A close-up of a document

Description automatically generated

1)Define the terms.

Steganography – Greek for covered writing .

It is the art and science of disguising the existence of a message.

2) Also for each term, further illustrate concept by choosing closely connected IT security concept and explain relationship between the concepts.

3)Give an example of an application of these tools/threats/concepts.

Structure answer with headings definition, relation to chosen concept and example.

To say more about steganography , should compare this to cryptography, which is a similar sort of idea.

Example – Use a JPEG picture and a special software to insert a message into the JPEG picture,it makes little difference to picture.

You cannot notice from looking at the picture that there is a difference between one that has message inside it and one that doesn’t.

With special software should be able to extract message.

DMZ – separates a completely internal network from an external network (like the internet.

**DMZ (Demilitarized Zone)**: A DMZ in network security is a physical or logical sub-network that separates an organization's internal local area network (LAN) from untrusted external networks, typically the internet.

The DMZ provides an additional layer of security and is used to host external-facing services, such as web servers, email servers, and DNS servers. The goal of a DMZ is to improve security by segmenting the network so that if a cyber attacker compromises a server in the DMZ, the attacker would still have to breach additional security measures to access the internal network.

What’s an example of a DMZ

**Social Engineering**

**Definition**: Social engineering is the psychological manipulation of people into performing actions or divulging confidential information.

It’s a type of confidence trick for the purpose of information gathering, fraud, or system access.

**Relationship to 'Phishing'**: Phishing is a specific type of social engineering where attackers masquerade as a trustworthy entity in an electronic communication. Social engineering is the broader category of these deceptive tactics, while phishing is a digital execution of social engineering.

**Example**: An example of social engineering is an attacker calling an employee and pretending to be an IT support person, convincing the employee to reveal their login credentials.

**Biometric Authentication**

**Definition**: Biometric authentication is a security process that relies on the unique biological characteristics of an individual to verify their identity. It can include fingerprints, facial recognition, iris or retina scans, voice recognition, and even DNA.

**Relationship to 'Access Control'**: Access control systems are the mechanisms that manage access to resources in a computing environment. Biometric authentication is often used as a secure method of access control, relying on unique personal features to grant or deny entry.

**Example**: A common example is using a fingerprint scanner on a smartphone to unlock the device or authenticate payments.

**Steganography**

**Definition**: Steganography is the practice of hiding a message, image, or file within another message, image, or file. Unlike cryptography, which obscures the content of a message, steganography conceals the existence of the message.

**Relationship to 'Cryptography'**: While both are used to protect information, cryptography encrypts the message so it cannot be understood if intercepted, whereas steganography hides the message so it isn't apparent there is a message at all.

**Example**: An example of steganography is hiding a secret text message within the least significant bits of an image file, so the image appears normal to the casual observer.

**DMZ (Demilitarized Zone)**

**Definition**: In network security, a DMZ or demilitarized zone is a physical or logical subnetwork that contains and exposes an organization’s external-facing services to an untrusted network, usually the internet. It acts as a buffer zone between the public and the internal network.

**Relationship to 'Firewall'**: A firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. A DMZ is often placed between firewall layers to add an additional layer of security and to segregate the external service traffic from internal network traffic.

**Example**: A web server hosting a company’s website might be placed in the DMZ. This allows external users to access the website while keeping the internal corporate network secure from direct access from the internet.

Phishing

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack, or the revealing of sensitive information.

Here's a step-by-step breakdown of how phishing works:

1. **Disguise**: The attacker chooses a disguise. They might pretend to be a bank, a corporate entity, an internet service provider, a colleague using a compromised email account, or any other entity that could plausibly contact the target.
2. **Communication**: The attacker crafts a message to resemble legitimate communications from the disguised entity. This message will usually incite urgency, fear, or similar emotions in the victim, prompting them to act quickly.
3. **Malicious Link**: The message includes a link to a fake website that closely resembles the legitimate one. The site is designed to trick the victim into entering personal information, such as passwords, credit card numbers, or social security numbers.
4. **Information Capture**: Once the victim enters their information, it is sent to the attacker's server, where it can be used for fraudulent purposes.
5. **Consequences**: The immediate consequence of phishing can range from unauthorized purchases and the stealing of funds to identity theft and beyond.

Phishing attacks can be very sophisticated, making it crucial for users to remain vigilant when handling unexpected or suspicious emails and messages. Common indicators of phishing attempts include spelling and grammar mistakes in emails, URLs that are similar but not identical to the official ones (often using a technique known as typosquatting), and email addresses that mimic legitimate ones but often have subtle differences.

Top of Form