Campus: ..... Course: ..... Class/Section: ..... Date: .....
Name of Faculty: ..... Name of Subject: ..... Code: .....

Introduction to Network security

In this modern era organization greatly rely on computer N/ws to share information throughout the organization in an efficient and productive manner.

organizational computer N/w are now becoming a large and new victus assuming that each steff member has a dedicated workstation.

A large scale company would have a few thousand workstations and many servers on the N/w.

It is likely that these workstations may not be centrally managed no

N/w security is an activity designed to protect the usability and integrity of your h/w and data.

It includes both H/w and s/w technologies. effective N/w security manges access to the N/w. It targets a variety of threats and stops them from entering or spreading on your N/w.

- Diff. to implt in cloud setups.
- simple way of security is assign a unique name and password. (for both personal and professional safety)

What is need of N/w security

Vulnerabilities in TCP/IP → Protocol suite which is most used protocol for comm (It uses HTTP)

1) Transfers are done in plain text
2) weak authentication between client and web-server
3) No solution to syn-packet flooding
4) IP ~~server~~ layer susceptible to many Vulnerabilities due to IP spoofing attacks

How does N/w security work?

→ Authentication - Checks the rights to access data or infrastructure.

→ Authorization - Determining level of access/ permission.

Types of N/w security

N/w Access Control (NAC) - Physical - Biometric system (small organizations) unathorized users

Antivirus and Antimalware s/ws. Technical - (N/w transaction = malware attacks

Firewall protection - administrative (Protects user behaviors)
- need to change in rules.

CIA principles

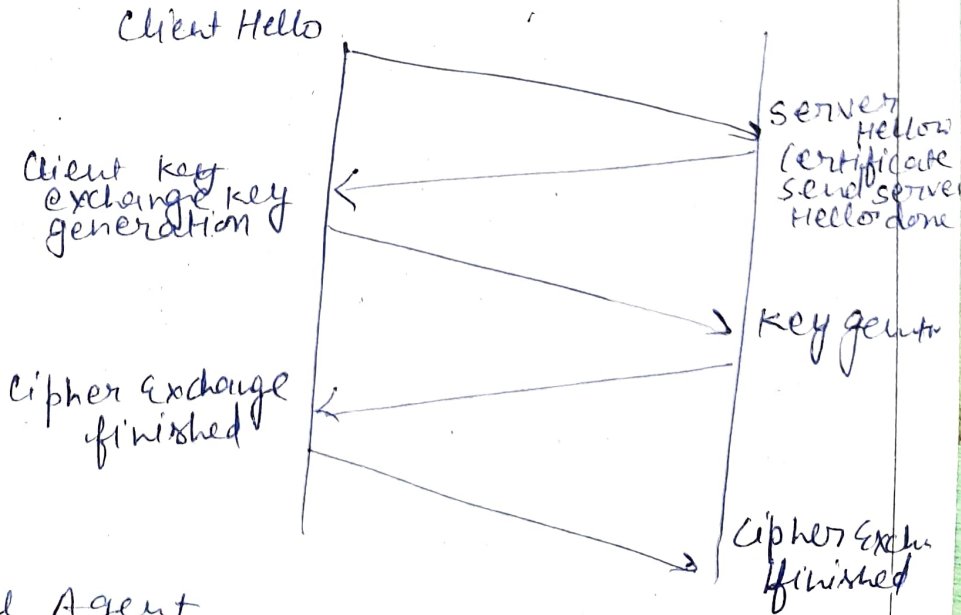
Encryption & decryption → Confidentiality - data is available only to the intended and authorized people.

Digital signature - Integrity - is the maintenance and assurance of accuracy and consistency of data. The data is reliable.

Access control → Availability - available to use.

Transport Layer

TLS is a cryptographic protocol designed to provide comm^{n} security over a N/W.



Appli^{n} Layer

Mail Agent

N/w Layer

IP security

IPsec is a secure N/w protocol suite that authenticates and encrypts the packets of data to provide secure encrypted comm^{n} b/w two computers over an IP N/w.

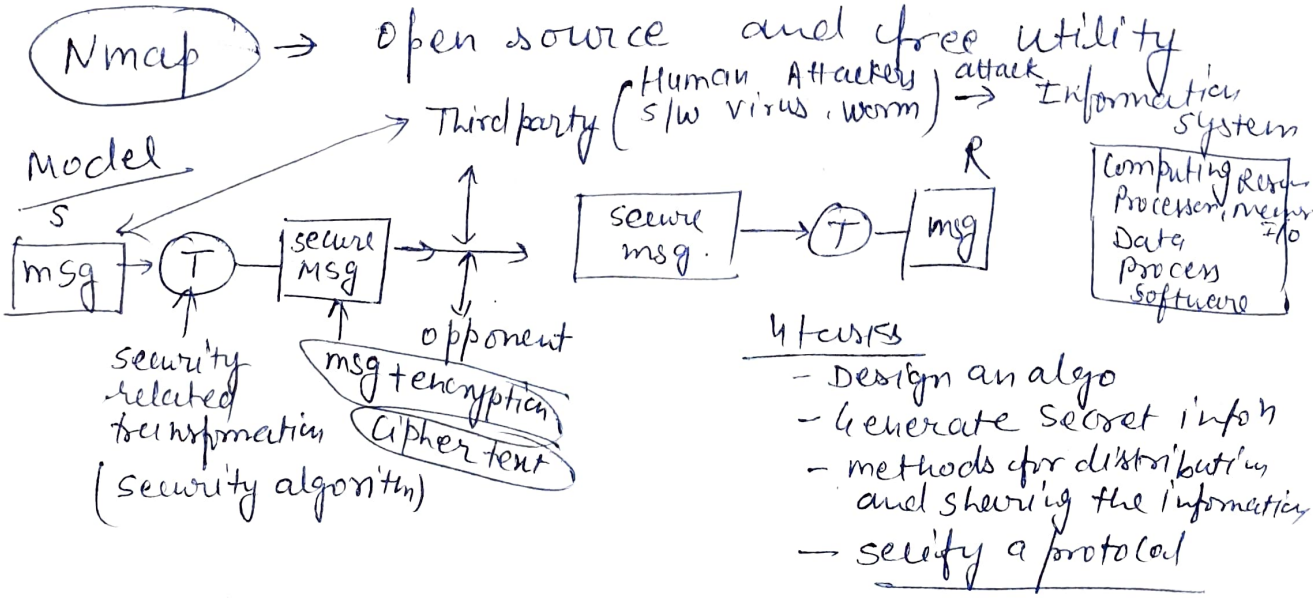
It is used in VPNs (virtual private N/w)

- used to encrypt applin layer data
- Router security (applied protocol)
- Authenticatin (clauses)
- IPsec tunneling (order to create VPNs)

Encapsulation security payload (ESP)

- It provids data integrity, encryption, authenticatin and anti-replay.
- It also provides authentication for payload.

Nmap → open source and free utility



4 tasks

- Design an algo
- Generate secret info
- methods for distributin and sharing the information
- Specify a protocol