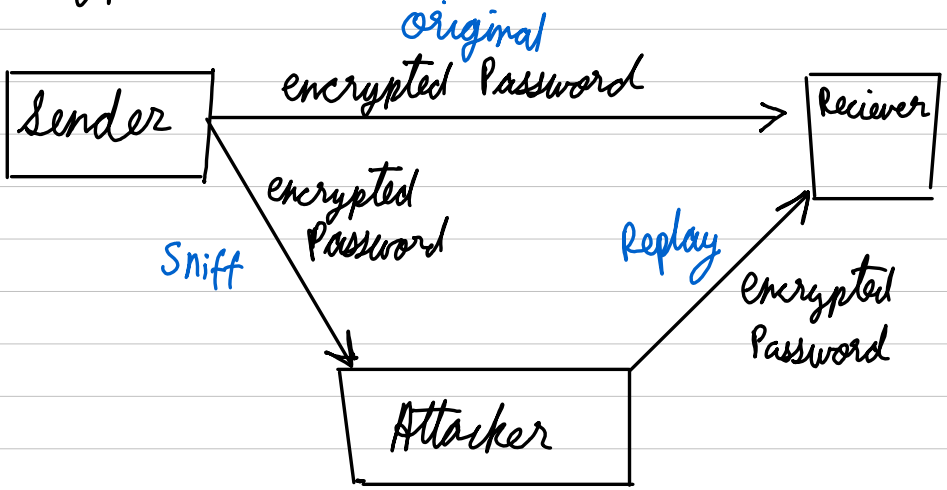
① Explain replay attack

Encrypted passwords & session keys can be stolen from the users

They can be replayed by Malicious users

This attack works even if data is encrypted



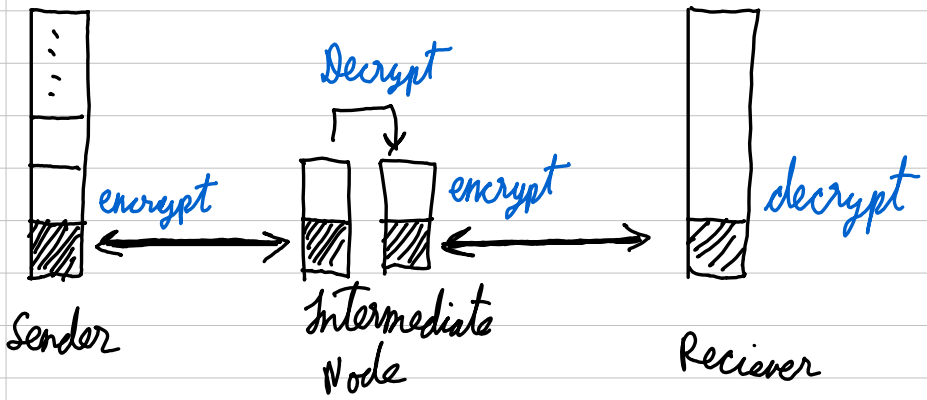
Prevention methods ① Use different keys every time.
② Keys must expire soon
③ Add authentication of device sending key

(2) "End to end" and "link" encryption

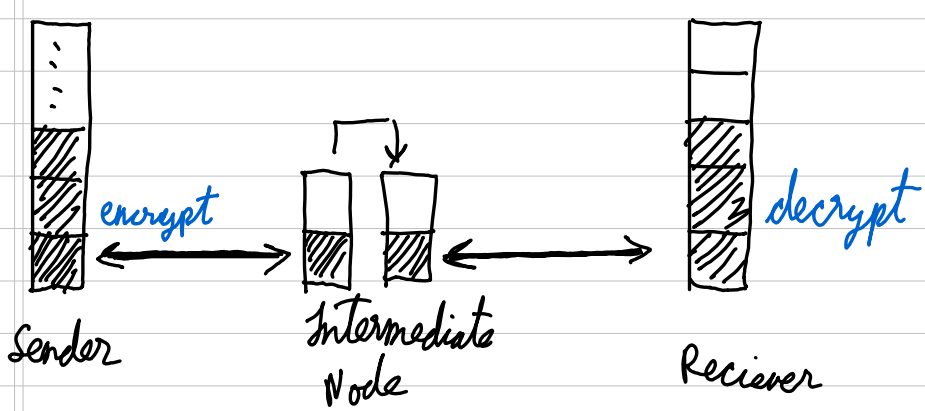
→ In link encryption, data is encrypted just before it is sent.

In end to end encryption, data is encrypted every time

link → Intermediate Nodes can decrypt
E to E → Intermediate Nodes can not decrypt



Link Encryption



End to end encryption

In end to end encryption, data is encrypted right from application layer

In link encryption it is encrypted only at last layer

③ Roll of SSL & TLS in Secure communication

→ SSL (Secure sockets layer) and TLS (Transport layer Security)

Used to protect communication between browser and server

(a) Encryption →

Client & server negotiate encryption algorithms called "cipher suite"
Server sends list of cipher suite options which client chooses from
Data is encrypted in that format

(b) Authentication →

Digital certificates used to prevent imposter

(c) Integrity →

Cryptographic hash functions used to prevent tampering

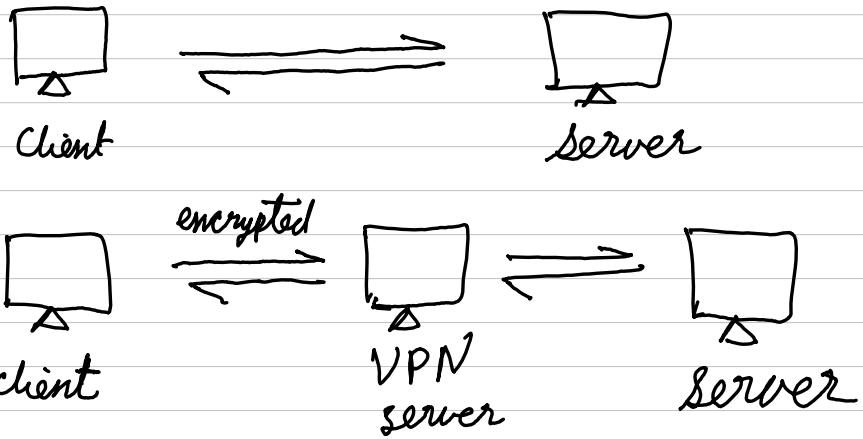
(Q4) what is a VPN

→ i) Virtual Private Network

ii) VPN hides IP address by letting the network redirect through a specially configured remote server

iii) It encrypts data so that the data remains private

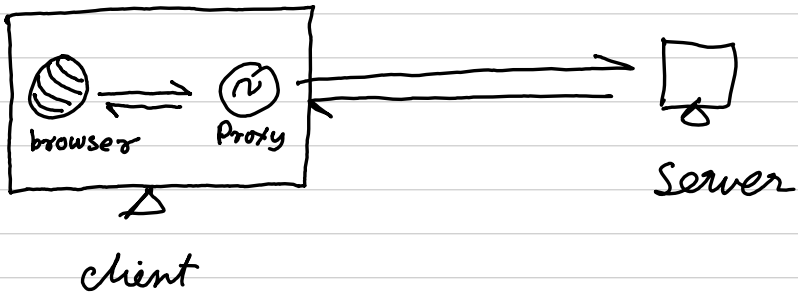
iv) It can be used to hide identity of the user through IP address



v) VPN ensures anonymity

(Q3) What is a network proxy?

→ i) A proxy server acts as intermediate between client & server



ii) Proxy server can act as a gateway between user & internet (web filtering)

iii) Proxy servers can be used to increase anonimity

iv) Proxy servers can be used for web penetration testing (eg. Burp suite)

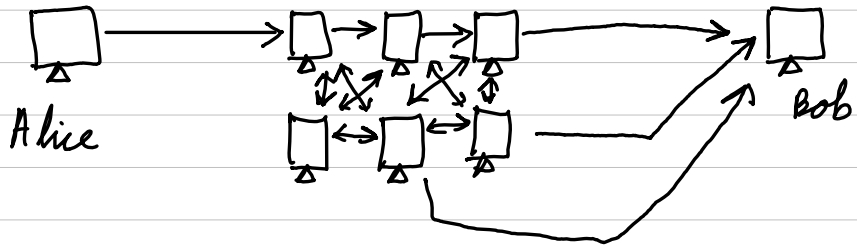
(Q6) Explain about Onion Routing

→ Used to prevent eavesdroppers

Evade authority and governments

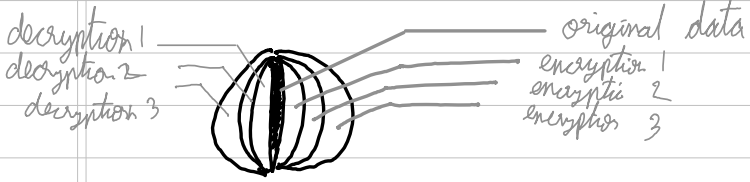
Uses asymmetric cryptography, as well as layers of intermediate hosts

Host does not know about the sender and destination



Client has access to all keys but servers have keys specific to it

Message is wrapped in layers of encryption



(Q7) Explain firewalls

→ A device that filters all traffic between inside & outside networks

Run on dedicated devices

Implement security policies

Set of rules to determine what traffic can or cannot pass through

Provide protection against outside cyber attacks

Protect sensative data

Privacy and security of data

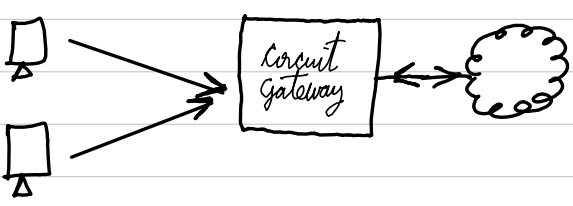
(98) Explain types of Firewalls in detail

→

Circuit level
Host based
Application level
Packet filtering
Stateful inspection

(A) Circuit level gateways

Allows one network to be the extension of another
Operates in Session (OSI-5) layer
Act like VPNs



(B) Host based (Personal firewalls)

Run on host (sender)
eg Windows Defender Firewall

Dont need seperate devices

Select IPs & applications that can access the internet

(C) Application based firewalls

Work on data Packets

Filter dangerous packets

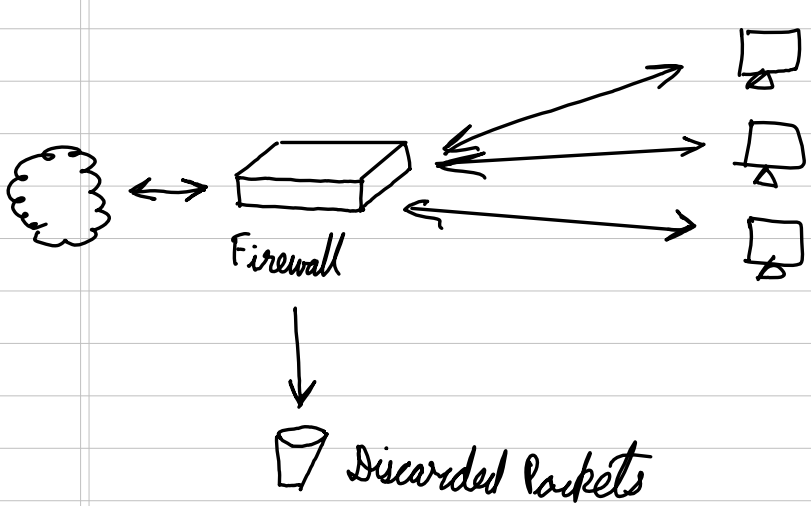
Protect against SQL injection

(D) Packet filtering firewalls

Work on packet headers

Dont access the data

Simple rules of allowed & disallowed IPs



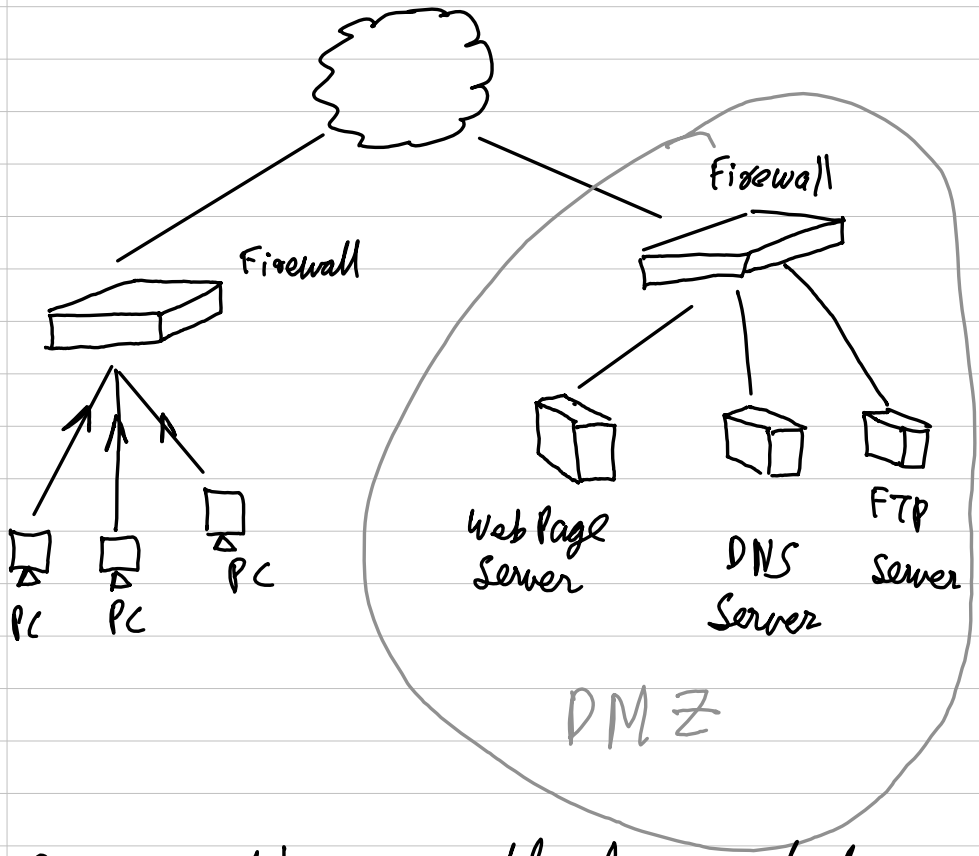
(E) Stateful Inspection Firewall

Packet filtering firewalls dont maintain state from one packet to next

Stateful Inspection Firewalls maintain states

(09) Explain Demilitarized zone

→ DMZ is this Network architecture —



DMZ must be accessable from outside but PC Must Not

Hence seperate the services which must be available from those that must not be.

Hence internal network will not be at any risk

Use two firewalls and form two seperate networks

(Q10) Explain WEP vs WPA

→

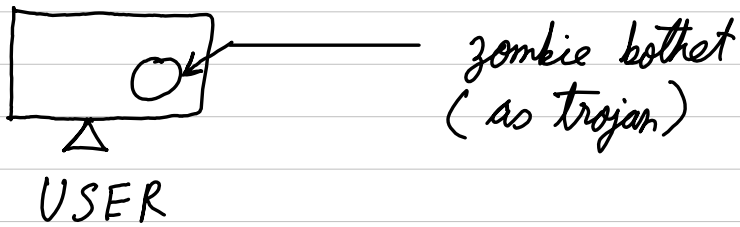
WEP	WPA
Wired equivalent Privacy	Wifi Protected Access
Short key size	long key size
Infrequently changed	Changed every packet
No authentication	Password, token, certificate
40 bit key	256 bit key
Weak encryption	strong encryption (AES)
Brute force	Not Possible brute force
Static key	Dynamic key
No Integrity check	Integrity check

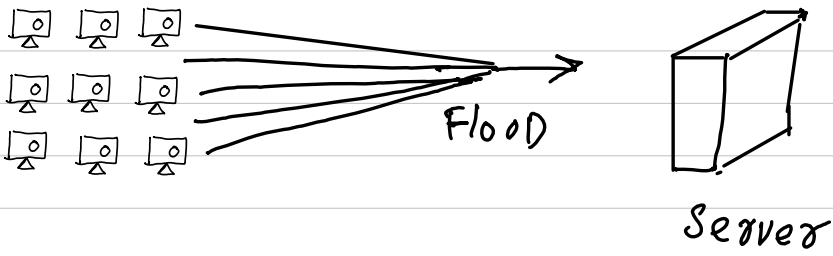
(911) Zombie DDOS

→ Botnets used for DOS

Deployed on users machines as malware

Botnets are undetected as they do little harm to the target device





(Q12) SYN-Flood

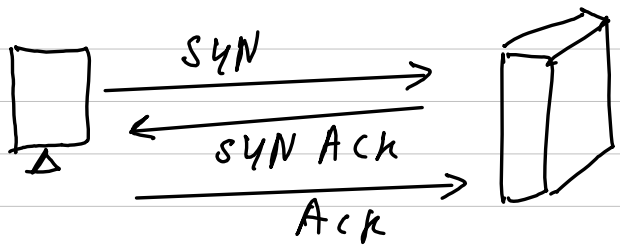
→ Protocol DDOS

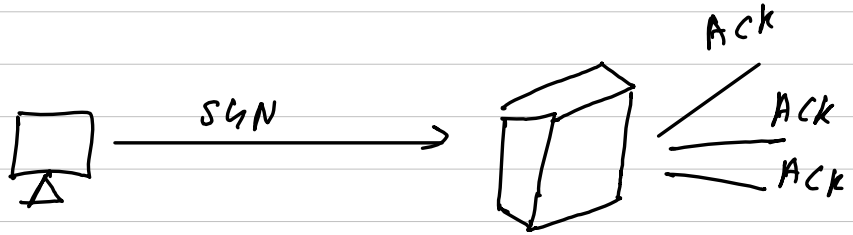
Networking layer is targetted

TCP/IP handshake, keep the target waiting for Ack

Many such waiting requests in FIFO overwhelm the server

Make multiple SYN with fake addresses





SYN Flood

(Q13) Explain Ping attacks, Teardrop & DNS spoofing attack

→ Ping flood → flood a device with ping requests

Ping of death → Send packet larger than maximum allowed size

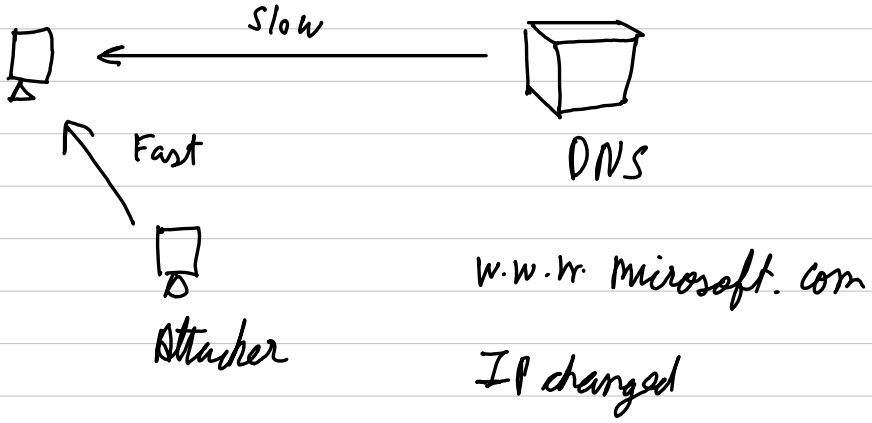
Causes system to crash

Teardrop attack → sends a fragmented packet with overlap that cannot be unfragmented.

Error occurs when device tries to reassemble the packet.

Exploit vulnerability in old systems that cause systems to crash

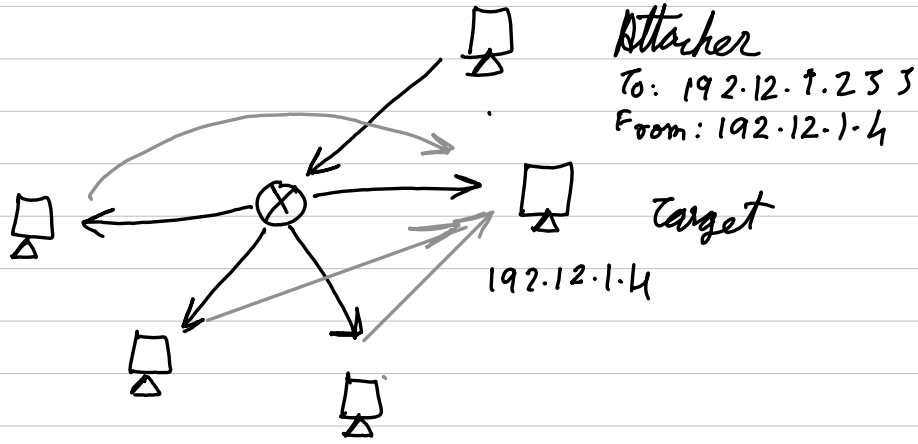
DNS spoofing → DNS records manipulated and users are redirected to malicious websites Attackers make fake DNS servers. Only first entry is valid



(Q14) Smurf attack DDoS

→ Attacker sends ICMP packets to all devices with victims IP.

Since ICMP does not have a handshake, there is no way to verify if source IP is correct.



Example: Prankster pretending to be CEO calls manager and tells him to tell all employees to call him. All employees call real CEO, disturbing him.

Prankster — attacker
CEO — Victim
Manager — router
employee — scrapegoats