Name: Sandeep Sahani. R.

TE IT

Page No.: 1

Date: 12/10/2021

Subject: CNS

Q2
A] Explain Access Control? How it is different from Availability?

Ans
- Access control is a fundamental component of data security that dictates who's allowed to access and use company information and resources.
- Through authentication and authorization, access control policies make sure users are who they say they are and they have appropriate access to company data.
- Availability refers to the percentage of time that the infrastructure, system, or solution remains operational under normal circumstances, in order to serve its intended purpose.
- For cloud infrastructure solution, availability relates to the time that the data center is accessible or delivers the intend IT service as a proportion of the duration for which the service is purchased.
- The component of Access Control are as fallows:
  1. Authentication
  2. Authorization
  3. Access
  4. Manage
  5. Audit.

Q3.

A] Describe IDS and Compare it with firewall.

Ans
- An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered.
- It is a software application that scans a network or a system for harmful activity or policy breaching.
- Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system.
- A firewall is a hardware and/or software which function in a networked environment to block unauthorized access while permitting authorized communications. firewall is a device and/or a software that stands between a local network and the Internet, and filters traffic that might be harmfull
- An Instrusion Detection System (IDS) is a software or hardware device installed on the network (NIDS) or hos (HIDS) to detect and report intrusion attempts to the network
- We can think a firewall as security personal at the gate and an IDS is a security camera of the gate.
- A firewall can block connection, while a IDS cannot block connection.

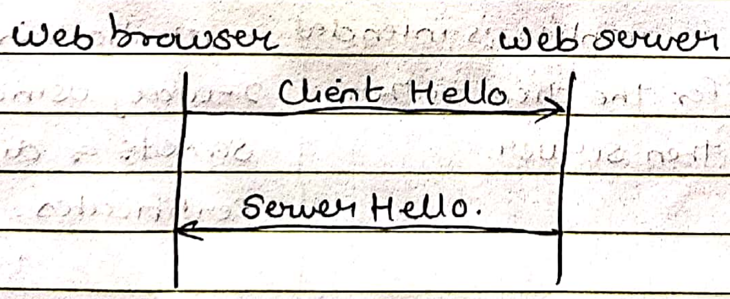
Q4.
B].

- The handshake protocal of SSL is the first sub-protocal used by the Client & the server to communicate using an SSL enabled connection.
- The handshake protocal is actually made up of four phases.

a. Establish security capabilities
b. Server authentication & key exchange.
c. Client authentication & key exchange.
d. finish.

Phase 1: Establish security ~~compa~~ capabilities

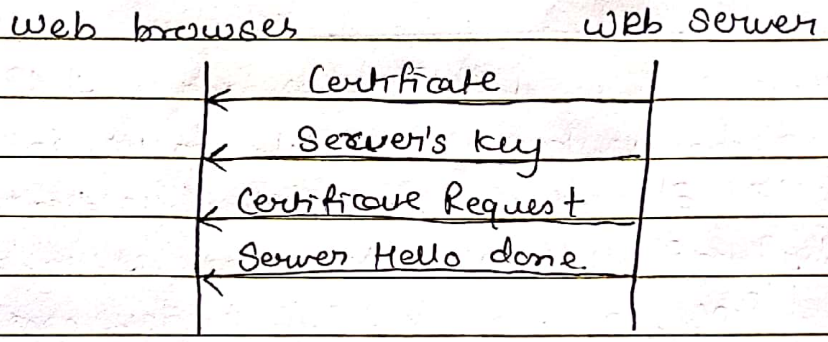
- This phase is used to indicate a logical connections and establish the security that connection.
- This consist of two messages - The 'Client' 'hello' & their server hello.



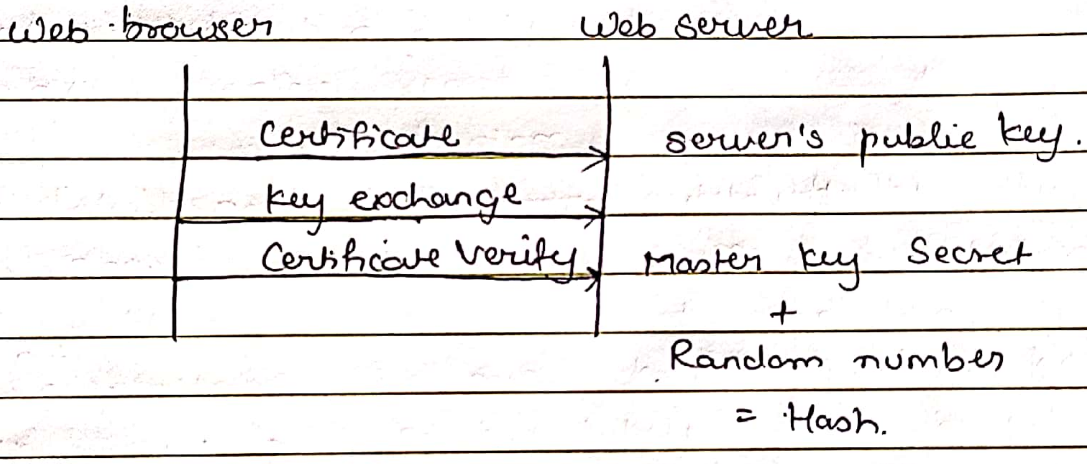
- This phase is limited by the Client by sending a client Hello message.

Q4
B]

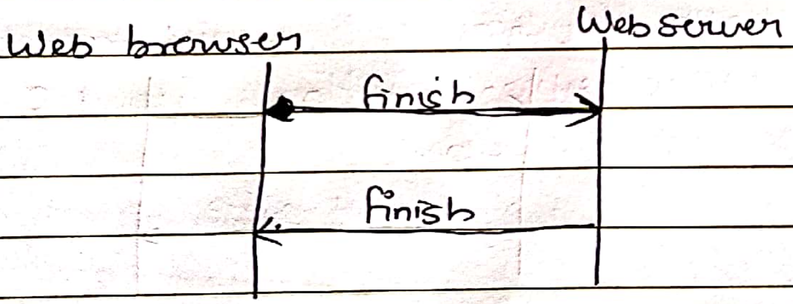
Phase II: Server authentication & key exchange.



Phase III: Client authentication & key change



Phase IV: Finish



- This phase is initiated by the Client
- The Client sends a finish message to the server & server send finish message to client.

Q6.
A]

SSL	TLS	IPSec.
1. The full form of SSL is secure socket layer.	1. The full form of TLS is Transport layer security	1. The full form of IPSec is Internet Protocal security.
2. It don't support TLS as a Compatibility Option.	2. TLS v1.0 had an SSL fallback machanism for backwords-compatibility	
3. SSL supports fortezza algorithm.	3. TLS does not support fortezza algorithm.	
4. The Configuration of SSL is Easy	4. The Configuration of TLS is medium.	4. The Configuration of IPSec is Hard.
5. SSL not has preshared key	5. TLS not has preshared key	5. IPSec has preshared key.
6. Same as TLS the there are 1-way or 2-way.	6. TLS authentication is implies, is intended for the client rather then server.	6. IPSec has authentication as 2-way using shared secrets or digital Certificates.