19261A04B1
S. DeviSri

CS Assignment - 1

1) Explain about the CAI Traid suggested for security?

A) CIA traid is designed to guide policies for information security within an organization. It stands for:

1) Confidentiality
2) Integrity
3) Availability

Confidentiality: It means that only the authorized systems can view classified information. Attacker may try to capture the data and gain access to information. This can be avoided by using encryption techniques to safeguard your data. VPN also helps data move securely over network.

Integrity: It is all about making sure that data has not been modified. Corruption of data is a failure to maintain data integrity.

Availability: This means that the network should be readily available to its users. This applies to system and to data. To ensure availability, the network administrator should maintain hardware, make regular upgradu, have a plan for fail-over and prevent bottleneck in a network. Attacks such as DOS or DDOS must be prevented by taking proper measures.

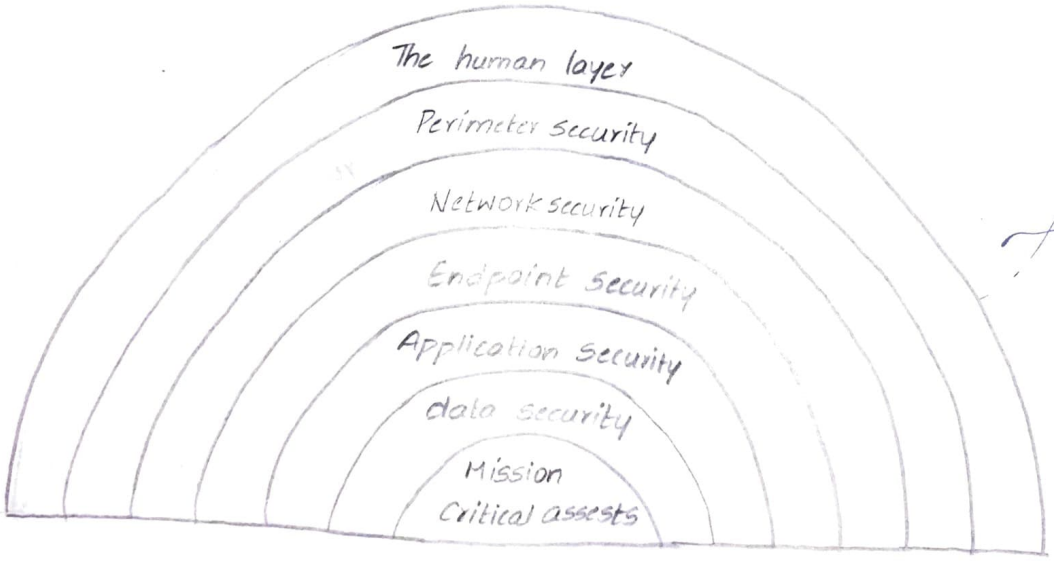
2) Write a neat ~~program~~ diagram explaining layers of security?

A) The 7 layers of Cybersecurity are:

1) Mission critical assests
2) Data security
3) Application security
4) End point security
5) Network security
6) perimeter security
7) The human layer

- The 7 layers of cybersecurity should center on the mission critical assests.

Mission critical assests - The data that needs to be protected.
Data security - controls, protect the storage and transfer of data.
Application security - Controls protect access to application, application access to assest, and the internal security of application
Endpoint Security - protect the connection between devices and the network.
Network security - protect an organization's network and prevent unauthorized access of network.
Perimeter Security - Controls include both the physical and digital security methodologies that protect the business overall.
The human layer - Controls include phishing simulations and access management controls that protect mission critical assests from a wide variety threats.



7-layers of cybersecurity

3) Discuss about various cyber threats.

A) Viruses: a sofware virus is designed in such a way that can be easily transmitted and often sent as email attachments. viruses corrupt and co-opt data, interfere with your security settings, generate spam and may even delete content.

Computer Worms :- they spread from one computer to the next by sending itself to all of the user's contacts and subsequently to all of the contact's contacts.

Trojans :- These malicious pieces of Software insert themselves into a legitimate program making the system vulnerable to the malware within.

Bogus Security Software :- tricks users to believe that their system has been infected with a virus.

Adware :- tracks your browsing habits and causes particular advertisements to pop up. Similarly Spyware, is an intrusion that may steal sensitive data from your systems.

Denial of Service (DOS) attack :- this occurs when hackers deluge a website with traffic, make it impossible for users to access it's content.

Phishing attacks :- are social engineering infiltrations whose goal is to wrongfully obtain senstive data.

SQL injections :- are network threats that involve using mallicious code to infiltrate cyber vulnerabilities in data systems. As a result, data can be stolen, changed or destroyed.

Man-in-the-middle attacks :- involve a third party intercepting and exploiting communications between two entities that should remain private.

Rookit tools: gain remote access to systems without permission and can lead to the installation of malware and the stealing of passwords and other data.

4) Write about Cyber Security Regulations. (IT Act)

4) A cybersecurity regulation comprises directives that safeguard information technology and computer systems with the purpose of forcing companies to protect their systems from attacks. Cyber law also called as IT law regarding information technology. It endoses aspects of contract, intellectual property, privacy and data protection laws. The indian cyber laws are governed by IT act, 2000. The ITA enacted by the parliment of India, highlights the grevious punishments and penalties safeguarding the e-governance, e-banking and e-commerce sectors

• Section 43 - applicable to people who damaged computer systems with owner permission. owner can claim compensation for entire damage.

• Section 66 - Applicable in case a person is found to dishonestly or fraudulently committing any act in section 43. The imprisonment can mount up to three years or a fine of 5 lakh.

• Section 66B - Incorporates the punishments for fraudulently receiving stolen communication devices, which confirms three years prison and can also be topped by Rs. 1 lakh fine, depending upon the severity

• Section 66C - This Section Scrutinizes the identity thefts related to imposter digital signatures, hacking passwords, or other distinctive identification features. If proven guilty, imprisonment of 3 years and 1 lakh fine.

• Section 66D - This section was inserted on-demand, focusing on punishing cheaters doing impersonation using computer resources.

Indian penal code (1980) and companies act of 2013 also play a major role in cybersecurity regulation.

5) Briefly explain about vision, mission and objectives of NSP.

A) National cyber security policy is a policy framework by Department of electronics and information Technology.

Vision: To build a secure and resilient cyberspace for citizens, business, and government and also to protect anyone from intervening in user's privacy.

Mission: To protect information and infrastructure in cyberspace, build capabilities to prevent and respond to cyber threat, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and co-operation.

Objective:

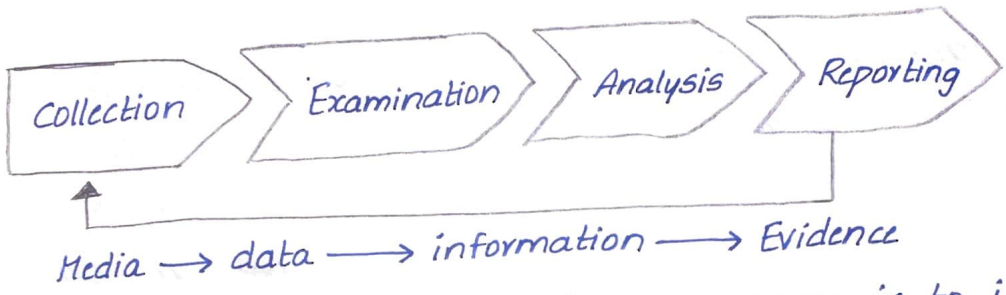
- To create a secure cyber ecosystem in the country, generate adequate trust and confidence in IT system and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.

To create an assurance framework for the design of security policies and promotion and enabling actions for compliance to global security standards.

- To strengthen the regulatory framework for ensuring a secure cyberspace ecosystem.
- To enhance and create National and sectoral level 24x7 mechanism for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective, predictive, preventive, protective response and recovery options.

6) Explain in detail the digital forensics life cycle?

A)



Collection: The first step in the forensic process is to identify potential sources of data and acquire data from them.

Examination: After data has been collected, the next phase is to examine the data, which involves assessing and extracting the relevant pieces of information from the collected data. This phase may also involve bypassing or mitigating OS or application features that obscure data and code, such as data compression, encryption and access control mechanisms.

Analysis: Once the relevant information has been extracted, the analyst should study and analyse the data to draw conclusions from it.

Reporting: The process of preparing and presenting the information resulting from the analysis phase. Many factors affect reporting, including the following:

a) Alternative Explanations: When the information regarding an event is incomplete, it may not be possible to arrive at explanation of what happened.

b) Audience Consideration

c) Actionable Information

7) What are the challenges in Computer Forensics ?

A) Digital forensic challanges are categorized into three major heads

• Technical challenges : digital forensic experts use forensic tools for collecting shreds of evidence against criminals and criminals use such tools for hiding, altering or removing the traces of their crime, this process is called Anti-forensic technique which is a major challenge in digital forensics world. Anti-forensic techniques include encryption, data hiding in storage space & covert channel which unfortunately is also used by criminals. Other technical challenges are operating in the cloud, time to archive data, skill gap, steganography.

• Legal challenges : The presentation of digital evidence is more difficult than its collection because there are many instances where the legal framework accuqires a soft approach and does not recognize every ascept of cyber forensics. Other legal challenges are privacy issues, Admissibility in courts, preservation of electronic evidence, power for gathering digital evidence, Analyzing a running computer.

• Resource challenges : As rate of crimes increase the amount of data increases and analyzing it becomes difficult because digital evidence is more sensitive compared to physical evidence. Types of resource challenges are change in technology and volume and replication.

8) What is mean by

i) Vulnerability: Weakness in an information system, internal controls or implementation that could be exploited or triggered by a threat source.

ii) Asset, Threat : An assest is any data, device of an organisation's system that is valuable.

An threat refers to any possible attack that seeks to unlawfully access of data or damage information.

iii) Active attacks, passive attacks : In active attack, attacker tries to modify the content of the messages.

In passive attack, attacker observes the messages and copies them.

iv) Cyber attack, Cyber crime: Cyber attacks are unwelcome attempts to steal, expose, alter or destroy information through unauthorized access.

CyberCrime is a crime that involves a computer and a network as a commission of a crime or as a target.

v) IP Spoofing: is the creation of internet protocol packets with a false source IP address for the purpose of impersonating another computer system.

vi) Cyber forensics: is the investigation of digital data gathered as evidence in criminal cases.

vii) digital evidence: is any probative information stored or transmitted in digital form that a party to a court case may use at trial.

viii) Chain of Custody: refers to the logical sequence that records the sequence of custody, control, transfer, analysis and disposition of electronic evidence in legal cases.