# OS Assignment – 5

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

# Q1

## Program Threats

Operating system's processes and kernel do the designated task as instructed. If a user program made these process do malicious tasks, then it is known as Program Threats. One of the common example of program threat is a program installed in a computer which can store and send user credentials via network to some hacker. Following is the list of some well-known program threats.

- Trojan Horse − Such program traps user login credentials and stores them to send to malicious user who can later on login to computer and can access system resources.
- Trap Door − If a program which is designed to work as required, have a security hole in its code and perform illegal action without knowledge of user then it is called to have a trap door.
- Logic Bomb − Logic bomb is a situation when a program misbehaves only when certain conditions met otherwise it works as a genuine program. It is harder to detect.

Virus − Virus as name suggest can replicate themselves on computer system. They are highly dangerous and can modify/delete user files, crash systems. A virus is generally a small code embedded in a program. As user accesses the program, the virus starts being embedded in other files/ programs and can make system unusable for user.

## System Threats

System threats refers to misuse of system services and network connections to put user in trouble. System threats can be used to launch program threats on a complete network called as program attack. System threats creates such an environment that operating system resources/ user files are misused. Following is the list of some well-known system threats.

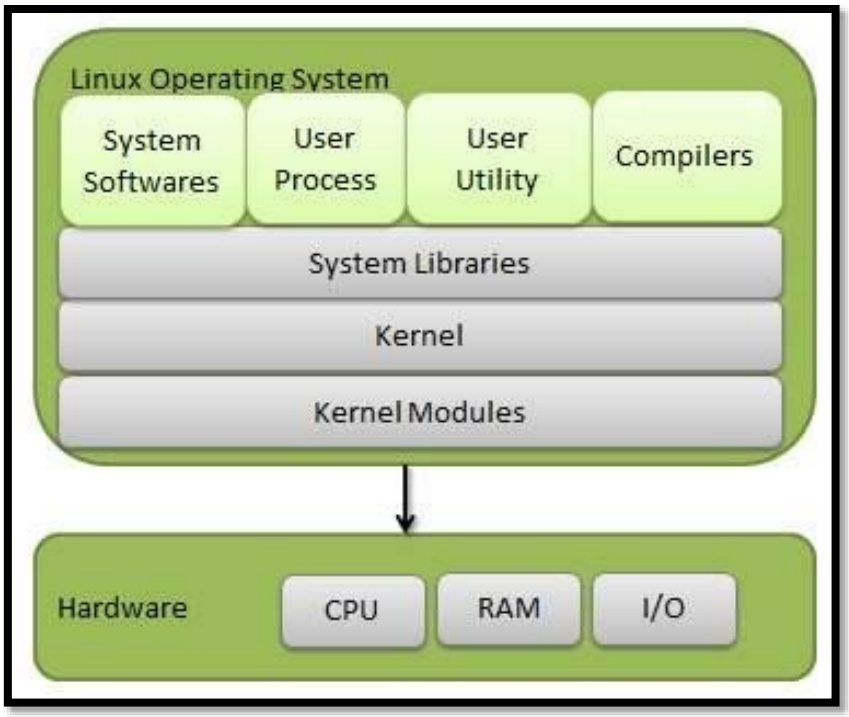
- Worm − Worm is a process which can choked down a system performance by using system resources to extreme levels. A Worm process generates its multiple copies where each copy uses system resources, prevents all other processes to get required resources. Worms' processes can even shut down an entire network.
- Port Scanning − Port scanning is a mechanism or means by which a hacker can detects system vulnerabilities to make an attack on the system.
- Denial of Service − Denial of service attacks normally prevents user to make legitimate use of the system. For example, a user may not be able to use internet if denial of service attacks browser's content settings.

# Q2

| S.N. | Classification Type & Description |
|---|---|
| 1 | Type A<br>Highest Level. Uses formal design specifications and verification techniques. Grants a high degree of assurance of process security. |
| 2 | Type B<br>Provides mandatory protection system. Have all the properties of a class C2 system. Attaches a sensitivity label to each object. It is of three types.<br>• B1 – Maintains the security label of each object in the system. Label is used for making decisions to access control.<br>• B2 – Extends the sensitivity labels to each system resource, such as storage objects, supports covert channels and auditing of events.<br>• B3 – Allows creating lists or user groups for access-control to grant access or revoke access to a given named object. |
| 3 | Type C<br>Provides protection and user accountability using audit capabilities. It is of two types.<br>• 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 Cl class.<br>• C2 – Adds an individual-level access control to the capabilities of a Cl level system. |
| 4 | Type D<br>Lowest level. Minimum protection. MS-DOS, Window 3.1 fall in this category. |

# Q3

Linux is one of popular version of UNIX operating System. It is open source as its source code is freely available. It is free to use. Linux was designed considering UNIX compatibility. Its functionality list is quite similar to that of UNIX. The Linux Operating System has primarily 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

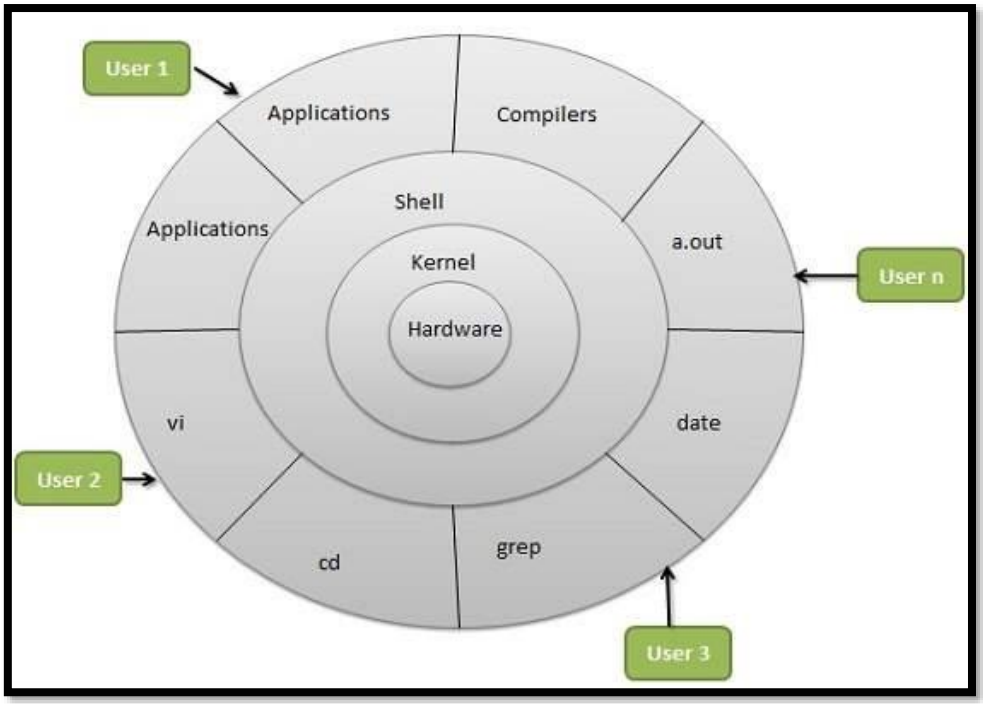
Following are some of the important features of Linux Operating System.

1. Portable – Portability means software can works on different types of hardware in 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 capability of Linux operating system and it is continuously evolving.
3. Multi-User – Linux is a multiuser system means multiple users can access system resources like memory/ ram/ application programs at same time.
4. Multiprogramming – Linux is a multiprogramming system means multiple applications can run at same time.
5. Hierarchical File System – Linux provides a standard file structure in which system files/ user files are arranged.
6. Shell – Linux provides a special interpreter program which can be used to execute commands of the operating system. It can be used to do various types of operations, call application programs. etc.
7. Security – Linux provides user security using authentication features like password protection/ controlled access to specific files/ encryption of data.

# Q5

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

- Hardware layer – Hardware consists of all peripheral devices (RAM/ HDD/ CPU etc.).
- Kernel – It is the core component of Operating System, interacts directly with hardware, provides low level services to upper layer components.
- Shell – An interface to kernel, hiding complexity of kernel's functions from users. The shell takes commands from the user and executes kernel's functions.
- Utilities – Utility programs that provide the user most of the functionalities of an operating systems.


User 1
Applications
Compilers
Applications
Shell
Kernel
Hardware
a.out
User n
vi
date
User 2
cd
grep
User 3