① The OSI Model

1. Physical layer → Bits over wire
2. Data link layer → error check and frame sync
3. Network layer → Routing
4. Transport layer → TCP/UDP
5. Session Layer → session Management
6. Presentation layer → Data formats
7. Application Layer → HTTP/API/HTTPS.

② Firewalls

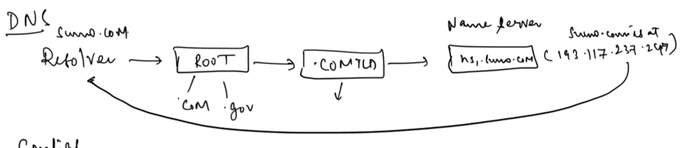
- Software based firewalls - Windows firewall
- Hardware firewall - Cisco ASA
- Network firewall - Cisco ASA
- NGFW - fotinet and check point
- Host-based firewall - Comodo
- WAF → Akamai, cloud flare
- proxy firewall → Squid
- Stateful firewall → Works with brain
- Stateless firewall → ACL Rules
- .... Many more

} Rules & actions taken to Prevent malicious actors

③ NAT - Network Address Translation

- Nat can help support the co-existence of IPV4 and V6 together and can talk to them each other using Nat 64 Translations

④ DNS



Configs

A - @ → points to specific IP-addresses (1.2.3.4)
CNAME → alias → www.hello.com / hello.com
MX → mail server IP
PTR → when lookup for 1.2.3.4 should return hello.com
TXT → helps us to add some human readable text
SOA → Start of authority, contains important info about admins, refresh periods etc
DMARC → Domain-based Message auth. Reporting and conformance.
This policy tells the receiving email server what to do after checking DKIM and SPF records of the receiving domain.
SPF → Guest list for the party, SPF is like the attendant, will not let you in/mark Spam if your IP is not in the SPF record.
DKIM → uses PKI for authenticity, in the form of DKIM header

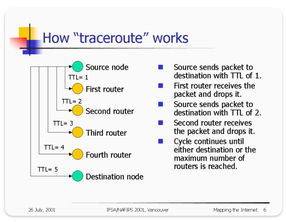
DMARC + SPF + DKIM (Copy) together work to check our mail & order to check who they r & they are

ARP → Address Resolution Protocol
- occurs at layer 2) IP-address to MAC.
- RARP → Discover own IP addresses
- GARP → notify other devices on the LAN about IP/MAC change
- PARP → helps devices to reach devices on other subnets without the need of routing

DHCP - Dynamic host config. protocol. (67/68 UDP)

Discover → Offer → Request → Ack
lease renewal request → Request Ack

Traceroute
- Generally uses UDP; path followed by the packet to reach destination
- → ICMP echo request → ICMP echo reply
- → By default UDP by windows, ICMP by unix (tracert)
- → TCP SYN / hop limit / TTL



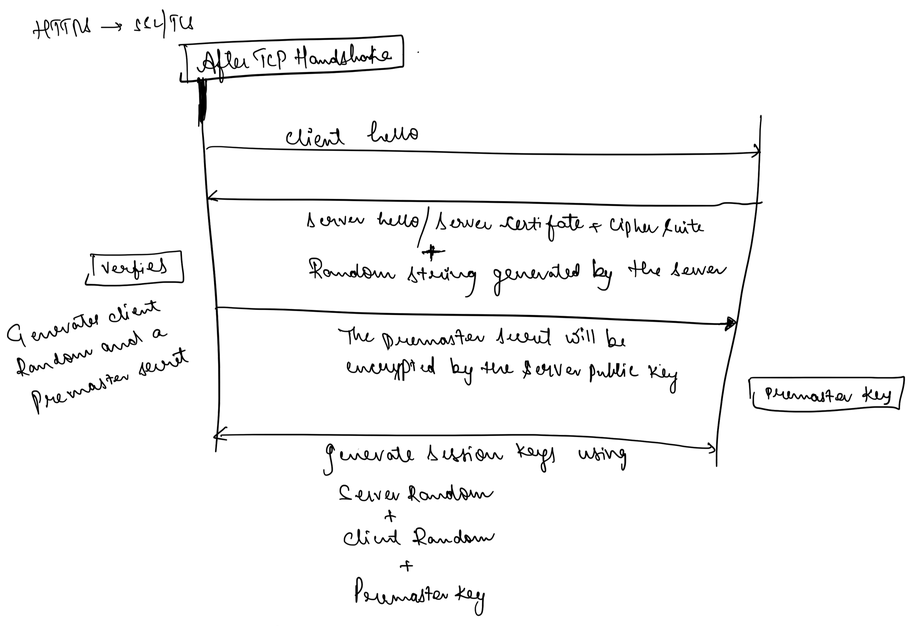
NMAP → Network Mapper
- TCP/UDP/SCTP

Gateway protocols

IGP
- Distance
  - Ripv1 → RIPV2
  - IGRP → EIGRP (advanced)
- Link state
  - OSPF
  - IS-IS

EGP
- Path vector
- BGP

HTTPS → SSL/TLS



Poodle → Downgrade
Beast → Vulnerability in CBC (Cipher suite)
Heartbeat → vulnerability in openSSL library heartbeat extension

Ports

	21 - ftp	137/8/9 → NETBIOS	
	22 - ssh	993/143 - IMAP	
SSL 992 /	23 - telnet	161 - SNMP	
	25 - SMTP	389 - LDAP	
	53 - DNS	443 - HTTPS	
	67,68 - DHCP	445 - SMB	
	69 - TFTP	514 - Syslog	
	80 - HTTP	3306 - MySQL	
	88 - Kerberos	3389 - RDP	
995 /	110 - POP3		
	135 - RPC		

Response headers

- 1xx → Information Response → 100: continue
- 2xx → Successful → 200: OK
- 3xx → Redirect → 302: found, 301: moved permanently
- 4xx → client error → 404: Not found; 403: forbidden
- 5xx → Server error → 502: Bad gateway, 503: Service unavailable