Name: **Mareena Fernandes**
Roll No.: **8669**
Class: **TE IT**
Batch: **B**

ASSIGNMENT NO: 2

**1. Classify network attacks according to sabotaging of resources, bandwidth exhaustion and connectivity.**

Ans:
Unauthorized access: It refers to attackers accessing a network without receiving permission. Among the causes of unauthorized access, attacks are weak passwords, lacking protection against social engineering, previously compromised account and insider threats.
The attacker can sabotage all the resources from the network and deplete the whole bandwidth of the network by sending large chunks of data.

DDOS: In a network layer attack, attacker sends a large amount of packets to saturate limited bandwidth or exhaust the network resources of a victim. Network resources like routers, servers and firewalls have a finite capacity when they are attacks and overloaded, end-users will not be able to get through because there is either no bandwidth left for them to use or the network infrastructure systems themselves all overwhelmed.
The DDOS attack will tell the limits of a web server, network and application resources by sending spikes of fake traffic. When it is launched, the botnet will attack the target and deplete the application resources.

Man in the middle attacks: A MIM attack involves attackers intercepting traffic, either between your network and external sites or within your network. If communication protocols are not secured or attackers find a way to invade that security, they can steal data that is being transmitted, obtain users credentials and hijack their sessions.

Code and SQL injection attacks: Many websites accept user IP and fail to validate and sanitize those IPs. Attackers can fill out a form or make an API call, paring indicious code instead of expected data values. The code is executed on the server and allows attackers to compromise it. In many cases, attacker can modify, delete this data and cause changes to application content or behavior. But there is no bandwidth exhaustion of the user.

**2. Differentiate between various internet security protocols.**

Ans:

| IP Sec | SSL |
|---|---|
| IP Sec is a set of protocols that provide security for Internet Protocol. | SSL is a secure protocol developed for sending information securely over the internet. |
| It works in internet layer of OSI model. | It works in between the transport layer and application layer of OSI model. |
| Configuration is complex. | Configuration is simple. |
| Used to secure a virtual private network. | Used to secure web transactions. |
| Installation process is vendor non-specific. | Installation process is vendor specific. |

**3. Give significance of different types of honeypot.**

Ans:
A honeypot is a security mechanism that creates a virtual trap to lure attackers. You can apply a honeypot to any computing resources from software and networks to file servers and routers.

2 types of Honeypot designs:

- Production honeypot serves as decoy systems inside fully operating networks and servers, often as a parted-on IDS.
- Research honeypots are used for educational purposes ad security enhancement. They contain trackable data that you can trace when stolen to analyze the attack.

3 types of Honeypot replacement:

- Pure honeypot: Complete production systems that monitor attacks through bug taps on the link that connects the honeypot to the network they are unsophisticated.
- Low-interaction honeypot: Imitate services and systems that frequently attract criminal attention. They offer a method for collecting data from blind attacks such as botnets and worms malware.
- High-interaction honeypots: Complex setups that behave like real production infrastructure. They don’t restrict the level of activity of a cyber-criminal, providing extensive cyber security insights. However, they are higher maintenance and require expertise and use of additional technologies like virtual machines to ensure attackers cannot access to the real system.

**4. How can you achieve confidentiality and integrity for messages over internet?**

Ans:

The basis security mechanics are confidentiality integrity and availability.

- Confidentiality: The capability to send (and receive) data without divulging any part to unauthorized entities during the transmission of data.
  Mechanisms: Encryption? Symmetric and Asymmetric
  Confidentiality is achieved using data encryption. Encryption can be done using either the symmetric key paradigm or the asymmetric key paradigm.
  1. Symmetric Key Encryption, often referred to as secret key encryption, use a common key and the same cryptographic algorithm to scramble and unscramble a message.
  2. Asymmetric Encryption is often referred to as public key encryption. It can use either the same algorithm or different but complimentary algorithm scramble and unscramble data. Two different but related key values are required: a public key and a private key it can only be decrypted using the private key (and vise versa)
- Integrity: The capability to send (and receive) data such that unauthorized entities cannot change any part of the exchanged data without the sender/ receiver detecting the change. Informally integrity mechanics are in place, data can be changed, but integrity will detect tempering.
  Mechanisms: Digital Signatures using one-way hash functions.
  Integrity mechanism are aimed at detecting any changes to a set of bytes. Digital signatures used the hash functions mechanism and encrypt the resultant hash
  A hash function takes an input message of arbitrary length and outputs fixed length-code. The fixed length output is called a hash.
  A digital signature is an encrypted message digest that is appended to a document. It can be used to confirm the identity of a sender and integrity of the document. They are based on the combination of a public key encryption and one-way hash functions.

**5. Ecommerce company is facing an issue getting online orders from customers compared to previous quarter. Find out different attacks which could be responsible for this case and give solution for the same.**

Ans:

The E-Commerce company may might be facing the following attacks:

- MAJOR THREAT – DIRECT SITE ATTACKS
  - While phishing is a passive approach, E-Commerce sites can be sometimes be subjected to direct attacks in the form of DDOS.
  - How it works?
    Those who want to put a store under siege will program many internet capable devices to near constantly attempt to use the store site. The attack will overwhelm the stores hosting. Example: Prevent the site from loading for most, especially regular visitors.

Solution: Active protection
DOS Protection service: The concept includes:
Incoming traffic is monitored and passed at when visit request are considered to be fraud in nature, they are entirely blocked.

- BRUTE FORCE ATTACK
  - Brute force attack targets an online stores admin panel.
  - They want to out the password and gain access, the directions of the attack make it brute force.
  - After using software to connect to a site, it uses code-crunching program to crack passwords by using every possible combination imaginable.

Solution: Protect your system by creating strong and complex passwords, changing them regularly.

- PHSIHING:
  - A social Engineering attack is the most infamous hack to manipulate human psychology.
  - Receiving fake "you must take action" emails, either to your company or customer a widely used play or form of trickery used by hackers.
  - It does require follow-throw and unintentionally offering up log in information as personal identification information.

Solution: Employee training and educating consumers.

- BOTS:

Bots can be good or bad. The bad bots scrape websites too for inventory information and alter price on a site, freeze popular items in shipping carts, and thereby damage site scale and revenue.
Solution: To protect exposed APIs and mobile apps and examine traffic sources regularly looking for spikes and then blocking those hosting providers and proxy services.

- MALWARE:

Malware are those that use malleating, consumes, cross-site scripting, SQL injections, targeting credit card info and personal data.
Solution: Those professional activities and anti-malware software to HTTPS, secure servers and admin panels and use SSL certificates while using or employing multilayer security.

**6. Differentiate between different digital signature schemes.**

Ans:
Some digital signature schemes are:

1. RSA – It is an asymmetric cryptography algorithm that works on 2 different keys: public and private. As the name suggests public key is given to everyone and private key is kept private.
2. Elgamal – It is a public key cryptography system. It uses asymmetric key encryption for communicating between two parties and encrypting the message. This cryptography system is based on the difficulty of finding discrete logarithm in a cyclic group.
3. Robin Cryptosystem – It is a public key cryptosystem invented by Michael Robin and it uses asymmetric key encryption for communicating between two parties and encrypt the message. The security of Robin Cryptosystem is related to the difficulty of factorization.
4. Schnorr Signature – It is a digital signature scheme knows for its simplicity and is efficient and generates short signatures. It is one of the protocols used to implement "Proof of knowledge". In cryptography, a proof of knowledge is an interactive proof in which the prover succeeds in 'convincing' a verifier knows something.
5. DSS – Digital Signature Standard is a FIPs which defines algorithms that are used to generate digital signatures with the help of SHA algorithm for authentication of electronic documents. DSS only provides us with the digital signature function and not with any encryption or key exchanging strategy.