1-HTTP->HyperText Transfer Protocol Can make communication between server and client

2-Every request is completely independent Usee state-header-body

3–HTTPS→HyperText Transfer Protocol Secure Encrypted data send by it use SSL/TLS

4-Method of HTTP Get→retrieve data Post→submit Put→update data Delete→delete data

5-Header of data : General→ (request url- request method - state of code-remote address -referrer policy)
Response→ (secure -set cookie-content type-content length -data-Date(name of file))
Request→ (cookies-accept(language)-content type-content length-authorization-user agent

6-State code : 1xx→ request/receive processing
2xx→ success accept and understood
3xx→ redirect action must be taken
4xx→client have erred
5xx→ problem in server Server error → fulfill request
200→ok
301→moved to new url
304→not modified
400→ bad request
500→ internal server error

7- response header without information / content

8- option method may be more dangerous to hack the web 9-date→ ebook folder (static code )

10-307 → temporary redirect status code indicate that target source under different url and user can’t change the request method if it perform an automatic redirection

11- DataBase :
–sql request from machine
-database work in server
-record return set of data but remain in server
-web→communication client & server

-client machine →smartphone (allow user to make a request)
-server→ computer program->save programs ->multiple clients Contain web resource /host web application -store user and programs data Server listing for request which →(received one -response with message )

12-peer to peer only client to client (torrent)

13-communication between server and client make by private and public key which use public key to symmetric the request by using the same key to encrypt data
-Asymmetric:use th e public key for encryption and private key for decryption

14-using OSI with 7 layers to know how to send and get data

15-using protocol DHCP to get an ip address to connect the internet but layer two using mac address inside lan network to know which device to get and send data to it

16-to send data message must have the destination port and ip address and source port and ip address

17-using :
TCP :-
- Connection oriented
- Reliability
- HTTP-SMTP-FTP-HTTPS-Telnet

UDP:-
- Connectionless
- Used for application need fast
- DNS - DHCP -TFTP - SNMP - RIP

18- Three way handcheck used (send-ack-ack ack) to open connection

19- to make DNS amplification attack :-
- Used wireshark to know connection state
- If config to config ip address and connection it with any protocol connection
- Used TLD to make Domain name and know how to make it
- Hacker can hack by subdomain which bind to main domain
- (CName-A-AAAA-AX)which every one related to domain
- Use ip tables to know where hacking and stop it
- Burp Suite used to proxy to know what happen exactly in web browser from (request-response-hacking)