performance by using system resources to extreme levels. A Worm process generates its multiple copies where each copy uses system resources, preventing other processes to acquire the resources they require.
* Port Scanning − Port scanning is a mechanism or means by which a hacker detects system vulnerabilities to make an attack on the system.
* Denial of service (DoS) – These attacks prevents user to legitimately use their system. For example, a user may not be able to access the internet if a denial of service attack occurs on the browser's content settings.

## Q2

1. Type A
   * Highest Level.
   * Uses formal design specifications and verification techniques.
   * Grants a high degree of assurance of process security.
2. Type B
   * Provides a mandatory protection system.
   * Has all the properties of a class C2 system.
   * Attaches a sensitivity label to each object.
   * It is of three types:
     + B1 − Maintains the security label of each object in the system. Label is used for making decisions to access control.
     + B2 − Extends the sensitivity labels to each system resource, such as storage objects, supports covert channels and auditing of events.
     + B3 − Allows creating lists or user groups for access-control to grant access or revoke access to a given named object.
3. Type C
   * Provides protection and user accountability using audit capabilities.
   * It is of two types:
     + C1 − Incorporates controls so that users can protect their private information and keep other users from accidentally reading/deleting their data. UNIX versions are mostly C1 class.
     + C2 − Adds an individual-level access control to the capabilities of a C1 level system.
4. Type D
   * Lowest level.
   * Provides minimum protection.
   * MS-DOS, Window 3.1 fall in this category.

## Q3

Linux is one of the most popular versions of UNIX. It is open source as its source code is publicly available and it is free to use. Linux was designed considering UNIX compatibility. Its functionality is quite similar to that of UNIX. The Linux Operating System primarily has three components



* Kernel − Kernel is the core part of Linux. It is responsible for all major activities of this operating system. It consists of various modules and it interacts directly with the underlying hardware. Kernel provides the required abstraction to hide low-level hardware details to system or application programs.
* System Library − System libraries are special functions or programs using which application programs or system utilities accesses Kernel's features. These libraries implement most of the functionalities of the operating system and do not requires kernel module's code access rights.
* System Utility − System Utility programs are responsible to do specialized, individual level tasks.

## Q4

Following are some of the important features of Linux Operating System.

1. Portability – It means that the software works on different types of hardware in the same way. Linux kernel and application programs supports their installation on any kind of hardware platform.
2. Open Source − Linux source code is freely available and it is community based development project. Multiple teams work in collaboration to enhance the capabilities of Linux and ensure its continuous evolution.
3. Multi-User – On Linux, multiple users can access the system and use its resources such as Memory/CPU/Application programs at the same time.
4. Multiprogramming − Linux is a multiprogramming system therefore multiple applications can run at the same time.
5. Hierarchical File System − Linux provides a standard file system in which files are arranged hierarchically.
6. Shell − Linux provides a special interpreter program which can be used to execute commands of the operating system. It can be used to perform various operations, call application programs. etc.
7. Security − Linux provides user security using authentication features like password protection, controlled access to specific files and encryption of data.

## Q5

The architecture of a Linux System consists of the following layers −

* Hardware layer − Hardware consists of internal components such as RAM, HDD, CPU etc. and devices such as input/output devices.
* Kernel − It interacts directly with hardware and provides low-level services to upper layer components.
* Shell − An interface to the kernel, hiding the complexity of kernel's functions from users. The shell takes commands from the user and executes kernel's functions.
* Utilities − Utility programs that provides the user most of the functionalities of the operating system.

