Lecture-6

Network Security

WHAT IS NETWORK SECURITY?

Network security involves all activities that organizations, enterprises, and institutions undertake to protect the value and ongoing usability of assets and the integrity and continuity of operations.

An effective network security strategy requires identifying threats and then choosing the most effective set of tools to combat them.

Threats to network security include:

Viruses : Computer programs written by programmers and designed to replicate themselves and infect computers when triggered by a specific event

Trojan horse programs : Delivery vehicles for destructive code, which appear to be harmless or useful software programs such as games

Attacks : Including investigation attacks (information-gathering activities to collect data that is later used to compromise networks); access attacks (which exploit network exposures in order to gain entry to e-mail, databases, or the corporate network); and denial-of-service attacks (which prevent access to part or all of a computer system)

Data interception : Involves eavesdropping on communications or altering data packets being transmitted

Social engineering : Obtaining confidential network security information through nontechnical means, such as posing as a technical support person and asking for people's passwords

Network security tools include:

Antivirus software packages : These packages counter most virus threats if regularly updated and correctly maintained.

Secure network infrastructure : Switches and routers have hardware and software features that support secure connectivity, perimeter security, identity services, and security management.
Dedicated network security hardware and software- Tools such as firewalls and intrusion detection systems provide protection for all areas of the network and enable secure connections.

Virtual private networks : These networks provide access control and data encryption between two

Network security tools include:

Identity services : These services help to identify users and control their activities and transactions on the network. Services include passwords, digital certificates, and digital authentication keys.

Encryption : Encryption ensures that messages cannot be intercepted or read by anyone other than the authorized recipient.

Security management : This is the glue that holds together the other building blocks of a strong security solution.