Assignment No. 6

Q1. What is need of Network Security?

Ans: Network Security refers to the measures taken by any enterprise or organisation to secure its computer network and data using both hardware and software systems. This aims at securing the confidentiality and accessibility of the data and network. Every company or organisation that handles large amount of data, has a degree of solutions against many cyber

threats.

Need of Network Security is as follows:

- Unless it's properly secured, any network is vulnerable to malicious use and accidental damage. Hackers, disgruntled employees, or poor security practices within the organization can leave private data exposed, including trade secrets and customers' private details.
- Losing confidential research, for example, can potentially cost an organization millions of dollars by taking away competitive advantages it paid to gain. While hackers stealing customers' details and selling them creates negative publicity and mistrust of the organization.
- Competent network security procedures keep data secure and block vulnerable systems from outside interference. This allows the network's users to remain safe and focus on achieving the organization's goals. More than that, it means that clients and partners can also interact with the organization confidently.

Q2. What are the threats in Network Security?

Ans:

- Information Security threats can be many like Software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion.
- Threat can be anything that can take advantage of a vulnerability to breach security and negatively alter, erase, harm object or objects of interest.
- Software attacks means attack by Viruses, Worms, Trojan Horses etc. Many users believe that malware, virus, worms, bots are all same things. But they are not same, only similarity is that they all are malicious software that behaves differently.
- Malware is a combination of 2 terms- Malicious and Software. So Malware basically means malicious software that can be an intrusive program code or anything that is designed to perform malicious operations on system.
- Theft of intellectual property means violation of intellectual property rights like copyrights, patents etc.

- Identity theft means to act someone else to obtain person's personal information or to access vital information they have like accessing the computer or social media account of a person by login into the account by using their login credentials.
- Theft of equipment and information is increasing these days due to the mobile nature of devices and increasing information capacity.
- Sabotage means destroying company's website to cause loss of confidence on part of its customer.

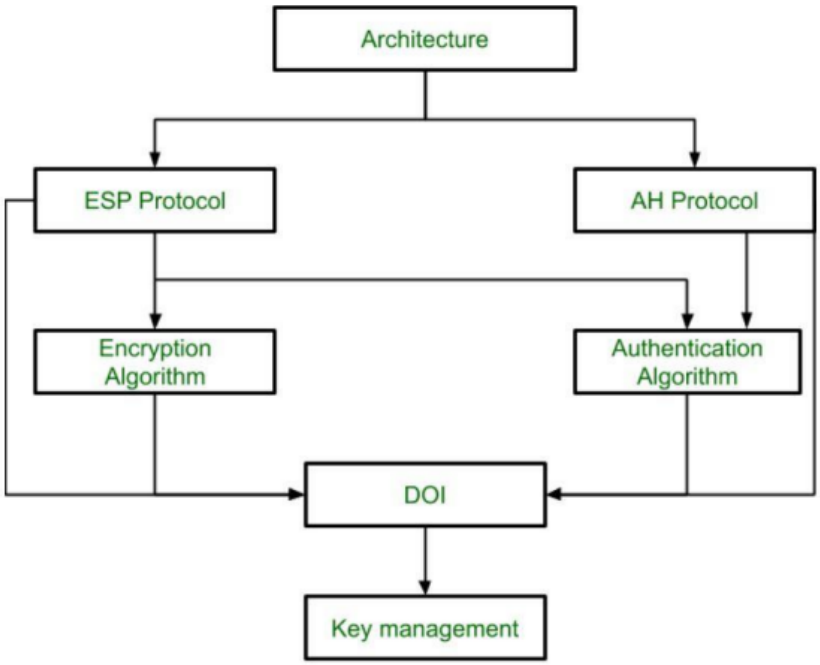
Q3. Define IP Security (IPSec) with IP Security Architecture.

Ans: The IP security (IPSec) is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.

IP Security Architecture:

IPSec (IP Security) architecture uses two protocols to secure the traffic or data flow. These protocols are ESP (Encapsulation Security Payload) and AH (Authentication Header). IPSec Architecture include protocols, algorithms, DOI, and Key Management. All these components are very important in order to provide the three main services:

- Confidentiality.
- Authentication.
- Integrity.



Q4. What are the different modes of operation?

Ans:

The IP security (IPSec) is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.

There are 2 modes of operation:

a.Tunnel Mode:

In tunnel mode, the entire original IP packet is encapsulated to become the payload of a new IP packet. Additionally, a new IP header is added on top of the original IP packet. Since a new packet is created using the original information, tunnel mode is useful for protecting traffic between different networks. An additional advantage of this mode is that it makes it very easy to establish a "tunnel" between two secure IPsec gateways.

b.Transport Mode:

The main difference in transport mode is that it retains the original IP header. In other words, payload data transmitted within the original IP packet is protected, but not the IP header. In transport mode, encrypted traffic is sent directly between two hosts that previously established a secure IPsec tunnel.

Since a new IP header isn't created, the process used by transport mode is less complex than tunnel mode.

Q5. Explain in Briefly:

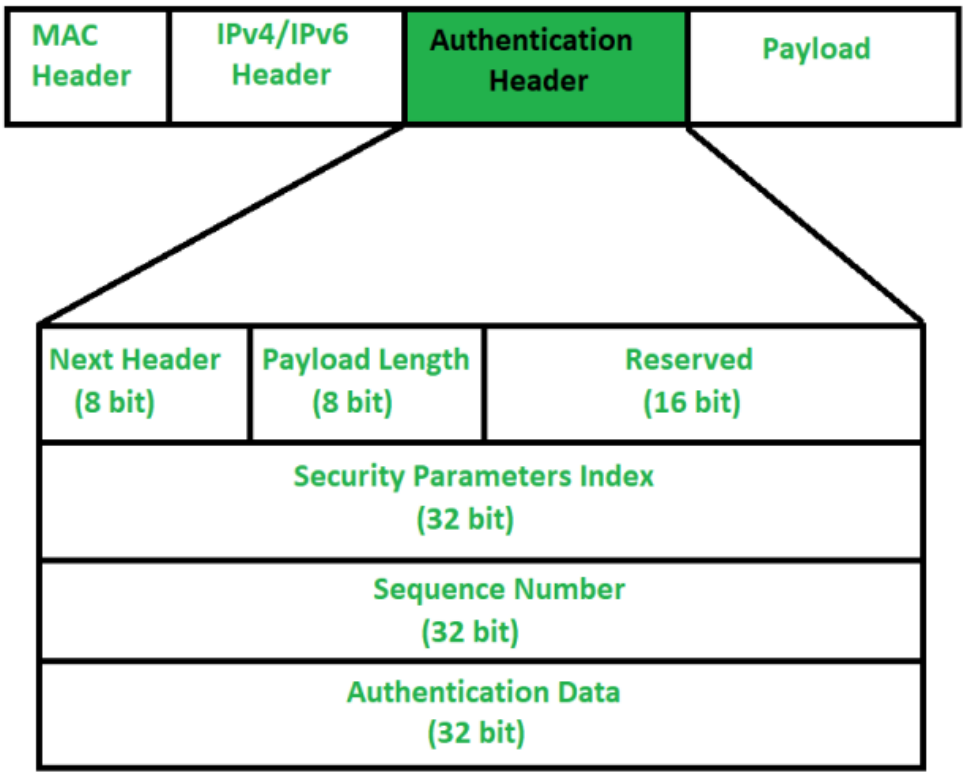
i)Authentication Header:

An Authentication Header or AH is a security mechanism used in authenticating the origins of datagrams (packets of data transmitted under Internet Protocol or IP conditions), and in guaranteeing the integrity of the information that's being sent. Authentication Headers are a protocol under the Internet Protocol Security (IPSec) suite.

IP Authentication Header is used to provide connection-less integrity and data origin authentication. There are two main advantages that Authentication Header provides:

- **Message Integrity:-** It means, message is not modified while coming from source.
- **Source Authentication:-** It means, source is exactly source from whom we were expecting data.

When packet is sent from source A to Destination B, it consists of data that we need to send and header which consist of information regarding packet. Authentication Header verifies origin of data and also payload to confirm if there has been modification done in between, during transmission between source and destination.



ii)Encapsulating Security Protocol:

The Encapsulating Security Payload (ESP) protocol provides data confidentiality, and also optionally provides data origin authentication, data integrity checking, and replay protection.

The difference between ESP and the Authentication Header (AH) protocol is that ESP provides encryption, while both protocols provide authentication, integrity checking, and replay protection. With ESP, both communicating systems use a shared key for encrypting and decrypting the data they exchange.

You can apply ESP in two ways: transport mode or tunnel mode:

Transport mode does not authenticate or encrypt the IP header, which might expose your addressing information to potential attackers while the datagram is in transit. Transport mode requires less processing overhead than tunnel mode, but does not provide as much security. In most cases, hosts use ESP in transport mode.

Tunnel mode creates a new IP header and uses it as the outermost IP header of the datagram, followed by the ESP header and then the original datagram (both the IP header and the original payload).

Q6. Explain the security association (SA) concept in IP Sec.

Ans: The concept of a security association (SA) is fundamental to IPSec. An SA is a relationship between two or more entities that describes how the entities will use security services to communicate securely. IPSec provides many options for performing network encryption and authentication. Each IPSec connection can provide encryption, integrity, authenticity, or all three. When the security service is determined, the two IPSec peers must determine exactly which algorithms to use.

After deciding on the algorithms, the two devices must share session keys. As you can see, there is quite a bit of information to manage. The security association is the method that IPSec uses to track all the particulars concerning a given IPSec communication session. You will need to configure SA parameters and monitor SAs on Cisco routers and the PIX Firewall.

ach SA consists of values such as destination address, a security parameter index (SPI), the IPSec transforms used for that session, security keys, and additional attributes such as IPSec lifetime. The SAs in each peer have unique SPI values that will be recorded in the Security Parameter Databases of the devices. The Security Parameter Database is set up in dynamic random-access memory (DRAM) and contains parameter values for each SA.

Q7. Explain Internet Key Exchange process in details.

Ans: Internet Key Exchange (IKE) is a key management protocol standard used in conjunction with the Internet Protocol Security (IPSec) standard protocol. It provides security for virtual private networks' (VPNs) negotiations and network access to random hosts. It can also be described as a method for exchanging keys for encryption and authentication over an unsecured medium, such as the Internet.

IKE is a hybrid protocol based on:

- ISAKMP:- Internet Security Association and Key Management Protocols are used for negotiation and establishment of security associations. This protocol establishes a secure connection between two IPSec peers.
- Oakley:- This protocol is used for key agreement or key exchange. Oakley defines the mechanism that is used for key exchange over an IKE session. The default algorithm for key exchange used by this protocol is the Diffie-Hellman algorithm.
- SKEME:- his protocol is another version for key exchange.

IKE enhances IPsec by providing additional features along with flexibility. IPsec, however, can be configured without IKE.

IKE has many benefits. It eliminates the need to manually specify all the IPSec security parameters at both peers. It allows the user to specify a particular lifetime for the IPsec security association. Furthermore, encryption can be changed during IPsec sessions. Moreover, it permits certification authority. Finally, it allows dynamic authentication of peers.