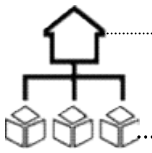


INFORMATION SECURITY

Introduction

We are living in the information age. Information is an asset that has a value like any other asset.Information security refers to the protection of safeguarding of information and information systems that use, store and transmit information form unauthorized access, disclousure, alteration, and destruction. Information is a critical asset that organizations must secure. If sensitive information falls into the wrong hands, then the respective organization may suffer huge losses in terms of finances, brand reputation, customers or in other ways.

Elements of Information Security:

Information security is a state of well-being of information and infrastructure in which the possibility of theft, tampering, and disruption of information and services is low or tolerable. This tree feature is the security goals.

Confidentiality: Assurance that the information is accessible only to those authorized to have access.

Integrity: The trustworthiness of data or resources in term of preventing improper or unothorized change.

Availability: Assurance that the system responsible for delivering, storing and processing information are accessible when require by the authorized users.

Note: This three is called CIA model.

NETWORK SECURITY BASICS

It is necessary to define some fundamental terms relating to network security and are the elements used to measure the security of a network. These terms are used to measure the security of a network. To be considered sufficiently advanced along the spectrum of security, a system must adequately address identification, integrity, accountability, non-repudiation, authentication, availability, confidentiality, each of which is defined in the following sections:

Principal of Security

- ✓ Identification
- ✓ Confidentiality
- ✓ Authentication
- ✓ Integrity
- ✓ Non-repudiation
- ✓ Availability
- ✓ Reliability
- ✓ Accountability
- ✓ Access Control (Authorization)

Identification

Identification is simply the process of identifying one's self to another entity or determining the identity of the individual or entity, with whom you are communicating.

Authentication

Authentication serves as proof that you are who you say you are or what you claim to be. Authentication is critical if there is to be any trust between parties. Authentication is required when communicating over a network or logging into a network. When communicating over a network you should ask yourself two questions.

- ✓ With whom am I communicating?
- ✓ Why do I believe this person or entity is who he claims to be?

Access Control (Authorization)

This refers to the ability to control the level of access that individuals or entities have to a network or system and how much information they can receive. Level of authorization basically determines what you're allowed to do once you are authenticated and allowed access to a network, system or some other resources such as data or information. Access control is the determination of the level of authorization to a system, a network of information.

Availability

This refers to whether the network, system, hardware and software are reliable and can recover quickly and completely in the event of an interruption in service. Ideally, these elements should not be susceptible to denial of service attacks.

Confidentiality

This is also called privacy or secrecy to the protection of information from unauthorized disclosure. Usually achieved either by restricting access to the information or by encrypting the information so that it is not meaningful to unauthorized individuals or entities.

Integrity

This can be thought of as accuracy, this refers to the ability to protect information, data, or transmissions from unauthorized, uncontrolled or accidental alterations.

Accountability

This refers to the ability to track or audit what an individual or entity is doingon a network or system.

Non-repudiation

The ability to prevent individuals or entities from denying (repudiation) that information, data or files were sent or received or that information or files were accessed or altered, when in fact they were.This capability is crucial in e-commerce, without if an individual or entity can deny that he, she or it is responsible for a transection and that he, she or it is, therefore, not financially liable.

Motives behind Information Security Attacks:

- ✓ Disrupting business continuity
- ✓ Damaging the reputation of the target
- ✓ Stealing information and manipulation of data
- ✓ Hacking money
- ✓ Demanding ransome
- ✓ Show his power
- ✓ Showing political power
- ✓ Take revenge.

Attacks=Motive(Goal)+Method+Vulnerability

Classification of attacks: *[Officer(IT/ICT)-2019] [BDBL(IT/ICT)-2017]*

Name	Description	Example
Active attacks	Active attacks tamper with the data in transit or disrupt the communication or services between the systems to bypass or break into secured systems.	✓ Denial-of-service(DoS) attack ✓ Bypassing protection mechanism ✓ Malware attacks(virus,worms,ransomeware) ✓ Spoofing attacks ✓ Password based attacks ✓ Session Hijaking ✓ Man-in-Middle attack ✓ DNS and ARP poisoing ✓ SQL Injection ✓ XSS attack ✓ Backdoor access
Passive attacks	Passive attacks do not tamper with the data and involve interceptiong and monitoring network traffic and data flow on the target network.	✓ Footprinting ✓ Sniffing and eavesdropping ✓ Network traffic analysis ✓ Decryption of weakly encrypted traffic
Close-in attacks	Close-in attacks are performed when the attacker is in close physical proximity with the target system or network in order to gather, modify, or disrupt access to information.	✓ Social Engineering(Eavesdropping, Shoulder surfing, dumpster diving, and other method)
Insider attacks	Insider attacks involve using privileged access to violate rules or intentionally causes a threat to the organization's information of information system.	✓ Eavesdropping and wiretapping ✓ Theft of physical devices ✓ Social engineering ✓ Data theft and spoliation ✓ Pod slurping ✓ Planting keyloggers, backdoors or malware
Distribution attacks	Distribution attacks occur when attackers tempers with hardware or software prior to installation	✓ Modification of software or hardware during production ✓ Modification of software or hardware during distribution.

Adversary behavioral Identification:

- ✓ Internal Reconnaissance
- ✓ Use of powershell
- ✓ Unspecified proxy Activities
- ✓ Use of Command-Line Interface
- ✓ HTTP User Agent

- ✓ Command and control Server
- ✓ Use of DNS Tunneling
- ✓ Use of Web Shell
- ✓ Data Staging

Hacking refers to exploiting system vulnerabilities and compromising security controls to gain unauthorized or inappropriate access toa system's resource.

Hacking Phases:

In general, there are five phases of hacking

- ✓ Reconnaissance and Footprinting
- ✓ Scanning
- ✓ Gaining Access
- ✓ Maintaining Access
- ✓ Clearing Tracks

Reconnaissance and Footprinting: Footprinting is one of the most convenient ways for hackers to collect information about targets such as computer systems, devices, and networks. Using this method, hackers can unravel information on open ports of the target system, services running, and remote access probabilities. For successful footprinting, the attacker needs to first check the visibility of the target and see how to gather related information on the internet through open sources. Through careful analysis, the attacker can determine the scope of potential entry points. The following information can be collected:

- ✓ Company names
- ✓ Domain names
- ✓ Business subsidiaries
- ✓ IP Addresses
- ✓ Business emails
- ✓ Network phone numbers
- ✓ Key employees

Scanning: Scanning refers to the pre-attack phase when the attacker scansthe network for specific information based on information gathered during reconnaissance. Scanning can include the use of dialers, port scanners, network mappers, ping tools, vulnerability scanner, or other tools. Attackers extract information such as live maschine, port, port status, OS details, and device type and system uptime to launch an attack.

Gaining Access: Gaining access to the point where the attackers obtains access to the operating system or applications on the target computer or network. The attacker can escalate privileges to obtain complete control of the system. In this process, the target connected intermediate system are also compromised. **Example: password cracking, buffer overflow, denial of and session hijacking.**

Maintaining access: Maintaining access refers to the phase when the attacker tries to retain their ownership of the system. Attackers may prevent the system from being owned by other attackers by securing their exclusive access with backdoors, rootkits or trojon. Attackers can upload, download or manipulate data, application and configurations on the owned system.

Clearing Tracks: Clearing tracks refers to the activities carried out by an attacker to hide malicious acts. Attackers will usually attempt to erase all evidence of their action also hide malicious acts.

Ethical hacking involves the use of hacking tools, tricks and technique to identify vulnerabilities and ensure system security.

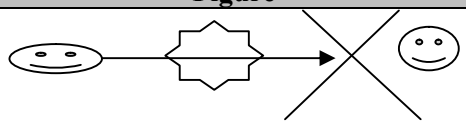
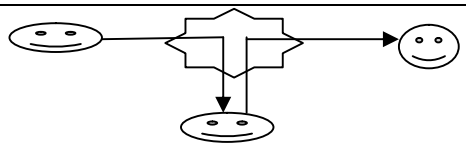
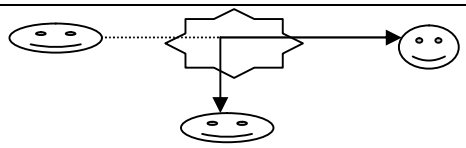
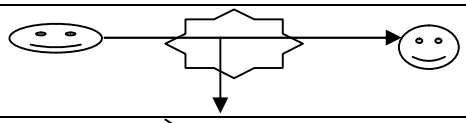
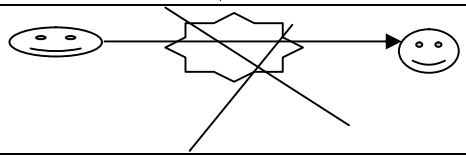
Threats

A threat is anything that can disrupt the operation, functioning, integrity, or availability of a network or system. This can take any form and can be malevolent, accidental, or simplyan act of nature.

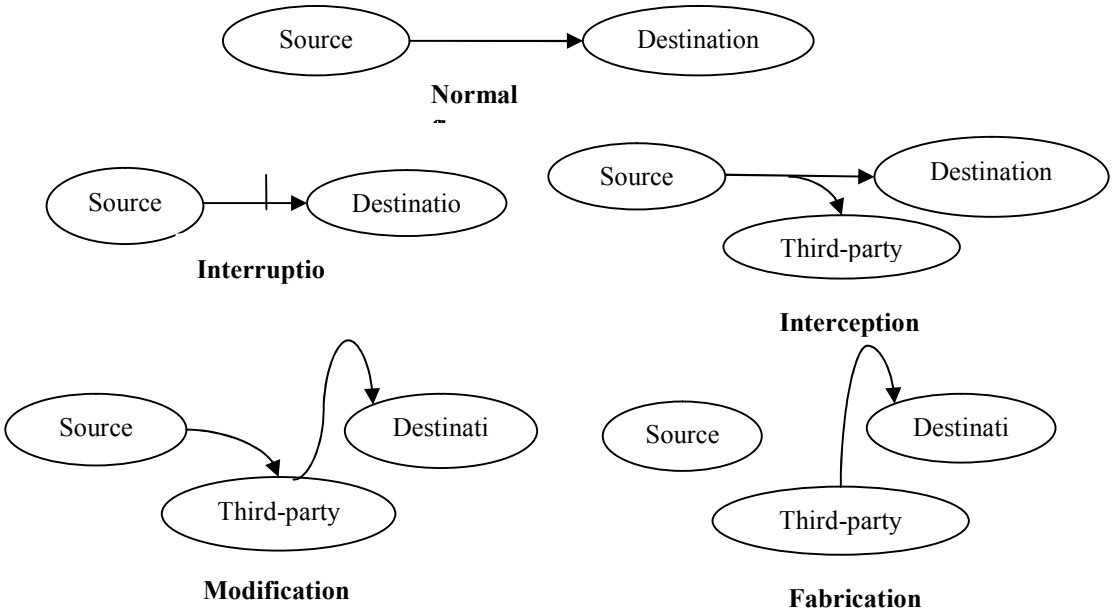
Vulnerabilities

Vulnerability is an inherent weakness in the design, configuration, implementation, or management of a network or system that renders it susceptible to a threat. Vulnerabilities are what make networks susceptible to information loss and downtime. Every network and system has some kind of vulnerability.

Attacks: The X.800 Threat Model

Item	Figure
Destruction (an attack on availability): ☞ Destruction of information and/or network resources	
Corruption (an attack on integrity) : ☞ Unauthorized tampering with an asset	
Removal (an attack on availability) : ☞ Theft, removal or loss of information and/or other resources	
Disclosure (an attack on confidentiality) : ☞ Unauthorized access to an asset.	
Interruption (an attack on confidentiality) : ☞ Network becomes unavailable or unusable.	

Security Attacks (Stallings)



Threats (or Perils)

Threats (or perils) are things which may cause loss to information assets. Examples of threats that pertain to the Internet and other networks include the following.

- **Tapping**
  - The interception of data by a third party with malicious intent.
- **Falsification**
  - The fraudulent rewriting of information in e-mail or web pages.
- **Spoofing**
  - The performance of fraudulent actions by impersonating another person (e.g., authorized user)
- **Theft**
  - The theft of files or data by a third party with malicious intent
- **Destruction**
  - The fraudulent destruction or erasure of files or data
- **Threats are classified into three types as follows:**
  - **Personal threat**
    - This is the type of threat that is caused by human behavior (with or without malicious intent).
  - **Technological threat**
    - This is the type of threat in which a third party with malicious intent uses computer technology to make attacks.
  - **Physical threat**
    - This is the type of threat against equipment itself or against the buildings in which equipment is located.

Personal threats

- **Information leakage**

- ✍ This is the leakage of information to a third party. It includes intentional leakage with the aim of receiving payment for information provision, and unintentional leakage of important information accidentally overheard by a third party. In addition, information in discarded equipment may be restored and leaked if not physically deleted (i.e., destroyed).

☞ **Loss / Theft / Damage**

- ✍ This means that IT devices, such as PCs and USB memory, where information is stored are left behind, stolen, or destroyed during use.

☞ **Error / Incorrect operation**

- ✍ This is data erasure or such other error that is caused by wrong operation. It includes the leakage of important information through mistaken entry of recipient e-mail addresses.

☞ **Social engineering**

- ✍ This is the act of stealing information through every day and common means.

☞ **Trashing (scavenging, dumpster diving)**

- ✍ This is the act of stealing important information from memos thrown away in the garbage bin, data left in memory or cache, etc. It is also used as a method of foot printing for prior collection of information about the target of attacks.

☞ **Spoofing**

- ✍ This is the impersonation of a person by a third party. The spoofed may pretend to be a customer or a supervisor in order to ask for PINs (PIN Numbers) or passwords.

☞ **Peeping**

- ✍ This is the act of sneaking a peek at keyboard operation of a person who is entering a password, or classified information displayed on another person's screen. In particular, the act of sneaking a peek at information over a person's shoulder is called shoulder hacking.

☞ **Cracking**

- ✍ This is the act of intruding into another person's PC with malicious intent, to steal or destroy data. A person who engages in cracking is called a cracker. Note that the software package used by a cracker after unauthorized intrusion is called a rootkit,and the path installed to facilitate later intrusion is called a back door.

☞ **Targeted attack**

- ✍ This is the act of attacking a specific organization or person as a target. Since humans select the target of the attack, this is classified as a personal threat. However, the attack method itself is primarily classified as a technological threat.

Technological threats

☞ **DoS attack (Denial of Service)**

- ✍ This is an attack that sends a large amount of data continually to the target server to place an excessive load on the server's CPU and memory, and thereby obstructs service. In addition, there is also a DDoS (Distributed DoS) attack in which malicious programs used for targeted attacks are used to attack the single target all at once from multiple PCs.

☞ **Key logger**

- ✍ This is an attack that uses the mechanism (e.g., software) that records keyboard input,and fraudulently acquires information (e.g., password) entered by another person.

☞ **Click jacking**
- ✍ This is an attack that sets up a web page with some sort of function that causes a user's click to execute operations not intended by the user.

☞ **Phishing**
- ✍ This is an attack that leads a user to a fake website through means such as e-mail pretending to be sent from a real company (e.g., financial institution), and defrauds the user of the credit card number, a bank account number, a PIN, and other personal information.

☞ **Cache poisoning**
- ☞ This is an attack that fraudulently overwrites cache information. In particular, DNS cache poisoning, which overwrites DNS cache, is used to lead users to fake websites for phishing.

☞ **IP spoofing**
- ✍ This is an attack that sends packets to another party with the source IP address disguised. This is used in actions including leading users to fake websites for phishing.

☞ **XSS (Cross Site Scripting)**
- ✍ This is an attack where a vulnerable target website is used as a stepping stone; a malicious script is sent to a user who is accessing the target website, and then executed on the user's browser to enable the theft of information.

☞ **CSRF (Cross Site Request Forgery)**
- ✍ This is an attack which, when a user is logged in to a website and then accesses another website that has a trap installed, causes a malicious request to be sent to and executed by the logged-in website in the guise of a request from the user (i.e., as a forgery).

☞ **Session hijacking**
- ✍ This is an attack that takes over a session (i.e., a series of communications between specified parties) during communication between correctly authorized users.

☞ **Directory traversal**
- ✍ This is an attack that accesses normally undisclosed directories (or files) by appending "../ " to file names, to traverse upward through directories.

☞ **Drive-by download**
- ✍ This is an attack that causes a user to download a malicious program, without permission during website browsing.

☞ **SQL injection** *[BTV(AP)-2019]*
- ✍ This is an attack that falsely modifies a database or fraudulently obtains information by providing part of an SQL statement as a parameter to a program (CGI program) in the website that is linked to the database.

Question: How can we prevent SQL injection Attack? *[SBL&JBL(AME)-2020]*

a) Show the database error to the users b) User input validation

c) Use the user input directly d) Donot remove potential malicious code Ans: **b**

- **Side channel attack**
  - This is an attack that obtains confidential information by measuring and analyzing some additional information (i.e., side channel information), such as the electric power consumption or radiated electromagnetic waves of active IC chips.
- **Zero-day attack**
  - This is an attack that takes advantage of vulnerability in software before fix for the vulnerability can be released by the software vendor.
- **Password cracking**
  - This is an attack that fraudulently decodes or otherwise obtains the password of a true user.
    - **Dictionary attack**
      - This is a method that uses a file (i.e., a dictionary file) that contains character strings likely to be used as passwords, to try such words in sequence.
    - **Brute force attack**
      - This is a brute-force method that attempts every combination of characters. It is used as an attack method of performing the exhaustive search for a decryption key.
- **Third-party relay**
  - This is an attack that abuses a freely usable server (e.g., mail server) as a "steppingstone" to transmit e-mail and other data.
- **Gumblar**
  - This is an attack that falsifies the website of a famous company or public institution, and infects the computer of a user who is browsing the falsified website with a computer virus.
- **Buffer overflow**
  - This is an attack that continually sends long character strings or such other data to flood the memory area (i.e., buffer) secured by a program, for the purpose of seizing access privileges to the program and creating malfunctions.

✓ The following computer crimes are also said to be types of technological threats.

- **Salami technique (Salami slicing)**
  - This is a method of repeatedly stealing assets little by little so that they are negligibly small when taken as a whole. An example is a technique that collects money from a bank account into another account, in fractions of less than one yen.
- **One-click fraud**
  - This is a type of fraudulent act; for example, clicking an image or link on matchmaking or adult websites causes an unfair fee to be charged.
- **Phishing fraud**
  - This is a general name for the act of phishing, or for fraudulent acts committed using information obtained illicitly through phishing.

Physical threats

- **Disaster**
  - ✓ This means that equipment or buildings are made unusable, or equipment itself is lost, due to a natural disaster (e.g., earthquake, flood) or a human disaster (e.g., fire).
- **Destruction**

- This means that equipment or buildings are made unusable, due to sabotage or destructive acts by a third party with malicious intent.

☞ **Accident / failure**

- This means that equipment or buildings are made unusable, due to unforeseen accidents or failures.

☞ **Unauthorized intrusion**

- This means that unauthorized persons intrude into buildings or rooms in which equipment is located.

☞ **Vulnerabilities (or Hazards)**

- Vulnerabilities (or hazards) are weaknesses or flaws that are exploited by threats, becoming the cause of even greater threats. A variety of vulnerabilities in equipment, technologies, management, and many other areas cause problems.

☞ **Security hole**

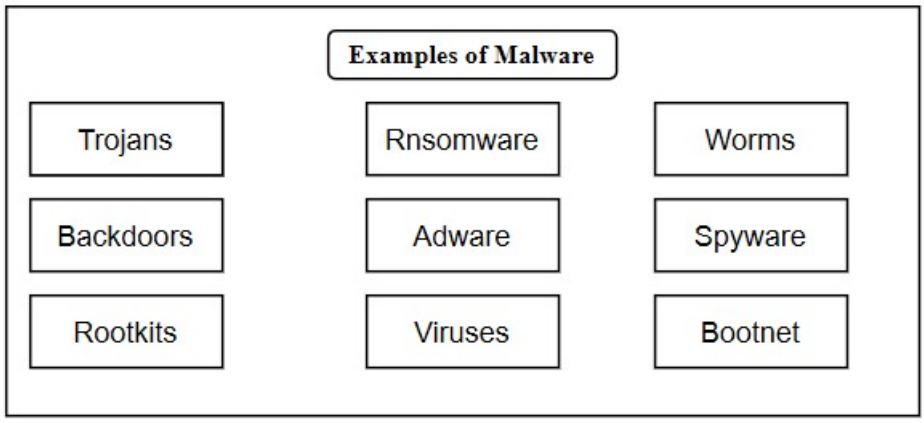
- This is a vulnerability of software or systems that is caused software design flaws, bugs, etc.

☞ **Man-made vulnerability**

- This is a vulnerability that is caused by human behavior, due to lack of enforcement or preparation of a code of conduct for companies, organizations, and people.

Malicious software *[Combined 3 bank (AP)-2018]*

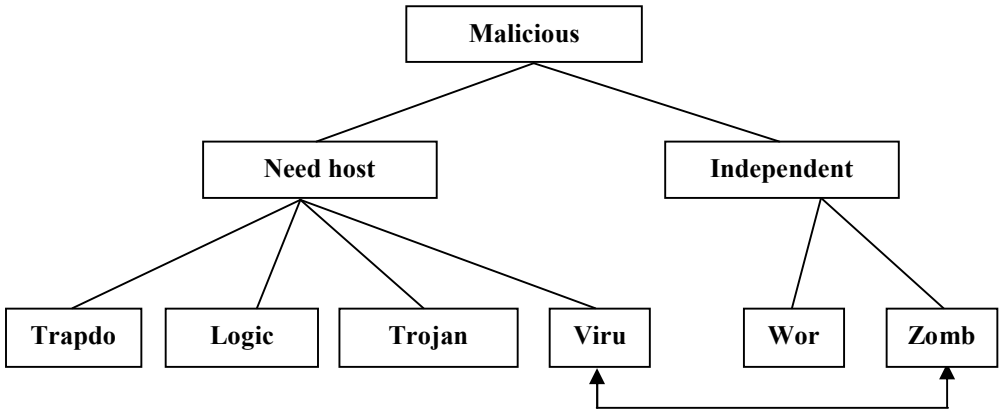
Malicious software, commonly known as malware, is any software that brings harm to a computer system. Malware is a malicious software that damages or disables computer systems and gives limited or full control of the systems to the malware creator for the purpose of theft or fraud. Malware can be in the form of worms, viruses, trojans, spyware, adware and root kits etc, which steal protected data, delete documents or add software not approved by a user.



How malware Enter Your System:

- ✓ Instant Messenger applications
- ✓ Portable hardware media/removable devices
- ✓ Browser and email software bugs
- ✓ Insecure patch management
- ✓ Rogue/decoy applications
- ✓ Downloading files from the Internet
- ✓ Email attachments

- ✓ Network propagation
- ✓ File sharing services (NetBIOS, FTP, SMB)
- ✓ Installation by other malware
- ✓ Untrusted sites and freeware web applications/ software I
- ✓ Bluetooth and wireless networks



Fraudulent programs (i.e., malware) created with malicious intent are also classified as technological threats. The following are typical examples of malware.

Trapdoor

- ☞ Trap Door is a type of security breach where the designer of a program or a system leaves a hole in the software that only he is capable of using.
- ☞ A Trap Door is a secret entry point into a program that allows someone to gain access without normal methods of access authentication.

Trojan horse

- ☞ A Trojan horse is a program that appears harmless, but is, in fact, malicious. The term comes from Greek mythology about the Trojan War. Trojans may allow an attacker to access users' personal information such as banking information, passwords, or personal identity (IP address). It can infect other devices connected to the network. Ransom ware attacks are often carried out using a Trojan.
- ☞ A Trojan horse is a code segment that misuses its environment.

A Trojan may give a hacker remote access to a targeted computer system. Operations that could be performed by a hacker on a targeted computer system may include-

- ✓ Use of the machine as part of a botnet (e.g. to perform automated spamming or to distribute Denial-of-Service attacks)
- ✓ Electronic Money theft
- ✓ Data Theft(e.g. retrieving passwords or credit card information)
- ✓ Installation of software, including third-party malware
- ✓ Downloading or uploading of files on the user's computer
- ✓ Modification deletion of files
- ✓ Crashing the Computer
- ✓ Anonym zing Internet Viewing

The following computer malfunctions are indications of a Trojan attack:

- ✓ The DVD-ROM drawer opens and closes automatically.

- ✓ The computer screen blinks, flips upside-down, or is inverted so that everything is displayed backward.
- ✓ The default background or wallpaper settings change automatically. This can be performed using pictures either on the user's computer or in the attacker's program.
- ✓ Printers automatically start printing documents.
- ✓ Web pages suddenly open without input from the user.
- ✓ The color settings of the operating system (OS) change automatically.
- ✓ Screensavers convert to a personal scrolling message.
- ✓ The sound volume suddenly fluctuates.
- ✓ Antivirus programs are automatically disabled, and the data are corrupted, altered, or deleted from the system.
- ✓ The date and time of the computer change.

Logic bomb

A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files (such as a salarydatabase trigger), should they ever be terminated from the company.

Computer virus

Computer **Viruses** a computer virus is defined as "a program that is created to intentionally cause some form of damage to third parties' programs or databases, and that has one or more of the following functions.

- ✍ **Self-infecting function:** Viruses make copies of themselves to infect other systems.
- ✍ **Concealment function:** Viruses do not reveal symptoms until the onset of their action.
- ✍ **Onset function:** Viruses perform actions not intended by designers, such as destruction of data.

Virus Phases

1. **Dormant phase:** The virus is idle.
2. **Propagation Phase:** The virus places an identical copy of itself into other programs.
3. **Triggering Phase:** The virus is activated to perform the function for which it was intended.
4. **Execution Phase:** The function is performed.

However, in general at present, file-infecting viruses that infect specific files are called computer viruses (in a narrow sense).

- ☞ **Boot sector virus**: This virus infects the boot sector (i.e., the system area that contains the boot program) that is read before an OS starts up.
- ☞ **Program file virus:** This virus infects the executable program files such as applications.
- ☞ **Interpreter virus:** This virus infects non-executable files, such as data files, other than program files. It includes two types of viruses: a macro virus that infects through the macro functions of application software, and a script virus that infects through a scripting language like JavaScript or VB Script.

Worm

A worm proliferates by duplicating itself on other computers through networks, without the need for a program to be infected. It often spreads a copy of itself automatically as an e-mail attachment file, or uses networks to continue spreading infection.

Bot

This is a program that is created for the purpose of controlling infected computers from outside via networks (e.g., the Internet).

Spyware

This is a program that illicitly obtains a user's information, such as personal information and access histories, and automatically sends such information to another party other than the user.

Zombie

A zombie is a computer connected to the Internet that has been compromised by a hacker, computer virus or Trojan horse program and can be used to perform malicious tasks of one sort or another under remote direction. Botnets of zombie computers are often used to spread e-mail spam and launch denial-of-service attacks (DOS attacks).

Root kit

- A **root kit** is a collection of computer software, typically malicious, designed to enable access to a computer or areas of its software that is not otherwise allowed (for example, to an unauthorized user) and often masks its existence or the existence of other software. The term rootkit is a concatenation of root (the traditional name of the privileged account on Unix-like operating systems) and the word kit (which refers to the software components that implement the tool). The term rootkit has negative connotations through its association with malware.
- **Rootkit** installation can be automated, or an attacker can install it after having obtained root or Administrator access. Obtaining this access is a result of direct attack on a system, i.e. exploiting a known vulnerability (such as privilege escalation) or a password (obtained by cracking or social engineering tactics like phishing). Once installed, it becomes possible to hide the intrusion as well as to maintain privileged access. The key is the root or administrator access. Full control over a system means that existing software can be modified, including software that might otherwise be used to detect or circumvent it.
- **Rootkit** detection is difficult because a rootkit may be able to subvert the software that is intended to find it. Detection methods include using an alternative and trusted operating system, behavioral-based methods, signature scanning, difference scanning, and memory dump analysis. Removal can be complicated or practically impossible, especially in cases where the rootkit resides in the kernel; reinstallation of the operating system may be the only available solution to the problem. When dealing with firmware rootkits, removal may require hardware replacement, or specialized equipment.

Ransomware

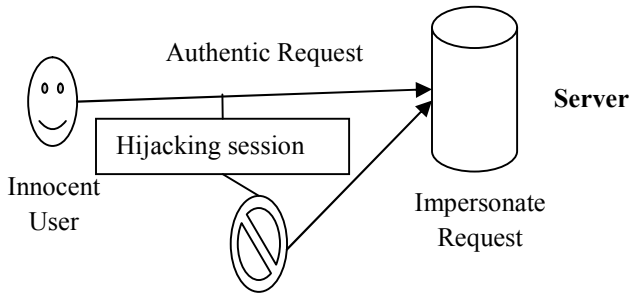
- **Ransomware** is a form of malicious software (or malware) that, once it's taken over your computer, threatens you with harm, usually by denying you access to your data. The attacker demands a ransom from the victim, promising not always truthfully to restore access to the data upon payment.
- Users are shown instructions for how to pay a fee to get the decryption key. The costs can range from a few hundred dollars to thousands, payable to cybercriminals in Bitcoin.

How Ransom ware works.

There are a number of vectors **ransom ware** can take to access a computer. One of the most common delivery systems is phishing spam — attachments that come to the victim in an email, masquerading as a file they should trust. Once they're downloaded and opened, they can take over the victim's computer, especially if they have built-in social engineering tools that trick users into allowing administrative access. Some other, more aggressive forms of ransom ware, like Not Petya, exploit security holes to infect computers without needing to trick users.

Session Hijacking

- Whenever a new session is created a cookie is generated for that user , this cookie becomes the session ID , so all the request can serve using that session ID.
- If somehow a hacker can sniff or steal the session id he can forge the request as a valid user (i.e impersonate as you).



Phishing.

Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

Phishing types

1. Spear phishing
2. Clone phishing
3. Whaling

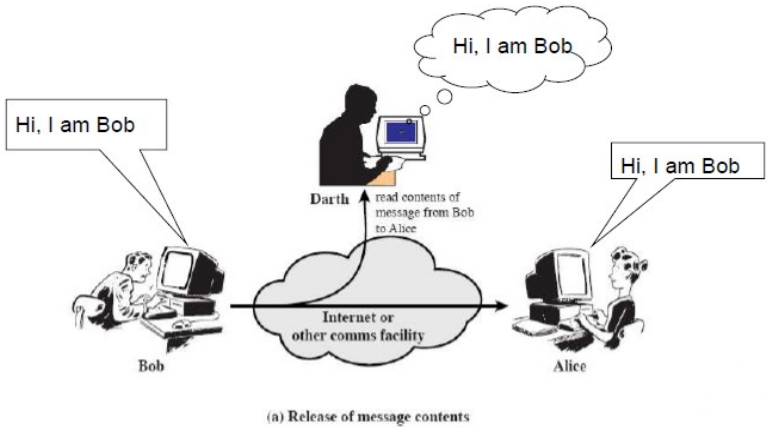
Others Security Category

- **Related security categories**
  - Cyber warfare
  - Computer security
  - Mobile security
  - Network security
  - Internet security
- **Threats**
  - Computer crime
  - Vulnerability
  - Eavesdropping
  - Exploits
  - Trojans

- Viruses and worms
- Denial of service
- Malware
- Payloads
- Rootkits
- Key loggers

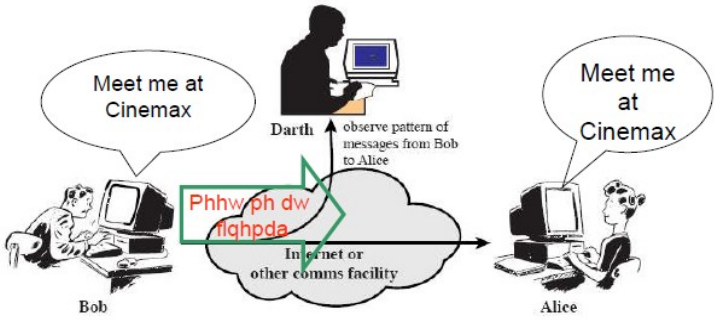
- **Defenses**
  - Computer access control
  - Application security
    - ✓ Antivirus software
    - ✓ Secure coding
    - ✓ Security by design
    - ✓ Secure operating systems
  - Authentication
    - ✓ Multi-factor authentication
  - Authorization
    - Data-centric security
    - Firewall (computing)
    - Intrusion detection system
    - Intrusion prevention system
    - Mobile secure gateway

Release of Message Contents



(a) Release of message contents

Traffic Analysis



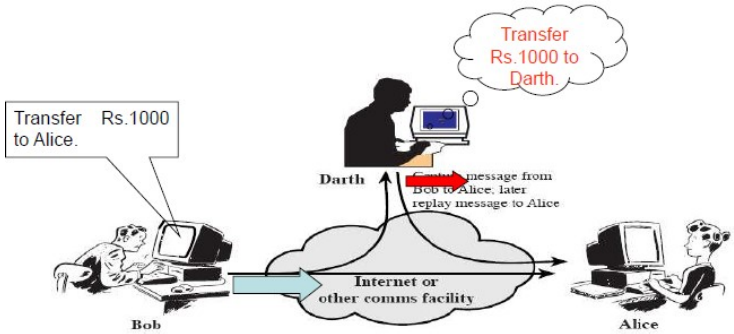
(b) Traffic analysis

Active Attack

- ☞ It involves some modification of data stream or creation of a false stream.
- ☞ Active attacks are Release of Replay, Modification, Denial of service and Masquerade.

Replay

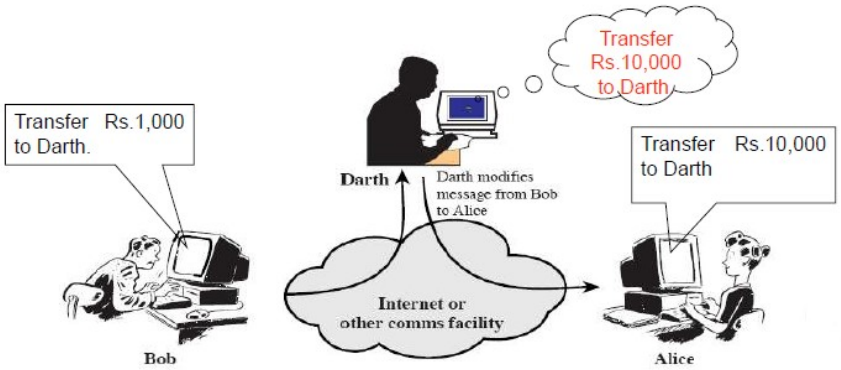
- ☞ It involves passive capture of data unit and its subsequent retransmission to produce an unauthorized effect.



(b) Replay

Modification

- ☞ In which some portion of message is altered or that message are delayed or reordered to produce an unauthorized affect.



(c) Modification of messages

Masquerade

- A masquerade is a type of attack where the attacker acts as an authorized user system in order to gain access to it or to gain greater privileges than they are authorized for.

(a) Masquerade

Malicious Types of attacks are included

- **Passive**
  - Wiretapping
  - Port scanner
  - Idle scan
  - Encryption
  - Traffic Analysis
- **Active**
  - Virus
  - Eavesdropping
  - Data Modification
  - Denial-of-service attack
  - DNS spoofing
  - Man in the middle
  - ARP poisoning
  - VLAN hopping

- Smurf attack
- Buffer overflow
- Heap overflow
- Format string attack
- SQL injection
- Phishing
- Cross-site scripting
- CSRF
- Cyber-attack

Sniffing

Sniffing is the process of monitoring and capturing all data packets that are passing through a computer network using packet sniffers. Packet Sniffers are used by network administrators to keep track of data traffic passing through their network. These are called network protocol analyzers. In the same way, malicious attackers employ the use of these packet sniffing tools to capture data packets in a network.

Data packets captured from a network are used to extract and steal sensitive information such as passwords, usernames, credit card information, etc. Attackers install these sniffers in the system in the form of software or hardware. There are different types of sniffing tools used and they include Wireshark, Ettercap, BetterCAP, Tcpdump, WinDump, etc.

Sniffing motives:

- ✓ Getting username an passwords
- ✓ Stealing bank related/transaction related information
- ✓ Spying on email and chat messages
- ✓ Identity theft

The Difference Between Sniffing and Spoofing:

In sniffing, the attacker listens into a networks' data traffic and captures data packets using packet sniffers. In spoofing, the attacker steals the credentials of a user and uses them in a system as a legitimate user. Spoofing attacks are also referred to as man-in-the–middle attacks since the attacker gets in the middle of a user and a system.

Types of Sniffing

There are two types of sniffing attacks, active sniffing and passive sniffing.

- ✓ **Active sniffing** – this is sniffing that is conducted on a switched network. A switch is a device that connects two network devices together. Switches use the media access control (MAC) address to forward information to their intended destination ports. Attackers take advantage of this by injecting traffic into the LAN to enable sniffing.
- ✓ **Passive sniffing** – passive sniffing uses hubs instead of switches. Hubs perform the same way as switches only that they do use MAC address to read the destination ports of data. All an attacker needs to do is to simply connect to LAN and they are able to sniff data traffic in that network.

Social engineering

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Social engineering attacks happen in one or more steps. A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack. Then, the attacker moves to gain the victim's trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources.Like the attacker gether information from organization official website, where employee's ID's, name,email are shared. Blogs, forum, facebook, twitter where employee share basic and personal or organizational information.

Social engineering attack techniques

Baiting: baiting attacks use a false promise to pique a victim's greed or curiosity.

Scareware: Scareware involves victims being bombarded with false alarms and fictitious threats.

Pretexting: The scam is often initiated by a perpetrator pretending to need sensitive information from a victim so as to perform a critical task.

Phishing: As one of the most popular social engineering attack types, phishing scams are email and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims. It then prods them into revealing sensitive information, clicking on links to malicious websites, or opening attachments that contain malware.

Spear phishing: This is a more targeted version of the phishing scam whereby an attacker chooses specific individuals or enterprises.

Spam Mail: Malicious mail send through attacker.

Pop-up window: pop up false window.

Social engineering prevention

- ✓ Don't open emails and attachments from suspicious sources
- ✓ Use multifactor authentication
- ✓ Be wary of tempting offers
- ✓ Keep your antivirus/antimalware software updated

Employee causes the most risk of fraud and computer compromises – Do you agree with the statement. Justify your answer. *[Uttara Bank(AP)-2019]*

Denial of service *[HBFC & KB(AP)-2018]*

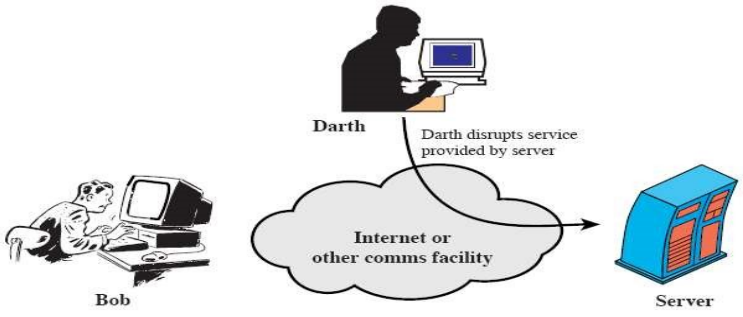
A **Denial-of-Service (DoS) attack** is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.

Victims of DoS attacks often target web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations. Though DoS attacks do

not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle.

There are two general methods of DoS attacks: flooding services or crashing services. Flood attacks occur when the system receives too much traffic for the server to buffer, causing them to slow down and eventually stop. Popular flood attacks include:

- ✓ **Buffer overflow attacks** – the most common DoS attack. The concept is to send more traffic to a network address than the programmers have built the system to handle. It includes the attacks listed below, in addition to others that are designed to exploit bugs specific to certain applications or networks
- ✓ **ICMP flood** – leverages misconfigured network devices by sending spoofed packets that ping every computer on the targeted network, instead of just one specific machine. The network is then triggered to amplify the traffic. This attack is also known as the smurf attack or ping of death.
- ✓ **SYN flood** – sends a request to connect to a server, but never completes the handshake. Continues until all open ports are saturated with requests and none are available for legitimate users to connect to.
  - ☞ It have a specific target (Server), in which prevents or inhabits the normal use or management of communication facilities.



(d) Denial of service

DoS attacks have various forms and target various services. The attacks may cause the following:

- ✓ Consumption of resources
- ✓ Consumption of bandwidth, disk space, CPU time, or data structures
- ✓ Actual physical destruction or alteration of network components
- ✓ Destruction of programming and files in a computer system

In general, DoS attacks target network bandwidth or connectivity. Bandwidth attacks overflow the network with a high volume of traffic by using existing network resources, thereby depriving legitimate users of these resources. Connectivity attacks overflow a system with a large number of connection requests, consuming all available OS resources to prevent the system from processing legitimate user requests.

Distributed denial-of-services (DDoS): *[KB(AP)-2016]*

A distributed denial-of-service (DDoS) attack is one of the most powerful weapons on the internet. When you hear about a website being "brought down by hackers," it generally means it has become a victim of a DDoS attack. In short, this means that hackers have attempted to make a

website or computer unavailable by flooding or crashing the website with too much traffic. Distributed denial-of-servics (DDoS) is a coordinated attack that involves a multitude of compromised system (Botnet) attacking a single target, thereby denying services to users of the targeted system.

How do DDoS attacks work?

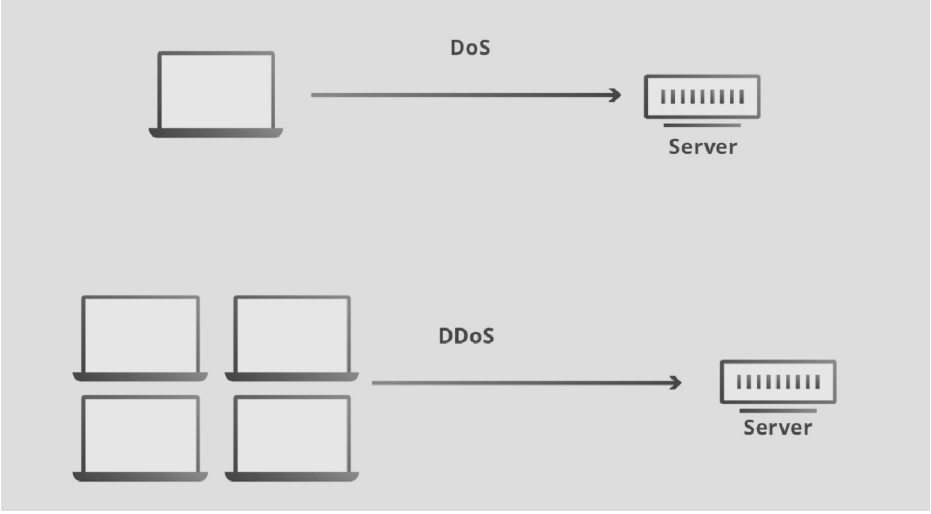
The theory behind a DDoS attack is simple, although attacks can range in their level of sophistication. Here's the basic idea. A DDoS is a cyberattack on a server, service, website, or network floods it with Internet traffic. If the traffic overwhelms the target, its server, service, website, or network is rendered inoperable.

Network connections on the Internet consist of different layers of the Open Systems Interconnection (OS) model. Different types of DDoS attacks focus on particular layers. A few examples:

- ✓ Layer 3, the Network layer. Attacks are known as Smurf Attacks, ICMP Floods, and IP/ICMP Fragmentation.
- ✓ Layer 4, the Transport layer. Attacks include SYN Floods, UDP Floods, and TCP Connection Exhaustion.
- ✓ Layer 7, the Application layer. Mainly, HTTP-encrypted attacks.

DoS vs DDos attack

- ✍ Denial of service (DOS)**:** when a single host attacks. Denial of service attacks are designed to shut down or render inoperable a system or network. The goal of the denial-of-service attack is not to gain access or information but to make a network or system unavailable for use by other users. It is called denial-of-service attack, because the end result is to deny legitimate users access to network services.
- ✍ **DDoS:** when multiple hosts attacks simultaneously



Differenc between Dos and Ddos attack

No	Dos	DDos
1.	Attacklaunchedby a singlemachine.	Attack launched by many machines, also called a botnet

2.	Can be stopped relatively easily with the right security.	Can be a real headache to prevent.
3.	Low threat level, as these will rarely be used to cover a breach attempt.	Medium to high threat level, as these can be used to do some serious damage to networks and even systems.
4.	No malware involved.	A botnet is usually made up oof thousands of infected pc's.

1. An attackersit between the sender and the receiver and capture the information and retransmit the receiver after some times without altering the information. The attack is called as----*[Rupali ANE-2021]*

a) Denial of service attack b) Masquerade attack

c) Simple attack d) Complex attack Ans: **a**

2. _____ is an assault on a service from a single source that floods it with so many requests that it becomes overwhelmed and it is either stopped completely or operates at a significantly reduced rate? *[SBL&JBL(AME)-2020]*

a) Denial-of-services(DoS) attack b) Spoofing attack

c) Cross-site scripting (XSS) d) Buffer overflow attack Ans:**a**

3. Viruses that take up residence in the computer's memory and making hard to detect is called: *[SBL&JBL(O-IT)-2020]*

a) Cluster Virus b) Self-Encrypting Virus

c) Stealth Virus d) Macro Virus Ans:**c**

Brief discussion about Firewall

A firewall is a type of cybersecurity tool that is used to filter traffic on a network. Firewalls can be used to separate network nodes from external traffic sources, internal traffic sources, or even specific applications. Firewalls can be software, hardware, or cloud-based, with each type of firewall having its own unique pros and cons.

Firewall types can be divided into several different categories based on their general structure and method of operation. Here are eight types of firewalls:

- ✓ Packet-filtering firewalls
- ✓ Circuit-level gateways
- ✓ Stateful inspection firewalls
- ✓ Application-level gateways (a.k.a. proxy firewalls)
- ✓ Next-gen firewalls
- ✓ Software firewalls
- ✓ Hardware firewalls
- ✓ Cloud firewalls

Compare GET vs. POST

Types	GET	POST
BACK button/Reload	Harmless	Data will be re-submitted (the browser should alert the user that the data are about to be re-submitted)
Bookmarked	Can be bookmarked	Cannot be bookmarked

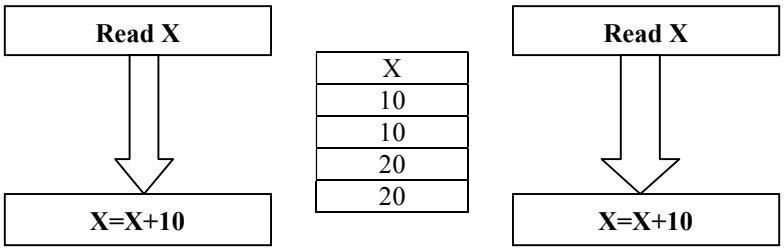
Cached	Can be cached	Not cached
Encoding type	application/x-www-form-urlencoded	application/x-www-form-urlencoded or multipart/form-data. Use multipart encoding for binary data
History	Parameters remain in browser history	Parameters are not saved in browser history
Restrictions on length data	Yes, when sending data, the GET method adds the data to the URL and the length of a URL is limited (maximum URL length is 2048 characters)	No restrictions
Restrictions on data type	Only ASCII characters allowed	No restrictions. Binary data is also allowed
Security	Never use GET when sending passwords or other sensitive information!	POST is a little safer than GET because the parameters are not stored in browser history or in web server logs
Visibility	Data is visible to everyone in the URL	Data is not displayed in the URL

Race Condition

A race condition or race hazard is the behavior of electronic, software, or other system where the output is dependent on the sequence or timing of other uncontrollable events. It becomes a bug when events do not happen in the order the programmer intended. The term originates with the idea of two signals racing each other to influence the output first.

Race conditions can occur in electronics systems, especially logic circuits, and in computer software, especially multithreaded or distributed programs.

Race condition example



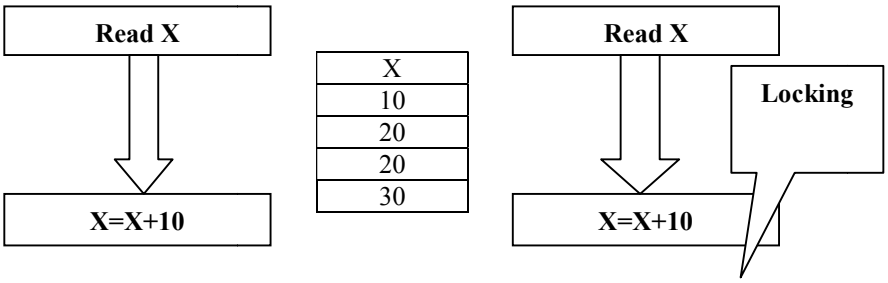
Consider the following set of operations:

Let left portion read first time

Left Portion	Right Portion
Read X=10	Read X=10
X=10+10	X=10+10
X=20	X=20
Actual X=20	**Actual X=30**

Solution

- ☞ Locking



What is Security Testing?

SECURITY TESTING is a type of Software Testing that uncovers vulnerabilities, threats, risks in a software application and prevents malicious attacks from intruders. The purpose of Security Tests is to identify all possible loopholes and weaknesses of the software system which might result in a loss of information, revenue, repute at the hands of the employees or outsiders of the Organization.

Types of Security Testing:

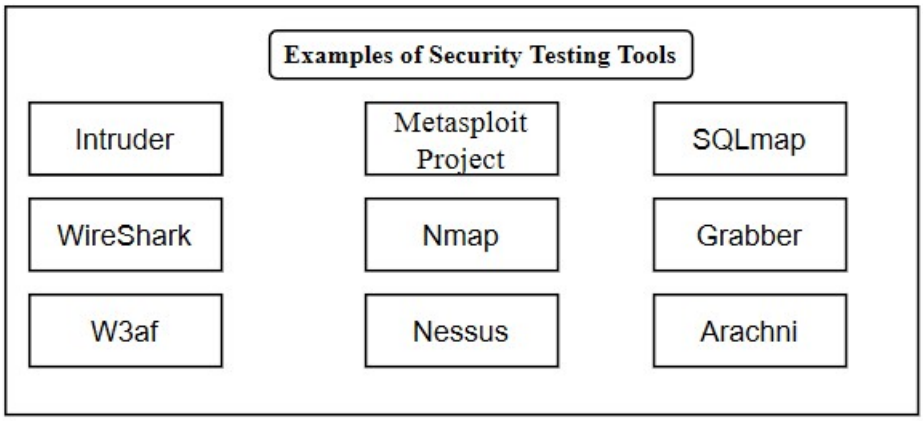
- ✓ Vulnerability scanning
- ✓ Security Scanning
- ✓ Penetration testing
- ✓ Risk Assessment
- ✓ Security Auditing
- ✓ Posture Assessment
- ✓ Ethical Hacking

Example Test Scenarios for Security Testing:

Sample Test scenarios to give you a glimpse of security test cases -

- ✓ A password should be in encrypted format
- ✓ Application or System should not allow invalid users
- ✓ Check cookies and session time for application
- ✓ For financial sites, the Browser back button should not work.

Some security testing tools:



Previous Year Problem

1. Which of the following is not a malware? *[Senior Officer (IT/ICT)-2018]*

a)Virus b)Worm c)Bug d)Trojan **Ans.:** c

2. Which of the following is not antivirus software? [*Senior Officer (IT/ICT)-2018*]

a) Win-pro b)AVG c) MeAfee d) Symantec **Ans.:** a

3. Elaboration of VIRUS is ----------*[SBL (SO-IT/ICT)-2013]*

a) Versatile Information Research Under Seize
b) Vital Information Resource Under Seize.
c) Volume of information Resource under Seize
d) Video Information Resource Under Seize **Ans.: b**

4. Which of the following is not a web server attack type? *[Senior Officer (IT/ICT)-2020]*

a) DOS attack b)Website Defacement using SQLi
c) Directory Traversal d) Password guessing **Ans.: d**

5. -------a means of regaining access to a compromised system by installing software or configuring existing software to enable remote access under attacker -defined conditions. *[Com (AP)-2020]*

a) Spyware b) Ransomware
c) Cross-site Scripting d) Backdoor **Ans.:** d

MODEL TEST

1. A firewall protects which of the following attacks?

a) Phishing b)Dumpster diving
c)Denial of Service (DoS) d) Shoulder surfing

2. SHA-**l has a message digest of**

a)160 bits b)512 bits c)628 bits d)820 bits

3. Message authentication is a service beyond

a)Message Confidentiality b)Message Integrity
c)Message Splashing d)Message Sending

4. In Message Confidentiality, transmitted message must make sense to only intended

a)Receiver b)Sender c)Modulor d)Translator

5. A hash function guarantees integrity of a message. It guarantees that message has not be

a)Replaced b)Over view c)Changed d)Violated.

6. To check integrity of a message, or document, receiver creates the

a)Hash-Table b)Hash Tag c)Hyper Text d)Finger Print

7. A digital signature needs a

a) Private-key system b)Shared-key system c)Public-key systemd)All of them

8. One way to preserve integrity of a document is through use of a

a) Eye-Rays b)Finger Print c)Biometric d)X-Rays

9. Compromising confidential information comes under _____
a) Bug b) Threat c) Vulnerability d) Attack

10. Encryption and decryption provide secrecy, or confidentiality, but not
a) Authentication b) Integrity c) Privacy d) All of the above

11. Who deploy Malwares to a system or network?
a) Criminal organizations, Black hat hackers, malware developers, cyber-terrorists
b) Criminal organizations, White hat hackers, malware developers, cyber-terrorists
c) Criminal organizations, Black hat hackers, software developers, cyber-terrorists
d) Criminal organizations, gray hat hackers, Malware developers, Penetration testers

12. When you use the word _____ it means you are protecting your data from getting disclosed.
a) Confidentiality b) Integrity c) Authentication d) Availability

13. When integrity is lacking in a security system, _____ occurs.
a) Database hacking b) Data deletion c) Data tampering d) Data leakage

14. _____ ensures the integrity and security of data that are passing over a network.
a) Firewall b) Antivirus c) Pentesting Tools d) Network-security protocols

15. _____enables a hacker to open a piece of program or application and re-build it with further features & capabilities.
a) Social engineering b) Reverse engineering
c) Planting malware d) Injecting code

MODEL TEST ANSWER

1	2	3	4	5	6	7	8	9	10
c	a	b	a	c	b	c	b	b	b
11	12	13	14	15					
a	a	c	d	b					