# NETWORK SECURITY

1] Threats in network

a) vulnerabilities in networks
- Annonimity
- Many points of attacks
- sharing
- complexity of the system.
- Unknown perimeter
- Unknown path.

b) The motives of Attacker
- challenge
- Fame
- Money
- Ideology.

c) Threats in Transit
- Eavesdropping, wiretapping.

choices for communication medium
- cable
- Microwave
- satellite communication
- optical fiber
- wireless

d) Impersonation
In impersonation attacker can:-
- Guess the identity & authentication details of the target.
- Pick up the identity from a previous comm$^n$ or from Wiretapping.
- Disable the authentication mechanism.
- Use a target that won't be authenticated.
- Use a target whose authentiation data are known.

- Authentication foiled by guessing
- Authentication thwarted by eavesdropping & wireta
- Authentication foiled by avoidance
- Nonexistent authentication.
- well known authentication.
- Trusted authentication.

e) spoofing.
- Masquarade
- session hijacking
- Man in middle attack.

f) Message confidentiality Threats.

- vulnerabilities that can affect confidentiality
  - Misdelivery
  - Exposure
  - Traffic flow analysis.

g) Message Integrity Threats.

- Falsification of messages.

An attacker may perform following actions.

- change some or all content of message
- replace a message entirely, including date, time & sender/receiver identificatio
- reuse an old message
- combine pieces of different messages into one.
- change the apparent message into or
- redirect message
- destroy or delete message.

The attack can be perpetrated in following w
- Trojon horse
- active wiretap
- preempted host
- preempted workstatio

impersonation

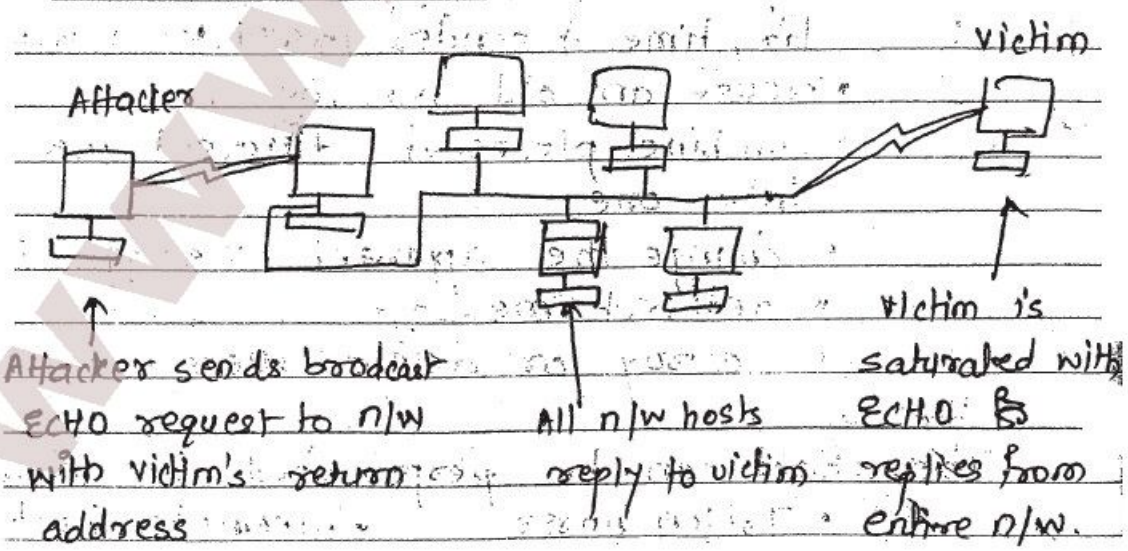
- Noise

h) web site defacement

- Buffer overflow
- Dot dot & address problem
- Application code error
- server side Include.

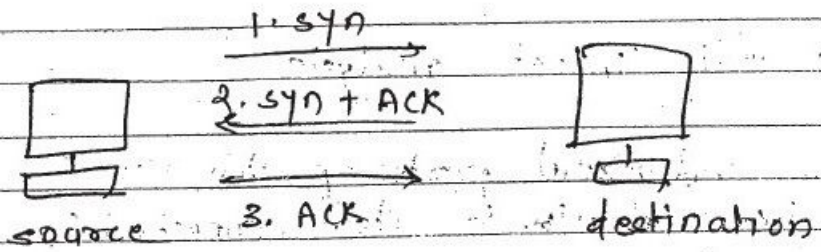
i) Denial of service

- Transmission failure.
- connection flooding.
  - ICMP protocol include
    - ping - requests a destination to return a reply
    - echo - request a destination to return the data sent to it
    - destination unreachable - indicates that dest address can not be accessed.
    - source quench - means dest$^n$ is becoming saturated.
  - Echo chargen
  - ping of death
  - smurf.



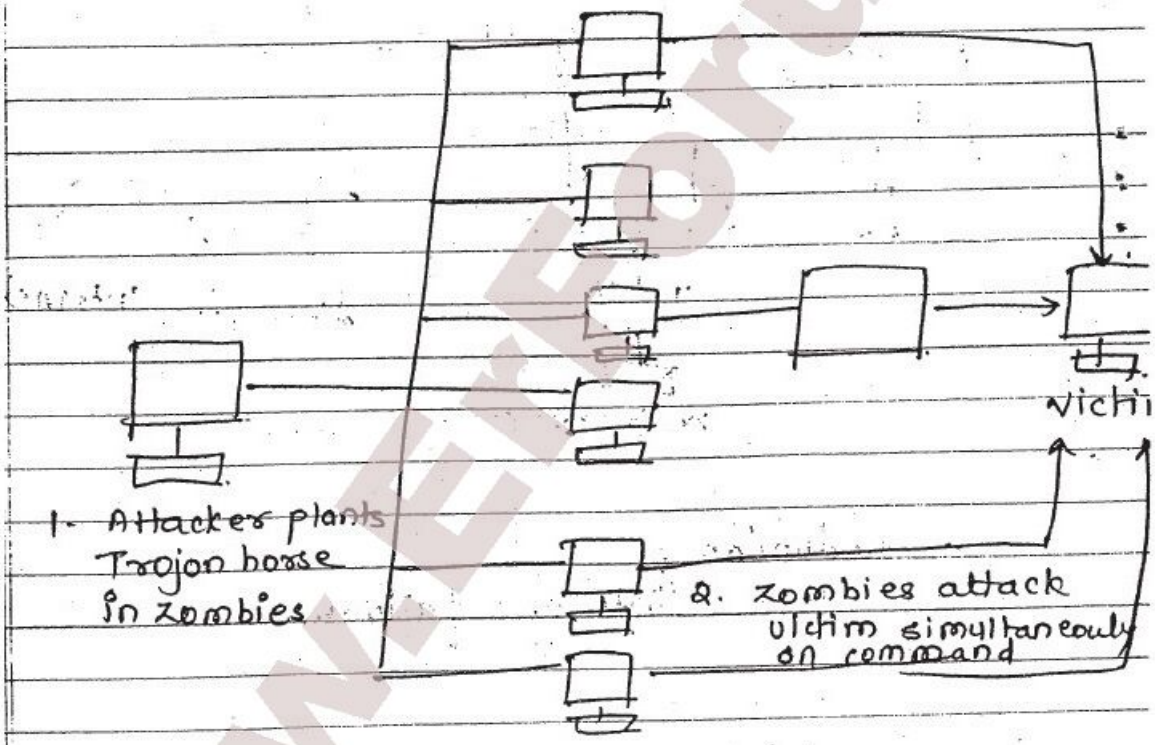
PAGE NO.
DATE

- syn flood




- Traffic redirection.
- DNS attacks.

ii) Distributed Denial of service



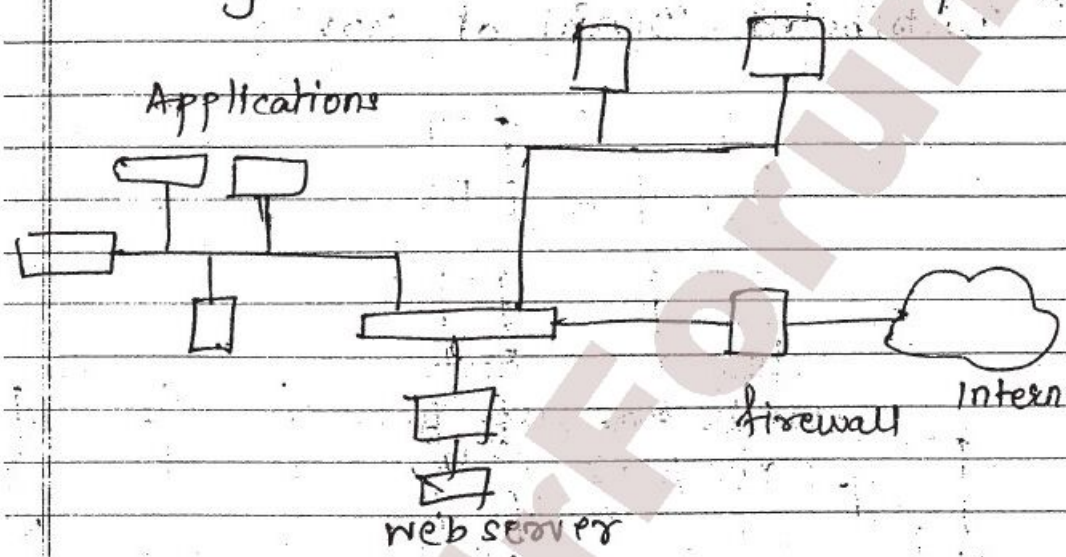
PAGE NO.
DATE

## 2] N/W security controls:

a) security Threat analysis.

- The individual parts of the n/w
- The local n/w is also connected to
- The treats in n/w.

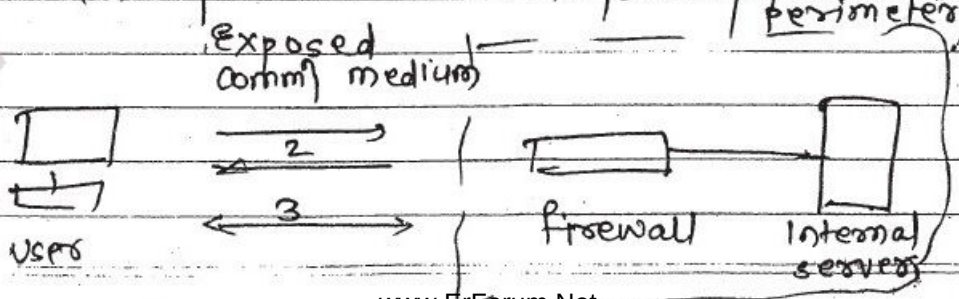
b) Design & implementation
- segmentation




- Redundancy.
- single point of failure.

c) Encryption.
- Link encryption
- End-to-end encryption.

d) - Virtual private n/w.



PAGE NO.
DATE

1. client authenticates a firewall
2. firewall replies with encryption key.
3. client & server communicate via encrypted tunnel.

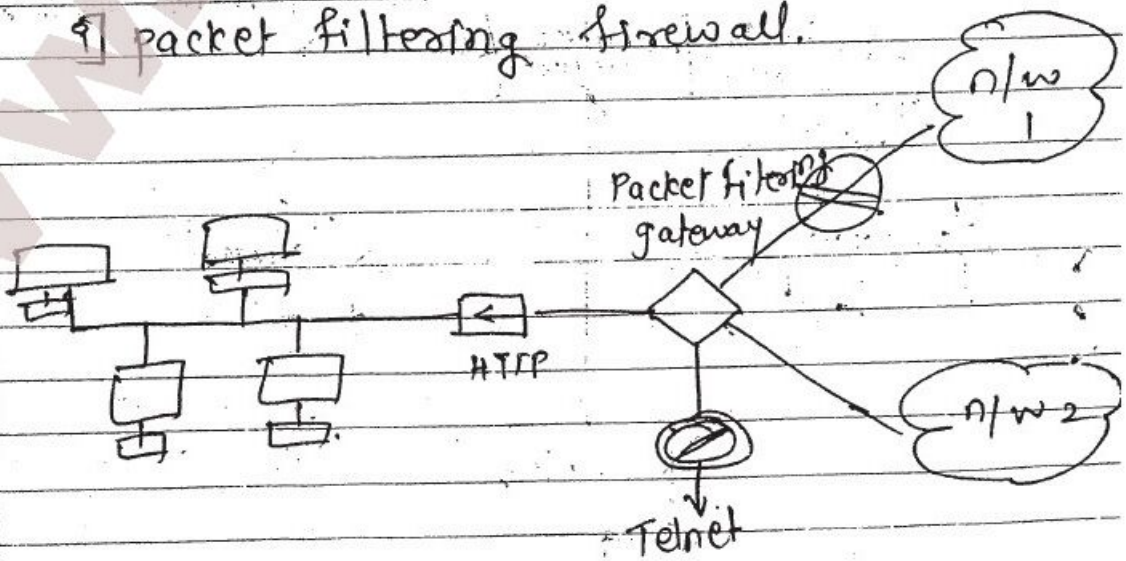
- PKI & certificates.
- SSH encryption.

d) Access control:
- ACL's on routers
- firewalls
- Alarm & Alerts
- Honeypot
- Traffic flow security.

3] Firewalls.
- firewalls are used for following controls
  - service control
  - user control
  - Direction control
  - Behaviour control.

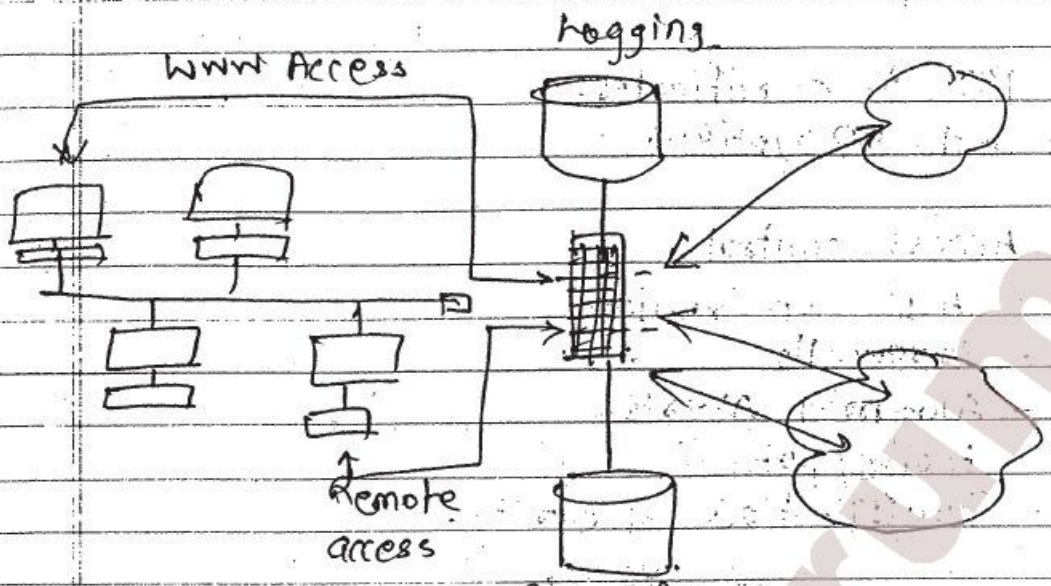
- Types of firewall.

1] packet filtering firewall.



ii) Stateful Inspection Firewall.

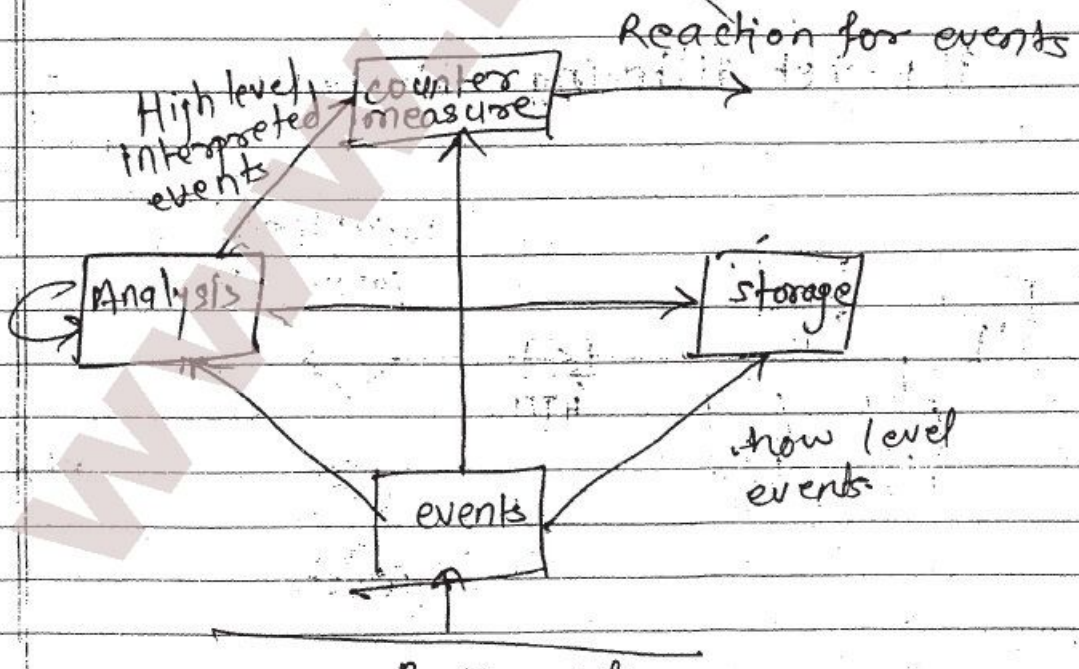
iii) Application Proxy.




iv) Guard

v) personal Firwall.

vi) Intrusion Detection system.



PAGE NO.
DATE

- Accuracy
- completeness
- Performance
- Timeliness
- Fault Tolerence.

functions

monitoring & activity
auditing system configuration
assessing the integrity of critical system & data files
recognizing known attack patterns.
managing auditing
identifying abnormal activity
installing information about intruders
correcting system configuration errors.

Types of IDS

- Heuristic based.
- signature based.
- stealth mode

Goals for IDS

filter packet header
filter packet content
filter in real time, online.
use complex, multipacket signature.
use minimul no. of signature.
hide its presence.
use optimal sliding time window size.

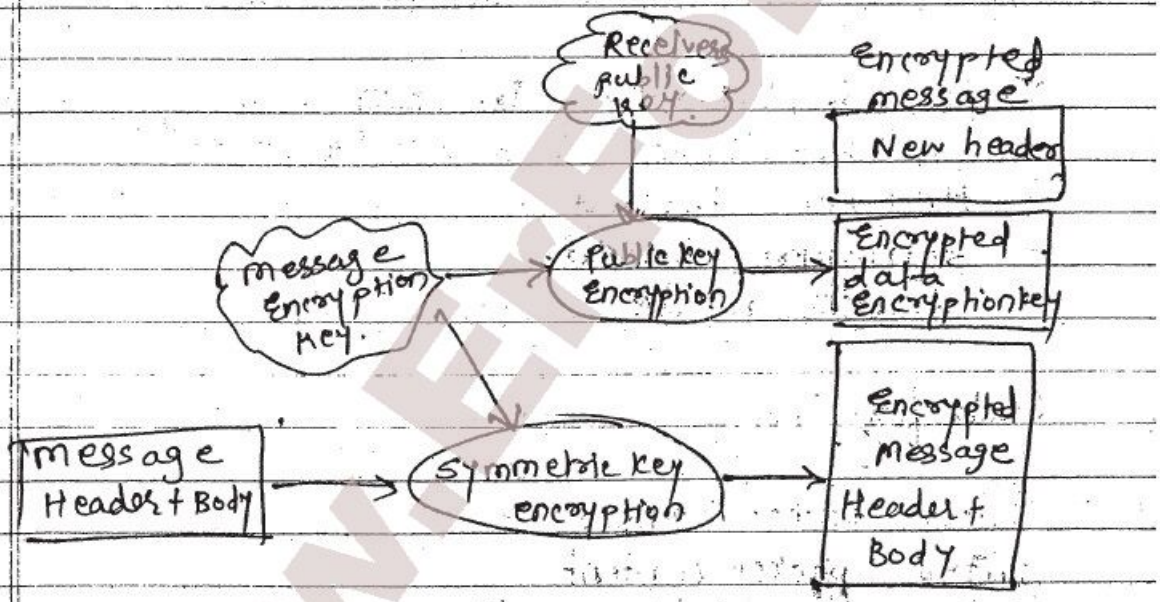
Responding to Alarms :-
To monitor, collect data,
To protect act to reduce exposure.
To call a human.

PAGE NO.
DATE

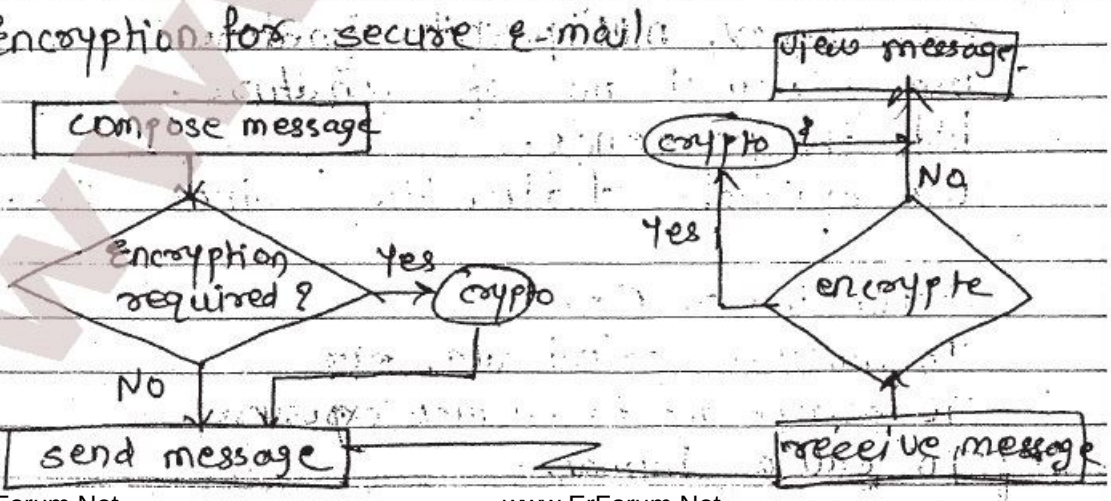
strength of IDS
adv over firewall.
limitations of IDS
- not well defended is useless
- stealth mode is difficult
- sensitivity
- does not run itself.

5] secure E-mail.

Threats to e-mail.
Requirements & solutions
Design.
- confidentiality




Encryption for secure e-mail:



PAGE NO.
DATE

Examples of secure e-mail system :-

PGP

- random session key
- encrypt k message using the session key
- encrypt session key using receipent public key
- Generate MD-5 or hash of the message.
- sign the hash by encrypting hash with sende private key.
- Attach the encrypted session key to encrypt message & digest
- Transmit the message to recipient.

S/MIME

different from PGP in key exchange method. use certificates for key exchange.

6] Network & cryptography.

Privately Enhanced mail (PEM)
first field - Proc type . - type of message
2nd field - contain domain

SSL.
use certificates for key exchange.

IPsec
encryption algo
— " — key
— " — parameters
authentication protocol & key
lifespan of association.
address of the opposite end
sensitivity level of protected data.

arguments against.

- false sense of precision & confidence
- lack of accuracy
- Immutability
- Hard to perform.

3. Organizational security policy.

Audience
users.
owners
benifiliars.

Contents.
- purpose
- protected resource.
- Nature of protection.

Characteristics of a good policy.
- coverage
- ~~secu~~ Realism
- ~~Secure~~, ~~understandable~~ usefulness.
- Durability.

4. Physical security.

i) Natural disasters
- flood
- other natural disasters.

ii) Power loss.
- uninterruptable power loss
- surge suppressor.

iii) Human vandals.