**DISTRIBUTED OPERATING SYSTEMS**
**ASSIGNMENT**
**VASU NEGI**
**UFID: 8495-3933**

**Interception:**

This means that some unknown or malicious person has gained the access to the system. The person can copy the files to his own computer, or wiretap to gain secret information from the network.

**Interruption:**

In this attack, the system is taken down by the attacker, where the system like a service/ program is made unavailable to the web/net. Some of the examples, include deleting a file/service or making the OS not able to access a specific disk.

**Modification:**

The hacker can change the service or resource of the system such as some hacker can change the database of the system, change the program so that it does some extra computation and send information to unknown parties.

**Fabrication:**

The hacker can create/insert fake data into the system. This is particularly important in financial databases where fake transactions created by hacker can pose a great security threat.

**Intrusion Detection:**

It is a system/program which monitors the system for any malicious attacks from the correct transactions. Any violation is reported back to the system and any precaution is taken at the same time such as blocking the user. However, the intrusion detection does not work as it should and is not reliable as after an attacker is into the system, it is very hard to distinguish between the attacker and the other transactions.

**Encryption:** Encryption is the key to everything.

PGP (Pretty good Privacy): PGP is an encryption which is used for sending files and email over the network in an encrypted fashion. This system uses public key symmetric encryption and allows strangers to share files securely over the network.

**Diffie Hellman Key Exchange:**

It is a method of exchanging keys (cryptographic) over the network and uses public key exchange. This key can also be used to encrypt further files or resources. This service provides various authentication protocols and provides security in TLS.

**Symmetric Encryption:**

It is a type of technique where only one key is used to encrypt and decrypt the message rather than two separate keys (public and private in asymmetric). In Encryption the data is converted to any form that is not readable by another entity until decrypted which is done using the key.

AES (**Advanced Encryption Standard**) is a specification for encryption which provides symmetric key and public key encryption used to encrypt and decrypt the message. It is based on substitution permutation network in which a block size of 128 bits and a key size of 128, 256 bits is used (preferred by army).

DES (**Data Encryption Standard**) is a specification for encryption which provides symmetric key and public key encryption used to encrypt and decrypt the message. It uses key of 56 bits which is considered insecure. DES can be broken on a laptop in 24 hrs.

3-DES: It is a technique for encrypting messaging where DES is used three times in a row. 2 -DES is as easy to break a DES.

**Secure Hash Algorithms:**

**SHA-1**: It is a 160-bit hash function which is similar to the md5 algorithm.
**SHA-2**: It has two hash functions SHA-256 and SHA-512, where 32-byte word size is used in the SHA-256 and 64-byte word size in the SHA-512.

**Public Key Cryptography:**

Public Key Cryptography is a technique where the system uses public keys and private keys. The public key is openly distributed, and private key is private with the receiver. The person can encrypt the message using public key and can be only decrypted using the private key.