BCA-504 Computer Security

Unit - 1

Introduction :

Computer security is the protection of computing systems and the data that they store or access. Enabling people to carry out their jobs, education, and research activities.

Definition of Computer security :

Computer security, also called cybersecurity, is the protection of computer systems and information from harm, theft, and unauthorized use.

Types of Computer Security :

1) Information Security
2) Application Security
3) Computer Security
4) Network Security
5) Cybersecurity

1) Information Security :

It is securing information from unauthorized access, modification & deletion.

2) Application Security :

It is securing an application by building security features to prevent from Cyber Threats such as SQL injection, DoS attacks, data breaches and etc.

3) Computer Security :

C*omputer Security* means securing a standalone machine by keeping it updated and patched.

4) Network Security :

Network Security is by securing both the software and hardware technologies.

5) Cybersecurity :

It is defined as protecting computer systems, which communicate over the computer networks.

Components of Computer System :

The components of a computer system that needs to be protected are:

- **Hardware,** the physical part of the computer, like the system memory and disk drive
- **Firmware,** permanent software that is etched into a hardware device's nonvolatile memory and is mostly invisible to the user
- **Software,** the programming that offers services, like operating system, word processor, internet browser to the user

The CIA Tried :

Computer security is mainly concerned with three main areas:

- **Confidentiality** *is* ensuring that information is available only to the intended audience
- **Integrity** *is* protecting information from being modified by unauthorized parties
- **Availability** *is* protecting information from being modified by unauthorized parties

In simple language, computer security is making sure information and computer components are usable but still protected from people or software that shouldn't access it or modify it.

Computer Security :

Cybercrime, also called computer crime, the use of a computer as an instrument to further illegal ends, such as committing fraud ,trafficking in child pornography and intellectual property, stealing identities, or violating privacy.

Today, the planet of the cyber criminals has became a lot of dangerous.

Types of Cyber Criminals :

1. Hackers
   - White hat hackers
   - Gray hat hackers
   - Black hat hackers
2. Organized Hackers
3. Internet Stalkers
4. Disgruntled Employees

1. Hackers:

The term hacker may refer to anyone with technical skills, however, it typically refers to an individual who uses his or her skills to achieve unauthorized access to systems or networks so as to commit crimes. The intent of the burglary determines the classification of those attackers as white, gray, or black hats. White hat attackers burgled networks or PC systems to get weaknesses so as to boost the protection of those systems.

- **White Hat Hackers –**
  These hackers utilize their programming aptitudes for a good and lawful reason. These hackers may perform network penetration tests in an attempt to compromise networks to discover network vulnerabilities. Security vulnerabilities are then reported to developers to fix them.
- **Gray Hat Hackers –**
  These hackers carry out violations and do seemingly deceptive things however not for individual addition or to cause harm. These hackers may disclose a vulnerability to the affected organization after having compromised their network.

- **Black Hat Hackers –**
  These hackers are unethical criminals who violate network security for personal gain. They misuse vulnerabilities to bargain PC frameworks.

2. Organized Hackers:

These criminals embody organizations of cyber criminals, hacktivists, terrorists, and state-sponsored hackers. Cyber criminals are typically teams of skilled criminals targeted on control, power, and wealth. These criminals are extremely subtle and organized, and should even give crime as a service. These attackers are usually profoundly prepared and well-funded.

3. Internet stalkers:

Internet stalkers are people who maliciously monitor the web activity of their victims to acquire personal data. This type of cyber crime is conducted through the use of social networking platforms and malware, that are able to track an individual's PC activity with little or no detection.
(rootkit)

4. Disgruntled Employees:

Disgruntled employees become hackers with a particular motive and also commit cyber crimes. It is hard to believe that dissatisfied employees can become such malicious hackers. In the previous time, they had the only option of going on strike against employers. But with the advancement of technology there is increased in work on computers and the automation of processes, it is simple for disgruntled employees to do more damage to their employers and organization by committing cyber crimes.

The attacks by such employees brings the entire system down.

Attack :

There are two types of Attacks.

1) Passive Attacks
2) Active Attacks

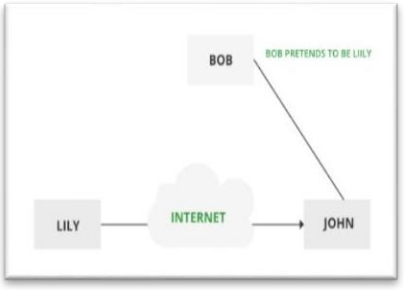
Active attacks:

An Active attack attempts to alter system resources or affect their operations. Active attacks involve some modification of the data stream or the creation of false statements. Types of active attacks are as follows:

- Masquerade
- Modification of messages
- Repudiation
- Replay
- Denial of Service

Masquerade –

A masquerade attack takes place when one entity pretends to be a different entity. A Masquerade attack involves one of the other forms of active attacks. If an authorization procedure isn't always absolutely protected, it is able to grow to be extraordinarily liable to a masquerade assault. Masquerade assaults may be performed using the stolen passwords and logins, with the aid of using finding gaps in programs, or with the aid of using locating a manner across the authentication process.

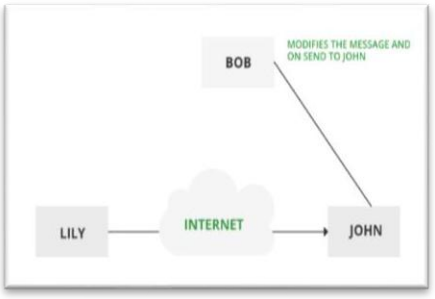


Modification of messages –

It means that some portion of a message is altered or that message is delayed or reordered

to produce an unauthorized effect. Modification is an attack on the integrity of the original data. It

basically means that unauthorized parties not only gain access to data but also spoof the data by triggering denial-of-service attacks, such as altering transmitted data packets or flooding the network with fake data. Manufacturing is an attack on authentication. For example, a message meaning “Allow JOHN to read confidential file X” is modified as “Allow Smith to read confidential file X”.

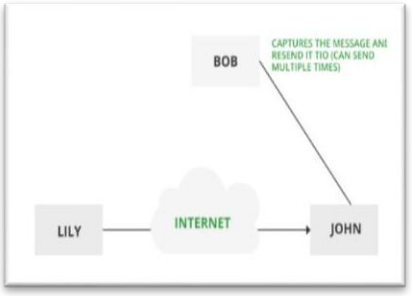


Repudiation –

This attack occurs when the network is not completely secured or the login control has been tampered with. With this attack, the author’s information can be changed by actions of a malicious user in order to save false data in log files, up to the general manipulation of data on behalf of others, similar to the spoofing of e-mail messages.

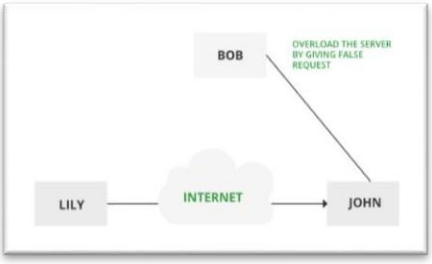
Replay –

It involves the passive capture of a message and its subsequent transmission to produce an authorized effect. In this attack, the basic aim of the attacker is to save a copy of the data originally present on that particular network and later on use this data for personal uses. Once the data is corrupted or leaked it is insecure and unsafe for the users.



Denial of Service –

It prevents the normal use of communication facilities. This attack may have a specific target. For example, an entity may suppress all messages directed to a particular destination. Another form of service denial is the disruption of an entire network either by disabling the network or by overloading it with messages so as to degrade performance.



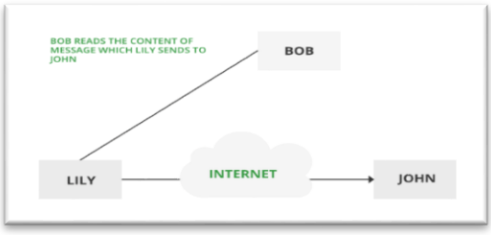
Passive attacks:

A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of eavesdropping on or monitoring transmission. The goal of the opponent is to obtain information that is being transmitted. Types of Passive attacks are as follows:

- The release of message content
- Traffic analysis

The release of message content –

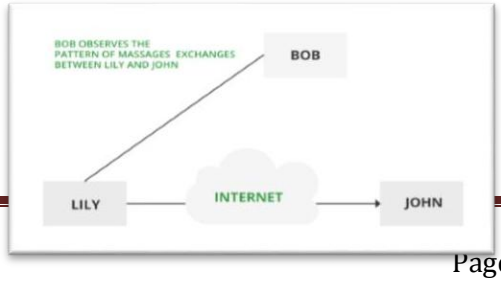
Telephonic conversation, an electronic mail message, or a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.



Traffic analysis –

Suppose that we had a way of masking (encryption) information, so that the attacker even if captured the message could not extract any information from the message.

The opponent could determine the location and identity of communicating host and could observe the frequency and



length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place. The most useful protection against traffic analysis is encryption of SIP traffic. To do this, an attacker would have to access the SIP proxy (or its call log) to determine who made the call.

Methods Of Defence :

The advancement of Technology has made man dependent on Internet for all his needs.internet has given man easy access to everything while sitting at one place.

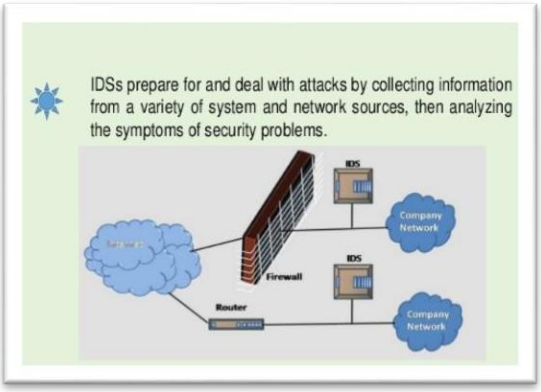
1) Firewall
2) Intrusion Detection Systems (IDS)
3) Intrusion Prevention Systems (IPS)
4) Unified Threat Management (UTM)
5) Antivirus

FIREWALL :

Using a firewall physically and logically isolates the internal network form the external of any organization. The rules for the firewall are based on the explicit directions from the system administrator. All firewalls activities are logged and analyzed by the system administrator on a periodic basis. There is need to create firewall rules to allow a Computer to send to or receive traffic from programs, system services, computer or users. Rules can be created to take one of three actions for all connections that match the rule's criteria:

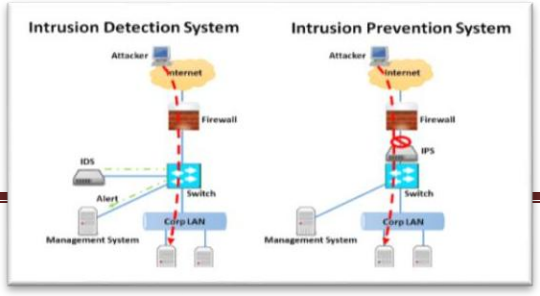
1) Allow the connection.
2) Allow a connection only if it is secured through the use of Internet Protocol security (IPSec).
3) Block the connection.

INTRUSION DETECTION SYSTEM (IDS) :



Intrusion Detection Systems are put in place to passively monitor traffic by listening to and examining the packets entering or exiting a backbone/access network. They can monitor and analyze events that occur on a network or system, thus looking for intrusion attempts based on signatures or patterns. IDS require careful tuning to network conditions to be effective and make the system useful; otherwise false positives are too high.

INTRUSION PREVENTION SYSTEM (IPS) :



Intrusion Prevention Systems (IPS) is put in place to passively monitor traffic by listening to and examining the packets entering or exiting a backbone/access

network. It is any device (hardware or software) that has

the ability to detect attacks, both known and unknown and prevents the attack from being successful.

UNIFIED THREAT MANAGEMENT (UTM) :

Unified Threat Management Systems are put in place to passively monitor traffic by listening to and examining the packets entering or exiting a backbone/access network. It has some advanced features such as URL and keyword filtering."

ANTI-VIRUS :

Antivirus- DefenceMechanisms are put in place to limit the spread of Viruses and other malware. An antivirus system will function in conjunction with a firewall to check all incoming traffic for any viruses or malicious code. In addition, antivirus software can also be installed on individual servers (server-version) and host machines.

Introduction to Cyber Security :

Introduction to Cyber Security was designed to help learners develop a deeper understanding of modern information and system protection technology and methods.

The learning outcome is simple: We hope learners will develop a lifelong passion and appreciation for cyber security, which we are certain will help in future endeavors. Students, developers, managers, engineers, and even private citizens will benefit from this learning experience.

Organizational Security :

An organizational security policy is **a set of rules or procedures that is imposed by an organization on its operations to protect its sensitive data**.

Physical security :

Physical security is **the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution**. This includes protection from fire, flood, natural disasters, burglary, theft, vandalism and terrorism.

5 ESSENTIAL SECURITY TOOLS FOR EVERY ORGANIZATION :

Every organization needs the right security products to deal with threats and uncertainty. In the past few years, the security experts have launched various security products to address the challenges that an organization faces from cybercriminals.

Given below are a few products that are essential to business enterprise security.

Network access control (NAC)

NAC products are essential tools for the cybersecurity of organizations. They allow the business enterprise to implement security policies on devices and users attempting to access their network. It helps the organization to identify who and from where they are attempting to log in to their network. NAC also ensures that the devices used within an organization have the needed security patches, antivirus software, and other controls before a user login into a system.

Data loss protection (DLP)

Another important security tool for an organization is a DLP tool, which is used to protect sensitive data from transmitting. The DLP monitors the network traffic for data that matches specific characteristics or patterns associated with credit card and Social Security numbers. These are the best devices to detect hacker's activity in case they are in. It is essential for an organization, as it is used to identify the threats and alerting the employees about the sensitive data and how they can block transmission of such data.

Firewalls

Firewall is an important security tool for an organization, as it helps to protect against malware, unauthorized logins, and other security threats. It is used to block IP ranges and URL to protect data from security breaches. The advanced firewall can do a deep inspection, application filtering, intrusion detection, and prevention of network.

Intrusion prevention systems (IPS)

The IPS is an advanced technology that is deployed behind an organization's firewall to inspect traffic flows and take automatic action to mitigate threats. The device also performs the function of intrusion detection systems (IDSs) that is used to scan networks and report on potential threats. It is important to an organization because through an IPS deep analysis on network traffic is done to identify threats.

Endpoint protection

The Endpoint protection tools are used to protect desktops, laptops and other endpoint devices against viruses, malware, worms, and malicious activity. Through these tools, various antiviruses are combined with antimalware's and firewalls to secure an organization's network.