Unit-1 Security in computing environment

Network Security

- Types of Network Security Devices. These security devices block the surplus traffic.
- Firewalls. A firewall is a network security system that manages and regulates the network traffic based on some protocols.
- Antivirus. An antivirus is a tool that is used to detect and remove malicious software.
- Content Filtering.
- Intrusion Detection Systems.

Computer security, **cybersecurity** or **information technology security** (**IT security**) is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

The field is becoming increasingly significant due to the increased reliance on computer systems, the Internet[2] and wireless network standards such as Bluetooth and Wi-Fi, and due to the growth of "smart" devices, including smartphones, televisions, and the various devices that constitute the "Internet of things". Owing to its complexity, both in terms of politics and technology, cybersecurity is also one of the major challenges in the contemporary world.

All security threats are intentional i.e. they occur only if intentionally triggered. Security threats can be divided into the following categories:

- **Interruption**

  Interruption is a security threat in which availability of resources is attacked. For example, a user is unable to access its web-server or the web-server is hijacked.

- **Privacy-Breach**

  In this threat, the privacy of a user is compromised. Someone, who is not the authorized person is accessing or intercepting data sent or received by the original authenticated user.

- **Integrity**

This type of threat includes any alteration or modification in the original context of communication. The attacker intercepts and receives the data sent by the sender and the attacker then either modifies or generates false data and sends to the receiver. The receiver receives the data assuming that it is being sent by the original Sender.

- **Authenticity**

  This threat occurs when an attacker or a security violator, poses as a genuine person and accesses the resources or communicates with other genuine users.

Types of Network Security Attack

1. **Trojan Horse.** A Trojan horse is a malicious program that appears to be useful and installed on a computer. Because of...
2. **Malware**. Malware attacks are among the most serious cyberattacks designed especially to disable or access a targeted...
3. **Botnet**. It's a private computer network that is a victim of malware. By knowing the user, the hacker controls all...
4. **Man in The Middle.** A man in the middle attack is someone standing between you and the other personal interaction.
5. **Packet Sniffer**-If a passive receiver is mounted on the wireless transmitter's land, it will store copies of each transmission packet. Such packages may include confidential information, sensitive and critical information, commercial secrets, etc. It will get through it when it flies across a packet receiver. The receiver acts as a sniffer to the packet and then sniffs all the packets that are sent to the sector. Cryptography is the most effective protection against sniffers.
6. **IP Spoofing**-This method uses a fake source address to insert packets into the Internet and is one way to masquerade them as another user. End-point authentication which guarantees that a message from the location we have decided is certain would help to protect against IP spoofing.
7. **DOS (Denial of Service)**- A Denial-of-Service is a critical attack that completely or partially kills the victim's network or the IT infrastructure to block authorized users from accessing it. The Dos attack divided into three parts which are as follows:

- **Bandwidth Flooding:** Through sending a cascade of packets the terrorist attacker can block valid packets from accessing the server. The transmitted packets are wide so that the connection for other people is blocked.
- **Vulnerability Attack:** When a few well-formed messages are sent to the insecure operating system or to the device on the target server, the service fails or gets worse if the host collapses.
- **Connection Flooding:** By creating large numbers of TCP connections on the targeted server, the attacker is bogging down. These fake connections block the network and prevent legitimate users from using it.

8. **DISTRIBUTED Denial of Service**-The dos attack is a complicated version and much harder to detect and protect than a dos attack. The attacker uses multiple compromised systems to target a single targeted dos attack system. In this assault. The assault from DDOS even lifts botnets.
9. **Worm**-Without user support, a worm will reach a computer. If a user runs a vulnerable network program, a malware attacker may send malware to that application on the same Internet connection. The application will accept and execute malware from the internet to build a worm.
10. **Virus**-A virus can not run itself; the interaction between the user and the machine is needed in order to infect and spread across the network. An example is an email containing a malicious link or an attachment. The malicious code triggers or eliminates system security controls when a receiver opens the attachment or clicks the connection. It is inefficient. In this scenario, the user corrupts the computer inadvertently.

Security services

- **Authentication**: assures recipient that the message is from the source that it claims to be from.
- **Access Control:** controls who can have access to resource under what condition
- **Availability**: available to authorized entities for 24/7.
- **Confidentiality**: information is not made available to unauthorized individual.

Information Security

Computer security, **cybersecurity** or **information technology security** (**IT security**) is the protection of computer systems and networks from information

disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

It is basically the **practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information**. Information can be physical or electronic one.

What are the 3 Principles of Information Security? The basic tenets of information security are **confidentiality, integrity and availability**. Every element of the information security program must be designed to implement one or more of these principles. Together they are called the CIA Triad.

IT security is a set of cybersecurity strategies that prevents unauthorized access to organizational assets such as computers, networks, and data. It **maintains the integrity and confidentiality of sensitive information**, blocking the access of sophisticated hackers.

It relies on five major elements: **confidentiality, integrity, availability, authenticity, and non-repudiation**.

One of the most secure encryption types, **Advanced Encryption Standard (AES)** is used by governments and security organizations as well as everyday businesses for classified communications. AES uses "symmetric" key encryption. Someone on the receiving end of the data will need a key to decode it.

Methods of protection in computing environment

- Application security. Secure coding. Secure by default. ...
- Computer access control. Authentication. Multi-factor authentication. ...
- Computer security software. Antivirus software. ...
- Data-centric security.
- Code obfuscation.
- Encryption.
- Firewall.
- Intrusion detection system. Host-based intrusion detection system (HIDS)

Follow these tips to protect your devices and safeguard your sensitive data:

- Use a firewall. ...
- Install antivirus software. ...
- Install an anti-spyware package. ...
- Use complex passwords. ...
- Keep your OS, apps and browser up-to-date. ...
- Ignore spam. ...
- Back up your computer. ...
- Shut it down.

E-Mail Security:-

Email security is a term for **describing different procedures and techniques for protecting email accounts, content, and communication against unauthorized access, loss or compromise**. Email is often used to spread malware, spam and phishing attacks.

E-mail security can be defined as the use of various techniques to keep sensitive information in email communication and accounts secure. These precautions are taken chiefly against unauthorized access, loss, or compromise. It allows an individual or an organization to protect the overall access to one or more email addresses or accounts.

Some of the proactive email security measures, from an end user's standpoint, include:

1. Strong passwords
2. Password rotations
3. Spam filters
4. Desktop-based anti-virus or anti-spam application

Types of Email Threats

- Malware Delivery via Spam. Malware is one of the most serious yet common threats that are commonly delivered through emails.
- Credential Theft via Phishing Emails.
- Business Email Compromise.
- Malicious Bot and DDoS Attacks.
- Authentication Attacks on Email Servers.
- Vulnerabilities in Email Servers.

Threats To Email Security:

1. Phishing

Email phishing is a security attack used by cybercriminals who use it in an attempt to steal sensitive business information. This type of data includes usernames and passwords of CEOs, CFOs and other senior management, details about financial accounts or valuable information which can be sold to competitors.

Phishing emails are often masked by official emblems of the company and usually target vulnerable accounts and lower-level employees. In most cases, these malicious emails contain links to sites that dispense malware. The best protection against such an attack is a surveillance network that monitors communication in and out of the company.

2. Spoofing

A spoofing email is a strategy used during spam and phishing attacks. By falsifying the header of an email to make it seem like its coming from inside the company, an attempt is made to confuse employees to provide sensitive information or in some cases even bank transfers.

While due diligence is the best method of dealing with spoofing attacks, companies should also look to software which improves **email security** for enterprises.

3. Malware

Malware, or malicious software, is a virus which contains coding programmed to attack and harm data, tech equipment or entire systems. Trojans,

viruses, spyware, worms, adware, botnets and ransomware are all types of malware, but so far, the list includes 796 million registered malware programs. In most cases, malware is via email during phishing and spam attacks. During an attack, multiple emails with a virus are sent across an enterprise. After being opened, malware infects the system and cause damage to it.

Teaching company employees is the first line of malware defense. If someone receives an email from an unknown source and with a large attachment, it is best they delete the mail immediately.

4. Ransomware

Ransomware is a specific type of malware which attacks the entire computer system and blocks access to users until the financial demand (ransom) is paid to the perpetrator. **Threats to email security** like this usually happen during other large-scale attacks when multiple users are targeted inside the company.

To preventing ransomware from harming your business system, a company's CTO will need to take several steps:

- Regularly patch and update operating systems;
- Periodically backup files and other data;
- Install software which limits administrative privileges to all users;
- Install and periodically upgrade firewalls and antivirus software;
- Integrate advanced **email security for enterprise**

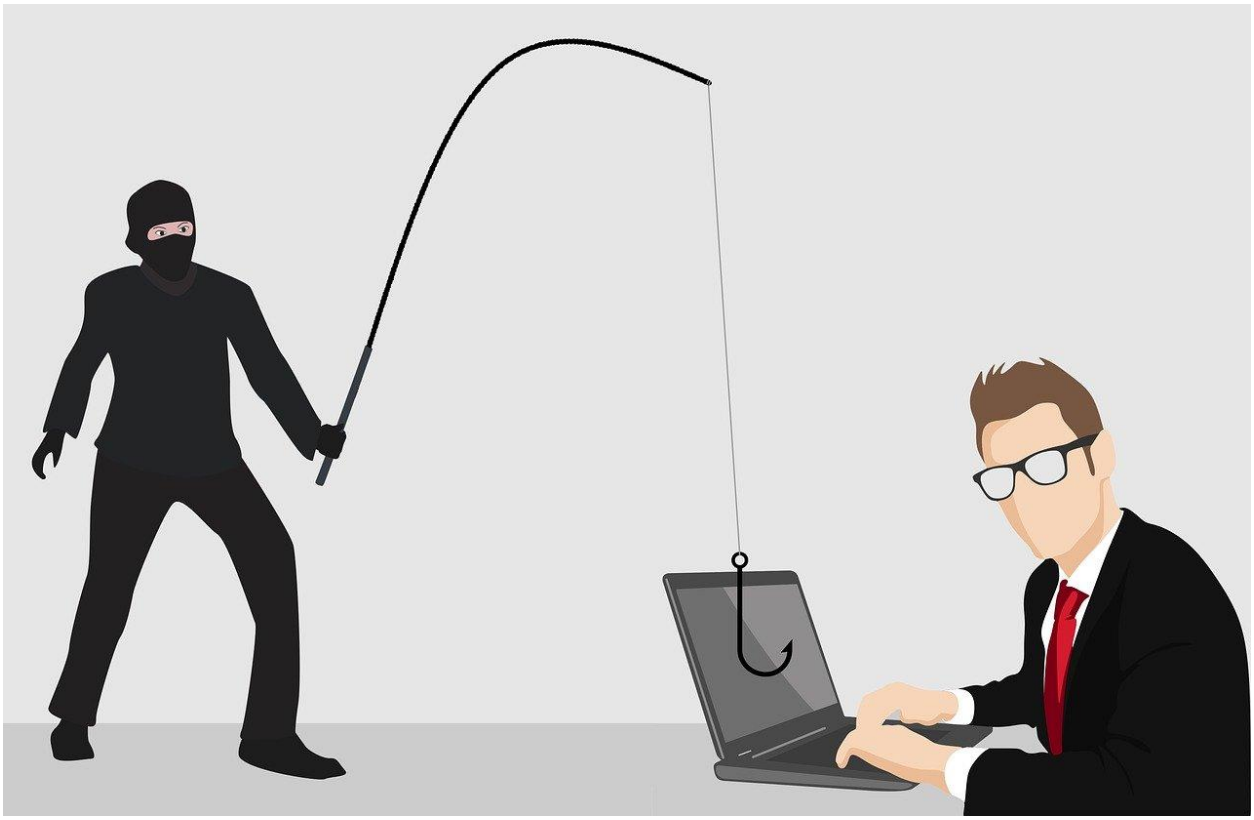
5. Directory Harvest Attacks

A directory harvest attack (DHA) is an **email** threat carried out by spammers which has a goal of accessing the email database attached to a company domain. Although simple tactics like a dictionary attack are used, DHAs target both personal and commercial information, inflicting massive damage across a large enterprise.

Using a Mail Protection Service (MPS) protects email accounts from any DHA attempts. By integrating the DHA feature onto the security server, technical staff will receive notification if someone is attempting to breach **email security**.

Requirements and solutions in email security

What's the impact of phishing scams on a business?



Businesses around the globe suffer a huge loss in terms of money, reputation, regulatory fines, and much more. Even the biggies like Facebook and Google with impeccable security patches have been infiltrated by the cybercriminals and have lost millions of dollars, check this report.

The motive behind such scams is not limited to stealing just money, but something even more important – data.

So, privacy of emails may be compromised b/w sender's and receiver's side without giving organizations' daily activity.