Please list the 4x basic attached and provide an example of each Basic attack.

- ⇨ The four basic attacks are:
  1. Snooping refers to unauthorized access to someone else's data or information. An example of snooping is when an attacker intercepts and reads sensitive information, such as login credentials or financial data, transmitted over an unencrypted network.

  2. Modification: Modification involves unauthorized changes made to data or information. For instance, an attacker could modify the content of an email or web page to deceive the recipient into clicking on a link or entering sensitive information.

  3. Masquerading: Masquerading, also known as impersonation, is when an attacker pretends to be someone else to gain access to a system or information. For example, an attacker might use stolen login credentials to impersonate a legitimate user and gain access to sensitive data or systems.

  4. Denial of service (DoS): A DoS attack aims to disrupt or disable access to a network or system. An example of a DoS attack is flooding a web server with excessive traffic, rendering it unavailable to legitimate users.

Question no.2

Comparing SSL and SET.

- ⇨ SSL (Secure Sockets Layer) and SET (Secure Electronic Transaction) are security protocols that provide secure communication over the Internet. However, there are some critical differences between the two:
  a) Purpose: SSL is primarily designed to provide secure communication between web browsers and servers. It encrypts the data exchanged between the two, ensuring confidentiality and integrity. On the other hand, SET is specifically designed to provide secure online payment transactions.
  b) Adoption: SSL is widely used by millions of websites to provide secure communication. On the other hand, SET has yet to be as widely adopted, and its use is limited mainly to payment processing.

Question no.3

What's the difference between IPSec transport mode and tunnel mode?

- ⇨ IPSec transport mode is used to encrypt the payload of an IP packet while leaving the IP header unencrypted. It is typically used for secure communication between two hosts on the same network. Transport mode provides end-to-end encryption between two hosts, but it only encrypts the data being transmitted and not the IP header. This mode is efficient and requires less processing and bandwidth than tunnel mode.

IPSec tunnel mode is used to encrypt the entire IP packet, including both the original IP header and the payload data. It is typically used for secure communication between two networks. In tunnel mode, the original IP packet is encapsulated within a new IP packet, and the original IP header is encrypted. The added IP header contains the necessary information to route the packet to its destination network, while the original header is only visible within the private network. Tunnel mode provides more comprehensive security than transport mode, but it is less efficient and requires more processing and bandwidth.

What are the benefits of IPSec?

⇨ The benefits of IPSec are:

a) Provide strong security if IPSec is implemented in a firewall or router.
b) IPSec in a firewall is resistant to bypass if all traffic from the outside must use IP. The firewall is the only means of the entrance from the Internet into the organization.
c) IPSec is below the transport layer (TCP, UDP) and is transparent to applications.
d) IPSec can be transparent to end users.
e) IPSec can provide VPN for individual users.

Where do we use the dual sign?

- ⇨ Dual sign, or dual control, ensures that multiple individuals authorize sensitive transactions or operations. It is commonly used in financial transactions and other sectors requiring a high-security level.

Please list 3x Trust Model and details.

- ⇨ The three Trust Models are:
  a) Direct trust: This model is based on personal knowledge and trust relationships between individuals. It involves establishing trust between individuals directly, without relying on any intermediaries. Direct trust is commonly used in social networks, where users can establish trust relationships with their friends based on their personal experiences.

  b) Hierarchical Trust: This trust model is based on a hierarchical structure, where trust is established through a chain of intermediaries. It involves delegating trust from higher-level entities to lower-level entities, with each level vouching for the trustworthiness of the entities below it. Hierarchical trust is commonly used in organizational structures, where individuals are granted access based on their position and level of trust within the organization.

c) Web of trust: This trust model is based on a decentralized network of trust relationships between individuals. It involves establishing trust relationships between individuals who are not directly connected, but who are connected through a network of trusted intermediaries. Web of trust is commonly used in public key infrastructure (PKI) systems, where individuals can verify the identity of others based on their trust relationships with other trusted parties.