4/10/22 Mikil Jalwani CNS A-2 D15B/37

Q1) Explain the concepts of double DES and Triple DES.

Ans a) As we know DES uses 56 bit key to encrypt any plain text which can be easily be cracked by using modern techniques.

b) To prevent this from happening double DES and triple DES were introduced which are much more secured than the original DES because it uses 112 bit and 168 bit keys respectively.

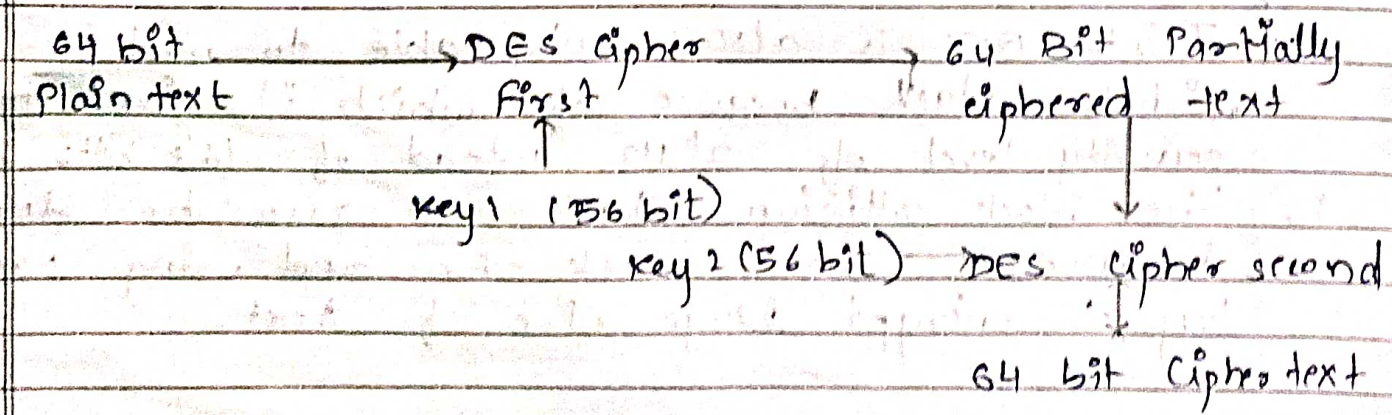
c) Double DES -

i) It is an encryption technique which uses two instances of DES on same plain text.

ii) In both instances it uses different keys to encrypt the plain text.

iii) Both keys are required at the time of decryption.

iv) The 64 bit plain text goes into first DES instance which then converted into a 64 bit middle text using the first key and then it goes to second DES instance which gives 64 bit cipher text by using second key.



Teacher's Sign.:

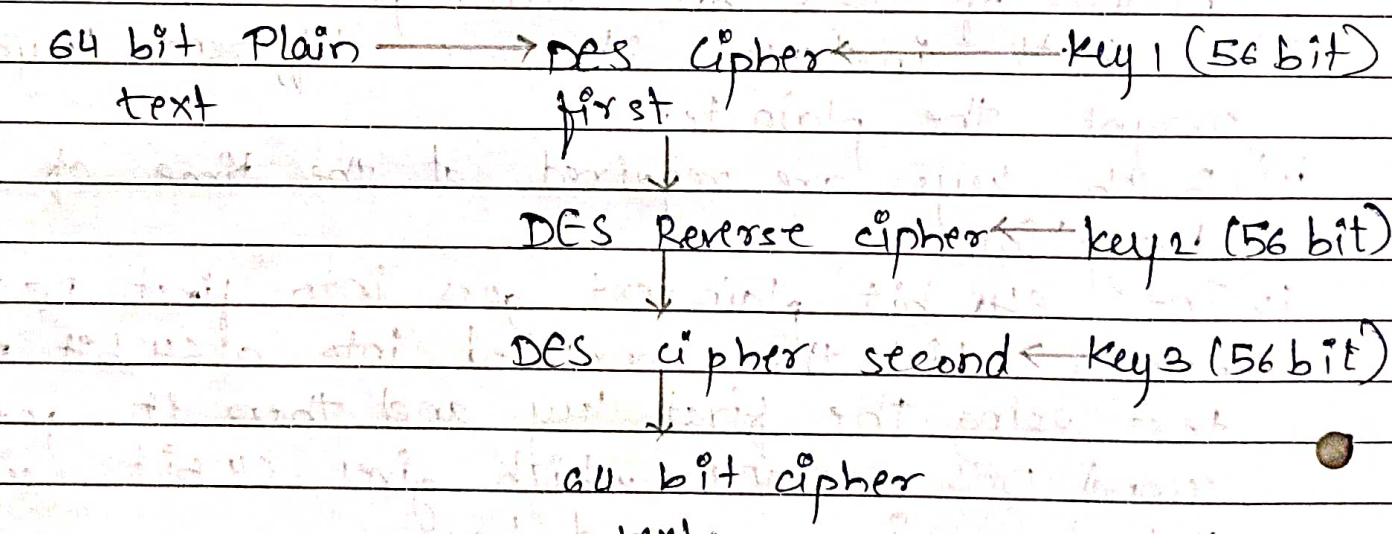
Page No.
Date

v) However, double DES uses 112 bit key but gives security level of 2^56 but not 2^112 and this is because of meet-in-the-middle attack which can be used to break through double DES.

d) Triple DES:

i) Triple DES is an encryption technique which uses three instances of DES on plain text.

ii) It uses three different types of key choosing technique in first all useds keys are different and in second two keys are same and one is different and in third all keys are same.



iii) Triple DES is also vulnerable to meet-in-the-middle attack because of which it gives total security level of 2^112 instead of 168 bits key.

iv) The block collision attack can also be done because of short block size and using same key to encrypt large size of text.

Teacher's Sign.: _____

Page No.
Date

Q2) Compare HMAC and CMAC.

	HMAC	CMAC
i)	MAC generation function	Hash function	Symmetric cipher.
ii)	speed of mac generation	Highest	~~lowest~~ Medium
iii)	Strength of mac	High	very high
iv)	Number of keys used	one	One key divided into multiple sub-keys.

Q3) List the steps involved in key generation, message signing and signature verification in RSA digital signature scheme.

Ans: i) RSA uses public key cryptography for creating and verifying digital signatures.

ii) Key Generation -
RSA digital signatures work on public and private key pairs.
The can be ~~seed~~ generated by the regular key pair generating method by a certificate Authority (CA) or on the user's ~~sub~~-system by herself.

public key = (n, e)
private key = (n, d).

Teacher's Sign.: _____

iii) Message signing -
To sign a message M

Calculate the hash value of message M at sender's end.
$h = hash(M)$
Encrypt h using RSA private key.
Signatures $S = (h)^d \bmod n$

iv) Signature verification -

Decrypt signature S using public key.
$h' = (S)^e \bmod n$.
Calculate the hash value of the message M at reciever's end.
$h = hash(M)$
If $h = h'$, the signature is valid else invalid.

Q4) Explain and compare SHA256 and SHA512

	SHA 256	SHA512
i)	SHA256 is a SHA2 type that generates a 256 bit hash value.	SHA512 is a SHA 2 type that generates a 512 bit hash value.
ii)	Block size is 512 bit	Block size is 1024 bit
iii)	Max message $2^{64}-1$ bit	Max message is $2^{128}-1$ bit.
iv)	Word size is 32 bit	Word size is 64 bit.
v)	64 rounds are performed.	80 rounds are performed.

Teacher's Sign.: _____

Page No.
Date

Q5) How does Kerberos work?

Ans Scenario1: User authenticating to a computer.

i) The user enters username and password on computer.

ii) Kerberos software running on computer sends the username to authentication service (AS).

iii) The authentication service (AS) checks if the username is present. If yes, it sends back a ticket granting ticket (TGT) which is encrypted with the user's ~~pre-installed~~ pre-shared secret key.

iv) If user entered correct password, she can decrypt the TGT and then access is granted to computer.

Scenario2: Authenticated user wants to print ~~doc~~ a document.

i) The computer sends the TGT it received earlier to TGS. The TGT is a proof for the TGS that the user is already been successfully authenticated

ii) TGS creates a new ticket and puts two copies of the same session key with the user's secret key and the second copy with print server's secret key. The ticket also contains an authenticator information that holds the value of the user's computer's IP address, sequence number and timestamp from where TGT came. It sends the ticket to user's computer.

iii) The user decrypts the ticket created by the TGS with her secret key and obtains session key. It adds another set of authenticator information to it and sends the ticket to print server.

Teacher's Sign.: _____

iv) The print server recieves the ticket and extracts the session key by decrypting it. It knows that the KDC created the ticket because the KDC had the knowledge about the print server's secret key. It also gets the two authenticator that uniquely identify the user's computer. If the two authenticators match, the user is successfully authenticated and the print server prints the user's document.

Q6) Alice chooses public key as (7, 33) and B chooses public key as (13, 221). Calculate their private keys. A wishes to send m=5 as a message to B. Show message signing and verification using RSA digital signature.

Alice $p=3, q=11, n=3, e=7$

$\phi(n) = (p-1)(q-1) = 20$

d = MI of 7 mod 20.

Q	A	B	R	T_1	T_2	T
2	20	7	6	0	1	-2
1	7	6	1	1	-2	3
6	6	1	0	-2	3	-20
-	1	0	-	(3)	-20	

$d = 3$

Private key of Alice is = $\{d, n\} = \{3, 33\}$.

Teacher's Sign.: _____

Bob

$p = 17$, $q = 13$, $e = 13$

$\phi(n) = 192$

$d = MI$ of $13 \bmod 192$

Q	A	B	R	T_1	T_2	T
14	192	13	10	0	1	-14
1	13	10	3	1	-14	-15
3	10	3	1	-14	+15	-59
3	3	1	0	+15	-59	=192
-	1	0	-	(59)	192	

$d = 192 - 59 = 133$

Private key of Bob is $\{d, n\} = \{133, 221\}$.

$h = hash(M)$

Assume hash value of M be 12.

$S = 12^3 \bmod 33$

$12^1 \bmod 33 = 12$

$12^2 \bmod 33 = 12$

$12^3 \bmod 33 = 12$

$S = 12$

For decryption, Bob will use Alice's public key.

$M = S^e \bmod n = 12^7 \bmod 33$

$\therefore M = 12$

Teacher's Sign.: _____

Page No.
Date

Q7) Write a short note on digital certificate. X.509 and PKI.

Ans a) X.509 is a digital certificate that is built on top of a widely trusted standard known as ITU or in which the format of PKI certificate is defined.

b) X.509 digital certificate is a certificate-based authentication security framework that can be used for providing secure transaction processing and private information.

c) The core of X.509 authentication service is the public key certificate connected to each user. These user certificates are ~~used~~ assumed to be produced by some trusted certification authority and positioned in the directory by the user or the certified authority.

d) Once an X.509 certificate is provided to a user by the certified user by certified authority, that certificate is attached to it like an identity card. The chances of someone stealing or losing it are less, unlike other unsecured password.

PKI -

a) Public key ~~of~~ infrastructure (PKI) is a catch all term for everything used to establish and manage public key encryption, one of the most common forms of an internet encryption.

b) It is baked into every web browser in use today to secure traffic across the public internet, but organisations can deploy it to secure their internal communications and access to connected devices.

Teacher's Sign.: _____

c) PKI is a technology for authenticating users and devices in the digital world. The basic idea is to have one or more trusted parties digitally sign documents certifying that a particular cryptographic key belongs to a particular user or device. The key can then be used as an identity for the user.

d) A public key infrastructure relies on digital signature technology, which uses public key cryptography. The basic idea is that the secret key of each entity is only known by that entity and is used for signing. The key is called private key. There is another key derived from it called the public key, which is used for verifying signatures but cannot be used to sign. The public key is made available to anyone and is included in the certificate.

Q8) Explain RC5 algorithm.

Ans It was designed by Ronald Rivest in 1994. RC stands for "Rivest Cipher" or "Ron's Code".

Major attributes of RC5-

i) Symmetric key based algorithm.
ii) It works as a block cipher.
iii) It uses a variable block size - 32, 64, 128 -bit
iv) It uses a variable length ~~block~~ key size ranging from 0 to 2040 bits.
v) It uses variable number of rounds of operation- 0 to 255.

Teacher's Sign.: _____

Page No.
Date

Internals of RC5 algorithm-

i) RC5 is word oriented. All of the basic computational operations have w-bits words as inputs and outputs. RC5 is a block cipher with a two word input block size and two word output. The nominal choice for w is 32-bits for which RC5 has 64 bit plaintext and ciphertext block size.

ii) The number of rounds r is second parameter of RC5. Choosing a large number of rounds provides an increased level of security. RC5 uses an expanded key table S that is derived from user's supplied secret key. The size t of table S also depends on the number of rounds r. S has $t = 2(r+1)$ rounds.

Key expansion-

i) Converting secret key from bytes to words.
ii) Initializing the array S.
iii) Mixing in secret key.

Encryption-

Assume that the input block is given in two w-bit registers A and B. Assume that the key expansion step is already performed and thus the array S is already populated. The encryption algorithm can be outlined in following pseudo code.

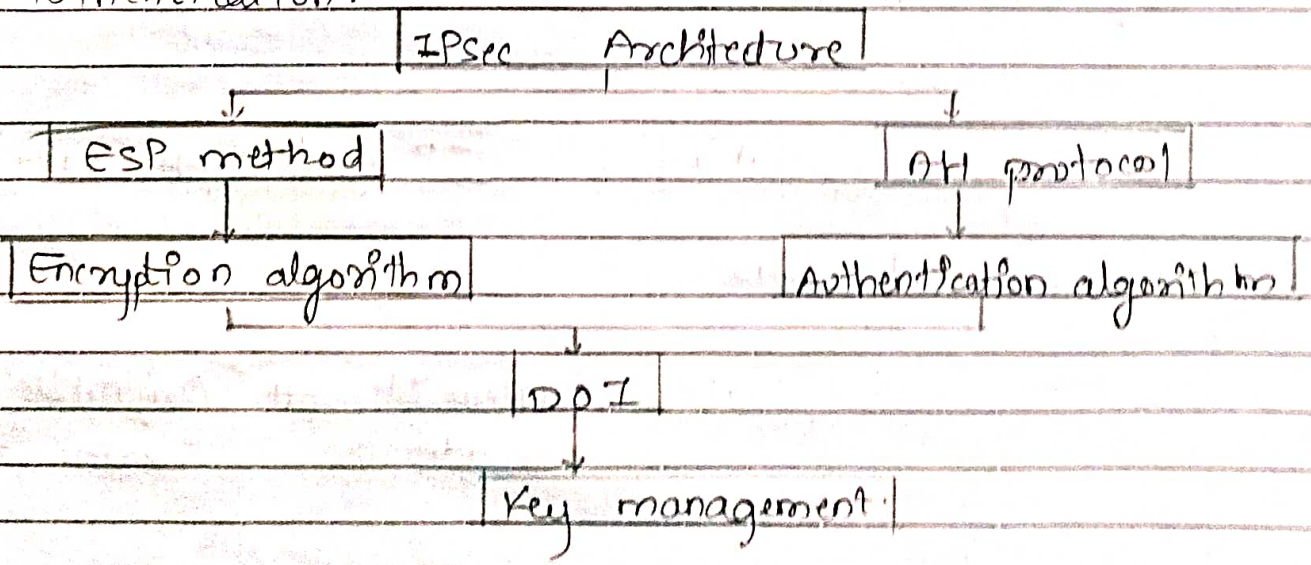
Teacher's Sign.: _____

```
A = A + S[0];
B = B + S[1];
for i = 1 to r do:
    A = ((A xor B) <<< B) + S[2*i];
    B = ((B xor A) <<< A) + S[2*i+1];
```

Q9) Explain IPSEC architecture and Protection mechanism of AH and ESP.

Ans IPsec architecture uses two protocols to secure the traffic or data flow.
There are protocols called ESP and AH.
IPsec architecture includes protocols, algorithm and key management.
All these components are very important in order to provide the three main services.

- Confidentiality
- Integrity
- Authentication.



Teacher's Sign.:

Next Header | Payload length | Reserved

Security Parameter Index
Sequence index
Authentication data.

Authentication header (AH)-

It also provides replay protection. It doesn't provide encryption.

AH calculates the integrity check value (ICV) over non-changing fields of IP header.

Next header
Reserved
Sequence number
Payload length
Security Parameter Index (SPI)
Padding types.

| IP header | Data |

| IP header | AH | Data |

Transport mode

| IP header | Data |

| New IP header | AH | Original IP header | Data. |

Teacher's Sign.: _____

Page No.
Date

Encapsuling Security payload (ESP)-

ESP can be applied with or without AH. Here ESP can itself provide integrity. You have an option to additionally calculate integrity using AH.
ESP in transport mode encrypts the actual payload so that it cannot be read by an unauthorized entity. In tunnel mode, the IP header information is encrypted as well.

Transport mode-

Before applying ESP

IP header	data

After applying ESP

IP header	ESP header	Data	ESP trailer	ESP ICV

Encrypted

Authenticated

Tunnel mode-

Before ESP

IP header	Data

After ESP-

New IP header	ESP header	Original IP header	Data	ESP trailer	ESP ICV

Encrypted

Authenticated

Teacher's Sign.: _____

Page No.
Date

Q10) Write short note on VPN.

Ans a) Organizations setup internal and private network for use by its authorized users. Its resources are not accessible from public network such as the Internet. Increasingly the task force is becoming global and remote. Physical presence to access the organisation resources is no more effient. At the same time, the organization cannot risk exposing its internal resources over the public network.

b) A VPN is a data network that enables two or more parties to communicate securely across a public network by creating a private connection or tunnel between them.

c) The authorized users can then securely access the private network over the public network. Physical presence within organisation premises is not required to access the private network. The entire traffic between the private network is encrypted. IPSec can be one of the mechanisms for establishing a VPN connection.

Types of VPN -

1) Remote access VPN -

This is setup for remote users. They can access the private network securely over the public network.

Remote user ← Secure tunnel → Private network.

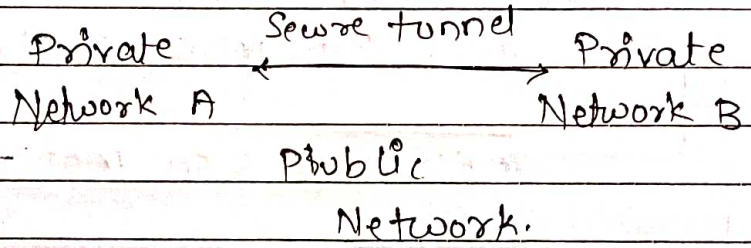
Pvt-Public network.

Teacher's Sign.: _____

2) site-to-site vpn -
This is established by the organization for connecting its multiple sites or branch offices so that the user can access the resources across the sites.

i) Intranet-based site-to-site VPN is used for organisation's own sites.

ii) Extranet-based site-to-site VPN is used for organization and its partners.



Q11) What is IKE? Explain with suitable block diagrams and phases.

Ans a) IKE is the protocol used to setup a Security Association (SA) in the IPSec protocol suite.

b) The following attributes are used by IKE and are negotiated as part of the ISAKMP Security Association:
Encryption algorithm. - DES, 3DES, AES, RC5
Hashing algorithm - MD5, SHA
Authentication method - RSA signature, DSS signature.
Information about a group over which to do Diffie-Hellman exchange.

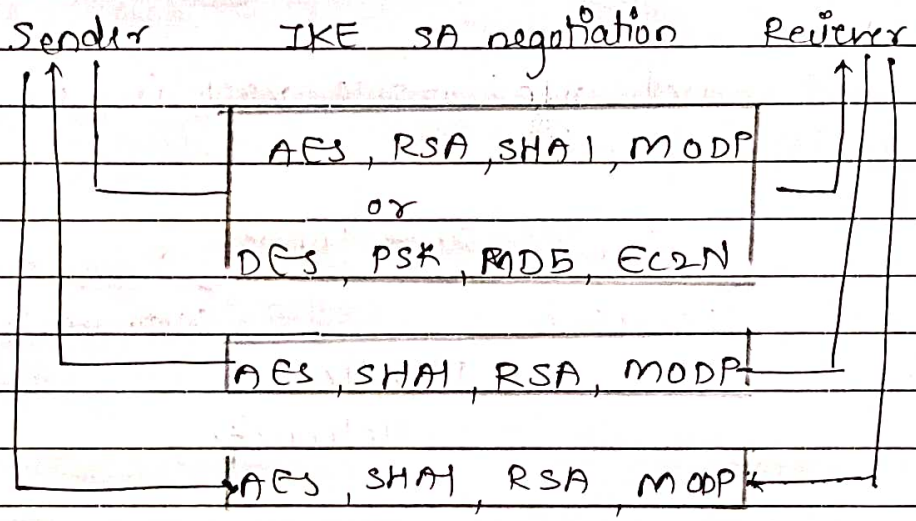
c) All of this attributes are necessary and must be negotiated between the communicating entities.

Teacher's Sign.: _____

Page No.
Date

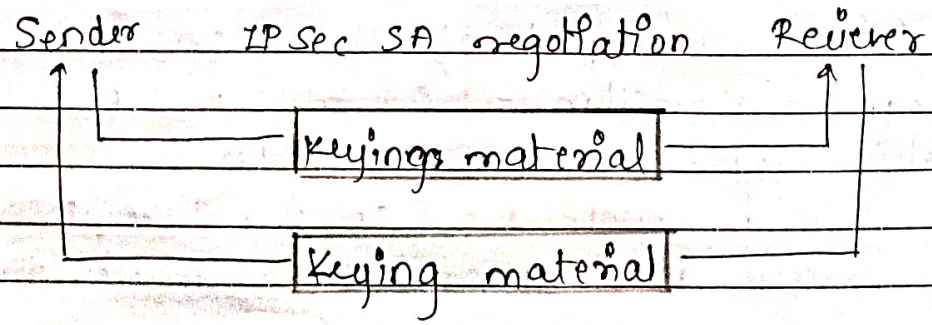
Phase 1 -

Mutual authentication of communicating entities.
Negotiating cryptographic parameters.
Creating session keys.



Phase 2 -

An IPSec tunnel is negotiated by creating key material for IPSec tunnel to use.



Teacher's Sign.: _____

Page No.
Date

Q12) Explain different protocols involved in SSL.

Ans a) SSL and TLS are the most widely use web security protocol.

b) SSL Record layer protocol:-

Its core function is to facilitate data transfer. The basic unit of data in SSL is a record. Each record consists of a five-byte record header, followed by data.

Types of SSL Records
1. Handshake Records
2. Change Cipher Spec Record.
3. Alert Records
4. Application Data Records.

SSL Record header-

SSL record type	SSL Major version	SSL Minor version	Length of data.
(1 byte)	(1 byte)	(1 byte)	(2 byte)

c) SSL Change Cipher Spec protocol-

Protocol consists of a single message, which is encrypted and compressed. It notifies the communicating parties about any change in the previously negotiated Cipher specifications or keys

The keys or the algorithms need to be changed at times for reasons such as renewing or resuming sessions. The change cipher spec message is sent by both the client and server to notify the otherparty about change

Teacher's Sign.: _____

Page No.
Date

d) SSL Alert protocol-
One of the content type supported by SSL record layer is alert type.

Alert message notify the
i) Severity of alert.
ii) Description of the alert.

Alert messages with a severity level of fatal result in immediate termination of connection. In this case other session corresponding to the session may continue, but the session identifier is invalidated, preventing the failed session from being used to establish new connections.

Alert record is of 2 bytes

Alert level (1 byte)	Alert code (1 byte)

e) SSL handshake protocol-
When an SSL client and server first start communicating, they need to agree upon certain parameters. There are also several steps that need to be carried out to establish a secured session. At high level the following four steps are carried out-

1. Agree on protocol version
2. Selet cryptographic algorithm
3. Optionally authentiate each other.
4. Use public key encryption technique to generate shared secrets.

Teacher's Sign.: _____

Page No.
Date

Q13) Write a note on S/MIME.

Ans a) S/MIME stands for Secure/ Multipurpose Internet mail extension.

b) It is based on certificates (Public key cryptography)

c) S/MIME services -

i) Provides following cryptographic services -
Authentication
message integrity
Non repudiation of origin
Message privacy and confidentiality
Message compression.

ii) S/MIME Algorithms -

	S/MIME services	Algorithms	Purpose
1.	Integrity	SHA-256, SHA1, MD5	Hashing
2.	Authentication, non-repudiation	RSA & DSA with hashing algorithms.	Digital signature
3	Key encryption	RSA, AES, Diffie-Hellman	Encrypting symmetric key
4.	Privacy and confidentiality	AES, DES, Triple DES	Message encryption.

Q14) Explain the working of SNMP.

←	Trap sent to NMS	←
NMS →	query sent to agent	→ Agent.
←	Response to query to NMS	←

Teacher's Sign.: _____

a) Two entities are involved in a SNMP managed network infrastructure - SNMP Managers and SNMP Agents.

b) SNMP Managers are often referred to as Network Management Stations (NMS). An NMS is responsible for polling and recieving traps from SNMP agents in the network. A poll in context of NMS is the act of quering an agent for some information. This can be used later to determine if some sort of catastrophic event has occurred. A trap is a way for the agent to tell the NMS that something has happened. Traps are sent asynchronously by agent on its own without queries from the NMS. The NMS is further responsible for performing an action based on the info recieved from the agent.

eg - When a router goes down, then it can send a trap to NMS informing about the same. In turn, the NMS can take some corrective actions automatically to fix the problem or notify network administrators who could look into the situation further and take the required action.

c) The second entity is SNMP agent-
It can be a separate program or it can be incorporated into the operating system. Today, most IP devices come with some kind of SNMP agent built-in. The fact that vendors are willing to implement agents in many of their products make the system administrators or manager's job easier. The agent provides management information to the NMS by keeping track of various operational aspects of the devices.

Teacher's Sign.: _____

For example, the agent on the router is able to keep track of the state of its interfaces and which ones are up, and which are down etc. This can be useful in determing when a problem situation is resolved. It is important to keep in mind that polls and traps can happen at same time. There is no restriction on when NMS can query the agent or when agent can send trap.

q15) How do the various elements of Network Access control system work together?

Ans

Elements of NAC

1. Access Requester (AR)
2. Policy Servers.
3. Network access servers (NAS)

a) Access requester (AR)-
The AR is the entity that is attempting to access the network resource. It could be any device that is ~~accessed~~ managed by the NAC system including workstations, servers etc.

b) Policy servers-
Based on AR's identity, authorization level, attempted request and organization's defined access policy, the policy server determines what access should be granted to AR.
The policy server often relies on backend systems, including antivirus, patch management to help determine

Teacher's Sign.: _____

the host's condition. An organisation defines various access policies to explicity allow or deny such access.

c) Network access server (NAS)-
NAS functions as an access control point for users in remote locations, connecting to an organisations internal network. Typically, these act as VPN and provide access to organisation's internal network.

d) The first step is generally to authenticate the AR. Authentication typically involves some sort of secure protocol and use of cryptographic keys. Authentication can be performed by NAS or authentication servers. In latter case, authentication takes place between the supplicant and authentication server that is part of policy server or that is accessed by policy server.

e) The authentication process serves a number of purposes. It verifies a supplicant's claimed identity, which enables the policy server to determine what access privileges, if any, the AR may have. The authentication exchange may result in the establishment of session keys to enable future secure communication between the supplicant and resources on the organisation's network.

f) Typically the policy server or a supporting server will perform checks on the AR to determine if it should be permitted interactive remote access conectivity.

Teacher's Sign.: _____

g) These checks should be performed before granting the AR access to organisation's network. Based on the results of these checks, the organization can determine whether the remote computer should be permitted to use interactive remote access.

Q16) What is computer intrusion? How can you detect and prevent it?

Ans a) Defined as tools, methods and resources to help identify, access, and report unauthorized or unapproved network activity.

b) An IDS detects activity in traffic that may or may not be intrusion.

c) IDSes can detect and deal with insider attacks, as well as, external attacks, and are often very useful in detecting violations of corporate security policy and other interal threats.

d) Host based intrusion detection-
Are usually installed on servers and are more focused on analyzing the specific operation systems and applications, resource utilization and other system activity residing on host-based IDS host.
It will log any activities it discovers to a seare database and check to see whether the events match any malicious event record listed in the knowledge base.

e) Network based ~~ist~~ intrusion detection-
Are dedicated network devices distributed within networks that monitor and inspect network traffic flowing through the device.
Instead of analyzing information that originates and

Teacher's Sign.: _____

resides on host, Network-based IDS uses packet sniffing techniques to pull data from TCP/IP packets or other protocols that are travelling along the network.

Q14) Explain firewalls and classification.

Ans a) Firewall is hardware or software tha to prevent a private computer or network of computers from unauthorized users from accessing private computers and networks.

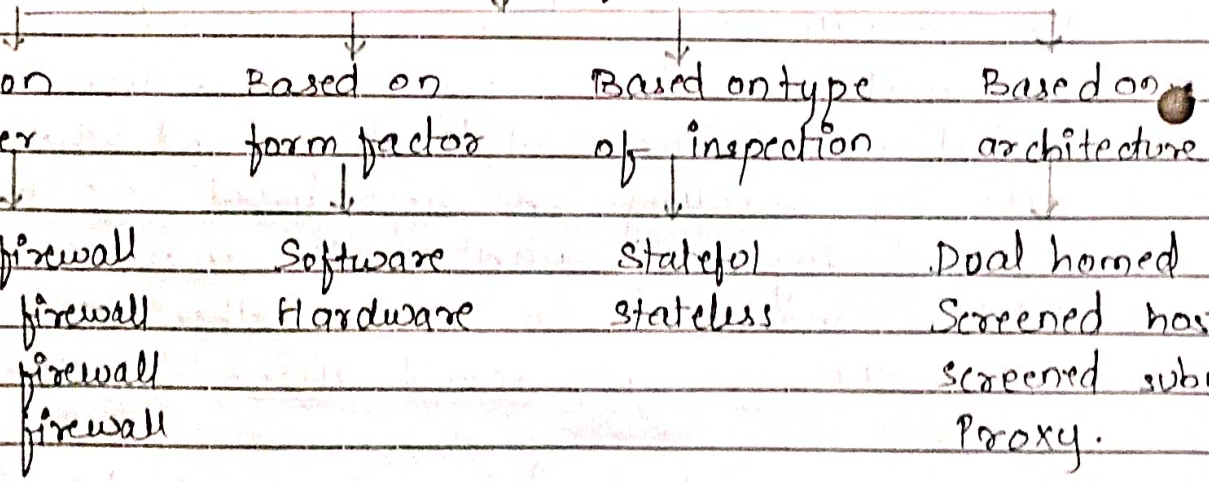
b) It is a vital component of network security. It is the first line of defense for network security.

c) It acts as barrier between internal private network and external sources.

d) Control flow of ~~net~~ network traffic.

e) Firewalls act on number of layers.

Classification of Firewalls.



Teacher's Sign.: _____