1 explain GDPR

The **General Data Protection Regulation (GDPR)** is the toughest privacy and security law in the world. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The regulation was put into effect on May 25, 2018. The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros.

With the GDPR, Europe is signaling its firm stance on data privacy and security at a time when more people are entrusting their personal data with cloud services and breaches are a daily occurrence. The regulation itself is large, far-reaching, and fairly light on specifics, making GDPR compliance a daunting prospect, particularly for small and medium-sized enterprises (SMEs).

Data protection principles

1. **Lawfulness, fairness and transparency** — Processing must be lawful, fair, and transparent to the data subject.
2. **Purpose limitation** — You must process data for the legitimate purposes specified explicitly to the data subject when you collected it.
3. **Data minimization** — You should collect and process only as much data as absolutely necessary for the purposes specified.
4. **Accuracy** — You must keep personal data accurate and up to date.
5. **Storage limitation** — You may only store personally identifying data for as long as necessary for the specified purpose.
6. **Integrity and confidentiality** — Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using encryption).
7. **Accountability** — The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles.

2 write a short note on network parameter security design

The main focus of perimeter security is the protection of networks, which includes the safeguarding of servers, workstations, and databases, amongst other things. If the network can survive any assault, it needs to be built from the ground up with security in mind.

Firewalls, VPNs, security policies, security awareness were some of the topics that were covered in previous posts. We also discussed the layered security or defense in depth approach. We will now see how see these different topics come together to form network perimeter security design for a fictitious eCommerce site. Perimeter security is securing the network (servers, workstations, databases to name a few) with different concepts. The network must be designed securely to withstand any type of attack.

Before designing an effective security plan for the network, there are three questions that have to be answered:

1. What is it that we are trying to protect?

We will have to determine what are the workstations, servers, databases and other devices that have to be protected.

2. What are the threats?

Next, we determine what are the different type of threats. Internet facing systems are always under the possibility of an attack. Other threats can also be from former employees who have access to vital resources.

3. And finally the business requirements of the organization.

Last but not least, the security design must meet the business goals of an organization. An eCommerce site with more online transactions will need a more robust security design than a site which just needs an online presence.

3 what do you mean by firewall and VPN

VPN:

A VPN (a virtual private network), changes your network address(IP) by conducting your computer address through a remote server into another location or shielding you from getting your private data leaked. This makes it

a secure choice for companies whose employees work from home or a remote location.

firewalls?

A firewall watches incoming and outgoing traffic on your network. Firewalls block attacks automatically and also allow you to set security preferences for what you let into your network or computer. If you don't program a firewall to block a certain kind of site, content, or traffic, it won't, even if that site has content that could hurt your system.

There are two types of firewalls:

1. Hardware or network firewalls

Hardware firewalls are physical devices that are placed between your computer and the internet. Their disadvantage is that they are separate devices that often require professional support for configuration and maintenance.

2. Software firewalls

Software firewalls are able to control the internet access and behavior of programs on your computer. Most computer operating systems (OSs) include a basic built-in software firewall feature, but firewall software is also available separately from computer stores and trusted online vendors.

The relationship between a VPN and a firewall:

- Firewalls stop cyberattacks by putting up a strong wall to protect users' private information. On the other hand, VPNs create a proxy network that hides your location from other people.
- A VPN gives you a secure way to connect to restricted sites, while a firewall can only add another layer of restrictions to sites you've already accessed.
- Firewalls let you choose which sites you don't want to be able to get to. With NordVPN, you can keep going to the same site for a long time.
- Firewalls are mainly used to block websites. NordVPN, however, is all about a private connection.

4 how to audit PAM

Since privileged access management (PAM) helps you protect critical assets and prevent unwanted changes to your network, it's critical that you include auditing as an essential component of your PAM strategy.

Step 1: Take Inventory - Identify Privileged Users (Human or Otherwise)

First, take an inventory of privileged accounts. Make a note of any users, human or machine, with the ability to modify networks and devices, add and update user profiles and privileges, or access confidential and sensitive data.

These may include:

- Human users with administrative permissions, including the ability to execute commands, make system changes, and grant or revoke access.

- Service accounts with the capacity to interact with an operating system, make changes and run scheduled tasks.
- Ephemeral infrastructure, including containers, Kubernetes, and serverless frameworks.
- Users outside of your organization, like third-party vendors and contractors.
- Privileged business users with access to sensitive data.

Step 2: Privileged Access Monitoring - Record and Replay

After you establish who has elevated access in your organization, you can begin to track and record privileged user activity. When auditing PAM, continuous observation is vital. According to Verizon's 2021 Data Breach Investigations Report, more than fifty percent of security breaches take months to detect. Consistently locating and monitoring privileged accounts helps you discover accidental or malicious handling of your data and critical systems before it becomes a problem.

Session recording and replay tools provide a contextualized understanding of who performed a behavior and when. You can monitor privileged accounts in real-time or replay sessions for incident management, training, or compliance.

As a guardrail against access control violations, host your session logs outside of the database they are monitoring and restrict write access for log admins to ensure that users cannot modify the data from the original input.

When auditing PAM, look for session monitoring tools that:

- Track every keystroke of an SSH or RDP session.
- View kubectl commands, API calls, and other k8s interactions.
- Observe queries from a variety of datasources.
- Record HTTP calls, including the headers and completion time.
- Monitor access gestures such as login attempts, user updates, and role changes.
- Collect and save audit logs from all sessions.

Retain access logs and other session monitoring data according to the regulatory requirements established in your PAM policy. A good rule of thumb is to keep your logs available for search and analysis for 90 days and retain encrypted archives for up to a year.

Step 3: Harness SIEM Tools - Analyze Privileged Account Activity

Next, it's time to analyze your logs. Modern Security Information and Event Management (SIEM) tools use machine learning to detect anomalous behavior and send alerts when user activity falls outside of the norm. These tools aggregate data from multiple sources, allowing you to correlate user access logs with other security events. More-detailed audit logs will yield richer SIEM outputs.

Favor tools that track:

- The addition or suspension of privileged users.
- Access of critical information, including protected or sensitive data.
- Signs of anomalous activity, like large file deletions.
- Updates to user roles or permission levels.
- Administrative changes to databases or servers.

SIEM tools generate a broad view of network activity while keeping a close eye on problems. They perform forensics if a security incident occurs and help prevent attacks by detecting unusual traffic patterns. Additionally, these tools can scan through a large volume of alerts from multiple systems and help you prioritize those with the highest risk to your organization. Not only does this save admins time and frustration, it also helps them determine the next right action to address the threat.

Step 4: Consider the Human Element - Review Privileged User Behavior

The last step in auditing PAM is auditing people.

Taking inventory gave you an overview of what to monitor. Session recordings gathered information about your network. And SIEM tools scanned that information to detect anomalous behavior. But PAM is only as effective as the humans who use it.

A 2018 survey by Accenture found that one in five healthcare employees would be willing to sell login credentials and other confidential data to unauthorized parties. Other industries are also at risk.

Thankfully, consistent, high-quality PAM auditing can make a difference. When it comes to security, regular access reviews help to establish collaboration

among departments, limiting the negative impact of bad actors and ensuring that any unmanaged accounts are properly deactivated.

5 explain analyse privilege account Activity

A privileged account is a user account with greater privileges than those of ordinary user accounts. Privileged accounts may access important data or systems or exercise administrative powers. For these reasons, it is especially important to secure privileged accounts to prevent unauthorized use.

Privileged accounts, including IT admin accounts, enable users to access an organization's business-critical systems and monetizable data. Users of these accounts are able to execute important tasks. They can:

- Install or remove software
- Upgrade the operating system
- Alter system or application configurations
- Access important files
- Access sensitive data such as credit card details or social security numbers

6 define ISO 20001 and its benefit

What Is ISO 27001?

ISO 27001 is an international standard for the implementation of an enterprise-wide Information Security Management System (ISMS), an organized approach to maintaining confidentiality, integrity and availability (CIA) in an organization. It offers double benefits — an excellent framework to comply with to protect information assets from malicious actors and a differentiating factor to give an organization an edge over its competitors. The global standard provides complete guidance on building, implementing, maintaining, and consistently improving the ISMS.

The establishment and implementation of ISMS depends upon various factors:

- ✔ Business objectives of the organization.
- ✔ Needs of the organization.
- ✔ Security requirements.
- ✔ Internal and external processes of the organization
- ✔ Size and structure of the organization.

Why Is ISO 27001 Required?

Complying with various mandatory requirements is not only a prerequisite but also a demanding, on-going process for all organizations. The recognized standard incorporates the requirements of different regulations, such as GDPR, NIST CSF, and others, to ensure that the implemented processes and services are secure, reliable, and of top quality.

ISO 27001 is now required more than ever before because it ensures that various information security risks, including cyber threats, vulnerabilities, and their impacts, get addressed with best security practices. It is also invaluable in terms of monitoring, reviewing, maintaining, and improving an organization's information security management system. An organization with a certified ISO 27001 standard demonstrates that the organization is aligned with the best security practices, assuring business partners and the existing customer base.

7 define ISO INFORMATION SECURITY STANDARDS

The International Organization for

Standardization (known as the ISO for short)

is a global organization that works to provide

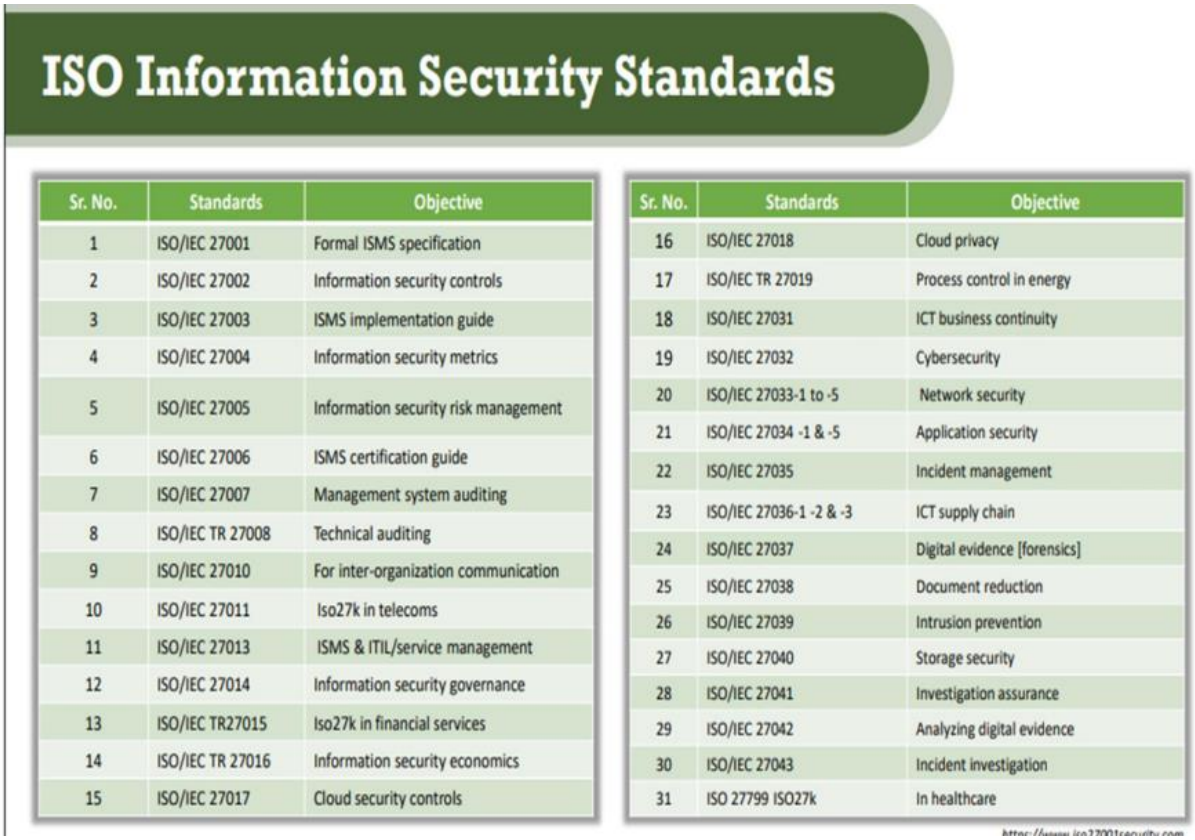
standardization across an array of products

and companies. Its main goal is to facilitate

trade, but its focus is on process

improvement, safety, and quality in several

areas.



ISO Information Security Standards

Sr. No.	Standards	Objective
1	ISO/IEC 27001	Formal ISMS specification
2	ISO/IEC 27002	Information security controls
3	ISO/IEC 27003	ISMS implementation guide
4	ISO/IEC 27004	Information security metrics
5	ISO/IEC 27005	Information security risk management
6	ISO/IEC 27006	ISMS certification guide
7	ISO/IEC 27007	Management system auditing
8	ISO/IEC TR 27008	Technical auditing
9	ISO/IEC 27010	For inter-organization communication
10	ISO/IEC 27011	Iso27k in telecoms
11	ISO/IEC 27013	ISMS & ITIL/service management
12	ISO/IEC 27014	Information security governance
13	ISO/IEC TR27015	Iso27k in financial services
14	ISO/IEC TR 27016	Information security economics
15	ISO/IEC 27017	Cloud security controls

Sr. No.	Standards	Objective
16	ISO/IEC 27018	Cloud privacy
17	ISO/IEC TR 27019	Process control in energy
18	ISO/IEC 27031	ICT business continuity
19	ISO/IEC 27032	Cybersecurity
20	ISO/IEC 27033-1 to -5	Network security
21	ISO/IEC 27034 -1 & -5	Application security
22	ISO/IEC 27035	Incident management
23	ISO/IEC 27036-1 -2 & -3	ICT supply chain
24	ISO/IEC 27037	Digital evidence [forensics]
25	ISO/IEC 27038	Document reduction
26	ISO/IEC 27039	Intrusion prevention
27	ISO/IEC 27040	Storage security
28	ISO/IEC 27041	Investigation assurance
29	ISO/IEC 27042	Analyzing digital evidence
30	ISO/IEC 27043	Incident investigation
31	ISO 27799 ISO27k	In healthcare

8 define data integration

Data integration is the process of combining data from different sources into a single,

unified view

 Data integration is the process of combining data from different sources to help data managers and executives analyze it and make smarter business

decisions. This process involves a person or system locating, retrieving, cleaning, and presenting the data.

 Data managers and/or analysts can run queries against this merged data to discover business

intelligence insights. With so many potential benefits, businesses need to take the time to align their goals with the right approach.

Types

Manual data integration: Manual data integration occurs when a data manager oversees all aspects

of the integration — usually by writing custom code. That means

connecting the different data sources, collecting the data, and cleaning it,

etc., without automation.

 Some of the benefits are:

 Reduced cost: This technique requires little maintenance and typically

only integrates a small number of data sources.

 Greater freedom: The user has total control over the integration.

 Some of the cons are:

 Less access: A developer or manager must manually orchestrate each

integration.

Manual data integration occurs when a data manager oversees all aspects

of the integration — usually by writing custom code. That means

connecting the different data sources, collecting the data, and cleaning it,

etc., without automation.

Middleware data integration: Middleware, a type of software, facilitates communication between

legacy systems and updated ones to expedite integration.

 Application-based integration: Software

applications locate, retrieve, and integrate data by making data from different sources and systems compatible with one another.

 Uniform access integration: A technique that retrieves and uniformly displays data, but leaves it in its original source.

 Common storage integration: An approach that retrieves and uniformly displays the data, but also makes a copy of the data and stores it.

9 explain life cycle of governance leader

10 explain threats

1. **Virus –** They have the ability to replicate themselves by hooking them to the program on the host computer like songs, videos etc and then they travel all over the Internet. The Creeper Virus was first detected on ARPANET. Examples include File Virus, Macro Virus, Boot Sector Virus, Stealth Virus etc.
2. **Worms –** Worms are also self-replicating in nature but they don't hook themselves to the program on host computer. Biggest difference between virus and worms is that worms are network-aware. They can easily travel from one computer to another if network is available and on the target machine they will not do much harm, they will, for example, consume hard disk space thus slowing down the computer.
3. **Trojan –** The Concept of Trojan is completely different from the viruses and worms. The name Trojan is derived from the 'Trojan Horse' tale in Greek mythology, which explains how the Greeks were able to enter the fortified city of Troy by hiding their soldiers in a big wooden horse given to the Trojans as a gift. The Trojans were very fond of horses and trusted the gift blindly. In the night, the soldiers emerged and attacked the city from the inside.

   Their purpose is to conceal themselves inside the software that seem legitimate and when that software is executed they will do their task of either stealing information or any other purpose for which they are designed.

   They often provide backdoor gateway for malicious programs or malevolent users to enter your system and steal your valuable data without your knowledge and permission. Examples include FTP Trojans, Proxy Trojans, Remote Access Trojans etc.

4. **Bots –**: can be seen as advanced form of worms. They are automated processes that are designed to interact over the internet without the need for human interaction. They can be good or bad. Malicious bot can infect one host and after infecting will create connection to the central server which will provide commands to all infected hosts attached to that network called **Botnet.**

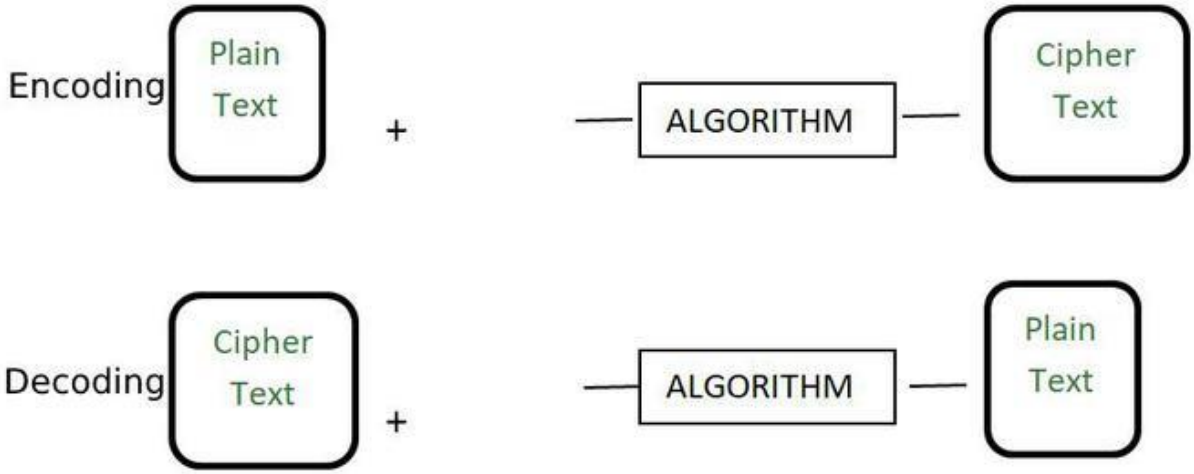
Malware on the **basis of Actions:**

1. **Adware –** Adware is not exactly malicious but they do breach privacy of the users. They display ads on a computer's desktop or inside individual programs. They come attached with free-to-use software, thus main source of revenue for such developers. They monitor your interests and display relevant ads. An attacker can embed malicious code inside the software and adware can monitor your system activities and can even compromise your machine.
2. **Spyware –** It is a program or we can say software that monitors your activities on computer and reveal collected information to an interested party. Spyware are generally dropped by Trojans, viruses or worms. Once dropped they install themselves and sits silently to avoid detection.

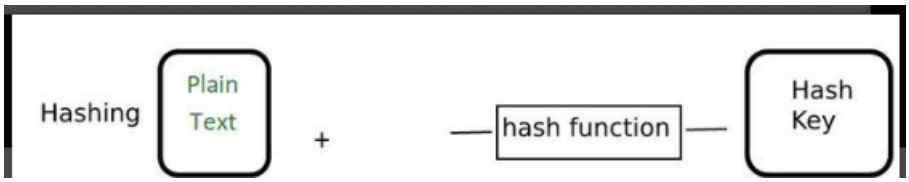
   One of the most common example of spyware is KEYLOGGER. The basic job of keylogger is to record user keystrokes with timestamp. Thus capturing interesting information like use

11 how is encryption different from hashing

Encryption is the process of converting a normal readable message known as plaintext into a garbage message or not readable message known as Ciphertext. The ciphertext obtained from the encryption can easily be transformed into plaintext using the encryption key



Hashing is the process of converting the information into a key using a hash function. The original information cannot be retrieved from the hash key by any means. Generally, the hash keys are stored in the database and they are compared to check whether the original information matches or not. They are generally used to store the passwords for login.



Basis	Hashing	Encryption
Definition	It is a process to convert information to a shorter fixed value known as the key that is used to represent the original information.	It is the process to encode data securely such that only the authorized user who knows the key or password is able to retrieve the original data for everyone else it is just garbage.
Purpose	The purpose of hashing is indexing and retrieving items from the database. The process is very fast.	The purpose of encryption is to transform data to keep it secret from others.
Reverse Process	The hash code or key can not be reversed to the original information by any means. It can only be mapped and the hash code is checked if the hash code is the same the information is the same otherwise not. The original information can not be retrieved.	The original information can be easily retrieved if we know the encryption key and algorithm used for encryption.
Secure	It is more secure in comparison to encryption.	It is less secure in comparison to hashing.
Creation of file	Generally, it tries to generate a new key for each information passed to the hash function but on rare occasions, it might generate the same key popularly known as a collision.	It will always generate a new key for each information.
Example	MD5, SHA256	RSA, AES and Blowfish
Output	The output of a hashing algorithm is a fixed-size hash value	the output of an encryption algorithm is ciphertext of the same size or larger than the original data
Length of information	The hashed information is generally of small and fixed length. It does not grow with the increase in the information length of information.	The encrypted information is not of fixed length. It grows with the increase in length of information.
key management	Hashing does not require a secret key or algorithm to produce a hash value	encryption requires a secret key or algorithm to encrypt and decrypt data.

12 explain CIA

The three letters in "CIA triad" stand for Confidentiality, Integrity, and Availability. The CIA triad is a common model that forms the basis for the

development of security systems. They are used for finding vulnerabilities and methods for creating solutions. (Fortinet)

• Confidentiality: Confidentiality involves the efforts of an organization to make sure data is kept secret or private. A key component of

maintaining confidentiality is making sure that people without proper authorization are prevented from accessing assets important to your business.

• Integrity: Integrity involves making sure your data is trustworthy and free from tampering. The integrity of your data is maintained only if the data is authentic, accurate, and reliable.

• Availability: Systems, networks, and applications must be functioning as they should and when they should. Also, individuals with access to

specific information must be able to consume it when they need to, and

getting to the data should not take an inordinate amount of time.

13 what is data leakage

Data leakage is the unauthorized transmission of data from within an organization to an external destination or recipient. The term can be used to describe data that is transferred electronically or physically. Data leakage threats usually occur via the web and email, but can also occur via mobile data storage devices such as optical media, USB keys, and laptops.

Barely a day goes by without a confidential data breach hitting the headlines. Data leakage, also known as low and slow data theft, is a huge problem for **data security**, and the damage caused to any organization, regardless of size or industry, can be serious. From declining revenue to a tarnished reputation or massive financial penalties to crippling lawsuits, this is a threat that any organization will want to protect themselves from.

ypes of Data Leakage

There are many different types of data leakage and it is important to understand that the problem can be initiated via an external or internal source. Protective measures need to address all areas to ensure that the most common data leakage threats are prevented.

The Accidental Breach

"Unauthorized" data leakage does not necessarily mean intended or malicious. The good news is that the majority of data leakage incidents are accidental. For example, an employee may unintentionally choose the wrong recipient when sending an email containing confidential data. Unfortunately, unintentional data leakage can still result in the same penalties and reputational damage as they do not mitigate legal responsibilities.

The Disgruntled or Ill-Intentioned Employee

When we think of data leakages, we think about data held on stolen or misplaced laptops or data that is leaked over email. However, the vast majority of data loss does not occur over an electronic medium; it occurs via printers, cameras, photocopiers, removable USB drives and even dumpster diving for discarded documents. While an employee may have signed an employment contract that effectively signifies trust between employer and employee, there is nothing to stop them from later leaking confidential information out of the

building if they are disgruntled or promised a hefty payout by cybercriminals. This type of data leakage is often refered to as **data exfiltration**

Electronic Communications with Malicious Intent

Many organizations give employees access to the internet, email, and instant messaging as part of their role. The problem is that all of these mediums are capable of file transfer or accessing external sources over the internet. **Malware** is often used to target these mediums and with a high success rate. For example, a cybercriminal could quite easily **spoof** a legitimate business email account and request sensitive information to be sent to them. The user would unwittingly send the information, which could contain financial data or sensitive pricing information.

Phishing attacks are another cyber attack method with a high data leakage success rate. Simply by clicking on a link and visiting a web page that contains malicious code could allow an attacker to access a computer or network to retrieve the information they need.

14 define cryptography

Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.

Modern cryptography techniques include algorithms and ciphers that enable the encryption and decryption of information, such as 128-bit and 256-bit encryption keys.

Services: Cryptography can provide the following services: •Confidentiality (secrecy) •Integrity (anti-tampering) •Authentication •Non-repudiation.

Types

Symmetric Key Cryptography ♣ Asymmetric Key Cryptography ♣ Hash Functions

15 explain blackhead amd whitehead

Black hat hackers are criminals who break into computer networks with malicious intent. They may also release malware that destroys files, holds

computers hostage, or steals passwords, credit card numbers, and other personal information.

Black hats are motivated by self-serving reasons, such as financial gain, revenge, or simply to spread havoc. Sometimes their motivation might be ideological, by targeting people they strongly disagree with.

White hat hackers – sometimes also called "ethical hackers" or "good hackers" – are the antithesis of black hats. They exploit computer systems or networks to identify their security flaws so they can make recommendations for improvement.

16 what do you mean by botnet

A Network of compromised computers is called a botnet. Compromised computers are also called **Zombies or Bots**. This software is mostly written in C++ & C. The main motive of botnet is that it starts with the dark side of the internet which introduced a new kind of Crime called Cybercrime**.**
Among the malware (malicious software) botnet is the most **widespread and severe threat**. Several large institutions, government Botnet Communication
At first, those who want to be botmaster finds the target system (here target system means finding the vulnerable system), then use popular social engineering techniques like phishing, click fraud, etc to install a small (Kbs) executable file into it. A small patch has been included in the code, making it not visible even with the running background process. A naive user won't even come to know that his/her system became part of a bot army. After infection, the bot looks for the channel through which it can communicate with its master. Mostly Channel (command and Control channel) uses the existing protocol to request the command and receive updates from the master, so if anyone tries to look at the traffic behavior then it will be quite difficult to figure it out. Botmaster is used to write scripts to run an executable file on different OS.

firm associated with the internet became the victim of this malware. This kind of malicious software is freely available in the market for lease. It can be used in DDoS attacks (Smurf Attacks), Phishing, Extortion, etc.