INTRODUCTION:

In today's world of international networks, every computer system is a potential target. Computers have been turned into attack platforms for launching massive denial of service attacks, credit-card numbers have been plundered from databases and then used for fraud or extortion, hospital medical records have been accessed by children who then used the information to play malicious practical jokes on former patients, business records have been surreptitiously altered, software has been replaced with secret 'back doors' in place, and millions of passwords have been captured from unsuspecting users. There are also reports of organized crime, agents of hostile nation states, and terrorists all gaining access to government and private computer systems, using those systems for nefarious purposes.

All attacks on computer systems are potentially damaging and costly. Even if nothing is removed or altered, system administrators must often spend hours or days analyzing the penetration and possibly reloading or reconfiguring a compromised system to regain some level of confidence in the system's integrity. As there is no way to know the motives of an intruder, and the worst must always be assumed.

Despite the risks, having an Internet presence has become all of the World. Why? For many years, Unix ran the Internet; the majority of web servers on the Internet are still Unix-based. Unix systems likewise make great firewalls, mail servers, domain name servers, and more. What's more, we can even download and install a fully functional, up-to-date free Unix system with only a floppy disk and a high-speed Internet connection.

Every day, the number of Internet-connected computers increases. Most of today's systems runs on embedded Unix operating system. And all of these systems demand protection so that they can be run securely.

WHAT IS COMPUTER SECURITY?

A computer is secure if we can depend on it and its software to behave as we expect. If we expect the data entered into our machine today to be there in a few weeks, and to remain unread by anyone who is not supposed to read it, then the machine is secure.

Years ago, Unix was generally regarded as an operating system that was difficult to secure. This is no longer the case. Today, Unix is widely regarded as the most secure operating system that is generally available. But despite the increasing awareness and the improvements in defenses, the typical Unix system is still exposed to many dangers.

UNIX SECURITY:

> ***"It was not designed from the start to be secure. It was designed with the necessary characteristics to make security serviceable - Dennis Ritchie"***

Unix is a multiuser, multitasking operating system.
Multiuser means that the operating system allows many different people to use the same computer at the same time.
Multitasking means that each user can run many different programs simultaneously.
One of the natural functions of such operating systems is to prevent different people or programs using the same computer from interfering with each other. Without such protection, a wayward program could affect other programs or other users, could accidentally delete files, or could even crash / halt the entire computer system. To keep such disasters from happening, some form of computer security has always had a place in the Unix design philosophy.
But Unix security provides more than mere memory protection. Unix has a sophisticated security system that controls the ways users access files, modify system databases, and use system resources. Unfortunately, those mechanisms don't help much when the systems are misconfigured, are used carelessly, or contain buggy software. Nearly all of the security holes that have been found in Unix over the years have resulted from these kinds of problems rather than from shortcomings in the intrinsic design of the system. Thus, nearly all Unix vendors believe that they can (and perhaps do) provide a reasonably secure Unix operating system. We believe that Unix systems can be fundamentally more secure than other common operating systems. However, there are influences that work against better security in the Unix environment.

The Aims of System Security:

In general, secure computing systems must guarantee the confidentiality, integrity, and availability of resources. This is achieved through a combination of different security mechanisms and safeguards, including policy-driven access control and process separation.

Authentication:

When a user is granted access to resources on a computing system, it is of vital importance to establish and verify the identity of the requesting entity. This process is commonly referred to as authentication.

Authorization:

As a multiuser system, Unix must protect resources from unauthorized access. To protect user data from other users and nonusers, the operating system has to put up safeguards against unauthorized access.

Availability:

Guarding a system (including all its subsystems, such as the network) against security breaches is vital to keep the system available for its intended use. Any system that has only the core operating system running but not the services that are supposed to run on the system is considered not available.

Integrity:

Ensuring that the Unix system is running in the intended way is most crucial, especially since the system might otherwise be used by a third party for malicious uses, such as a relay or member in a botnet.

Confidentiality:

Protecting resources from unauthorized access and safeguarding the content is referred to as confidentiality. As long as it is not compromised, a Unix system will maintain the confidentiality of system user data by enforcing access control policies and separating processes from each other.

Security Building Blocks:

Unix user accounts and password systems:

Everyperson who uses a Unix computer should have her ownaccount. An account is identified by auserID number (UID) that is associated with one or more usernames. Traditionally, each account also has a secret passwordassociated with it to prevent unauthorized use. We need to know both your username and your password to log into a Unixsystem.