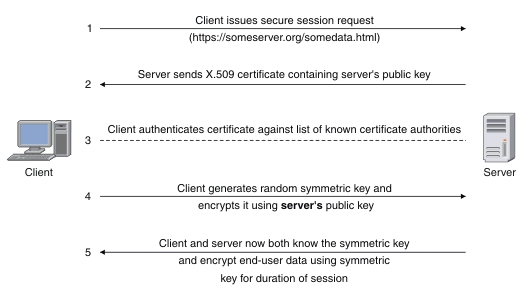
**BE ICS**

**Unit Test -2 Question Bank**

1. Explain the SSL handshake

SSL is a security protocol that provides communications privacy. SSL enables client and server applications to communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery. SSL applies only to internet protocols, and is not applicable to SNA.

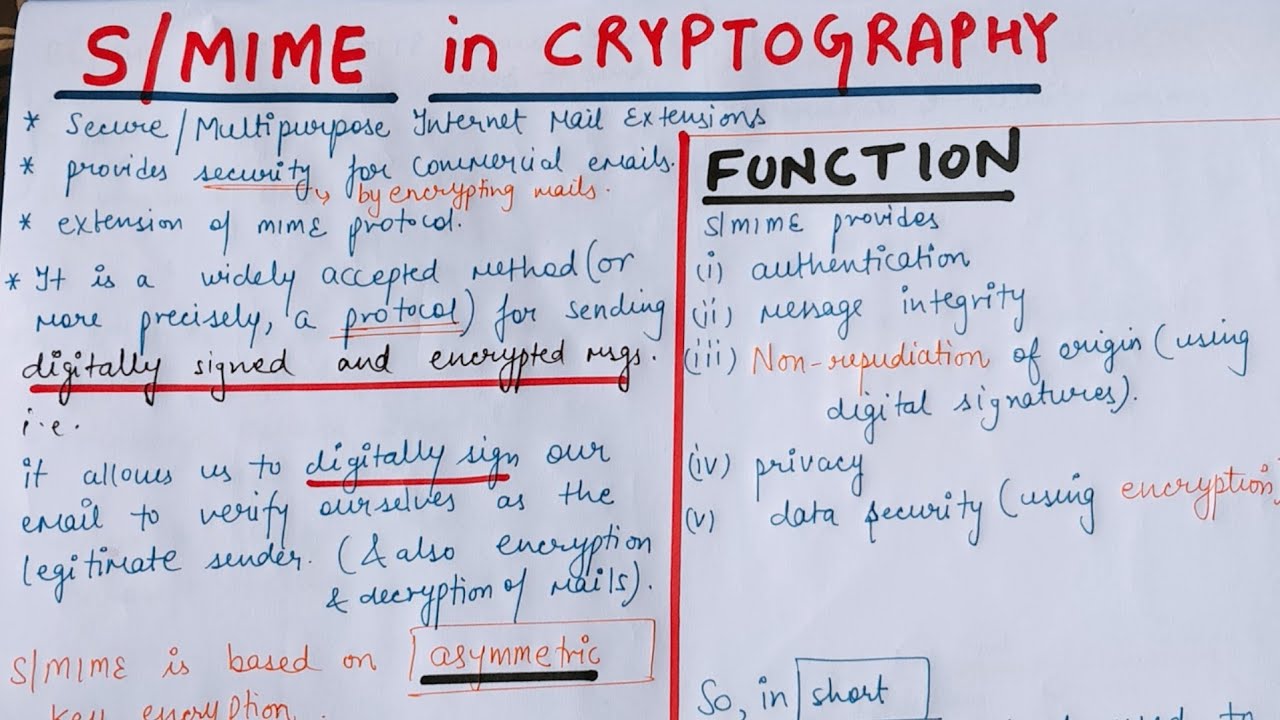
An SSL connection is established though a handshake (a series of communications exchanges) between the client and the server.

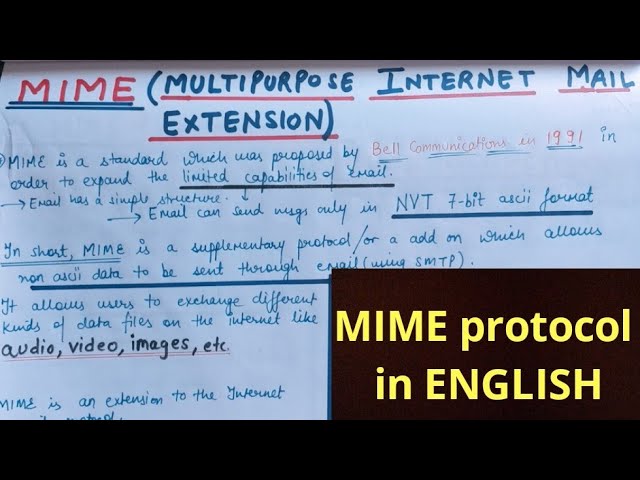


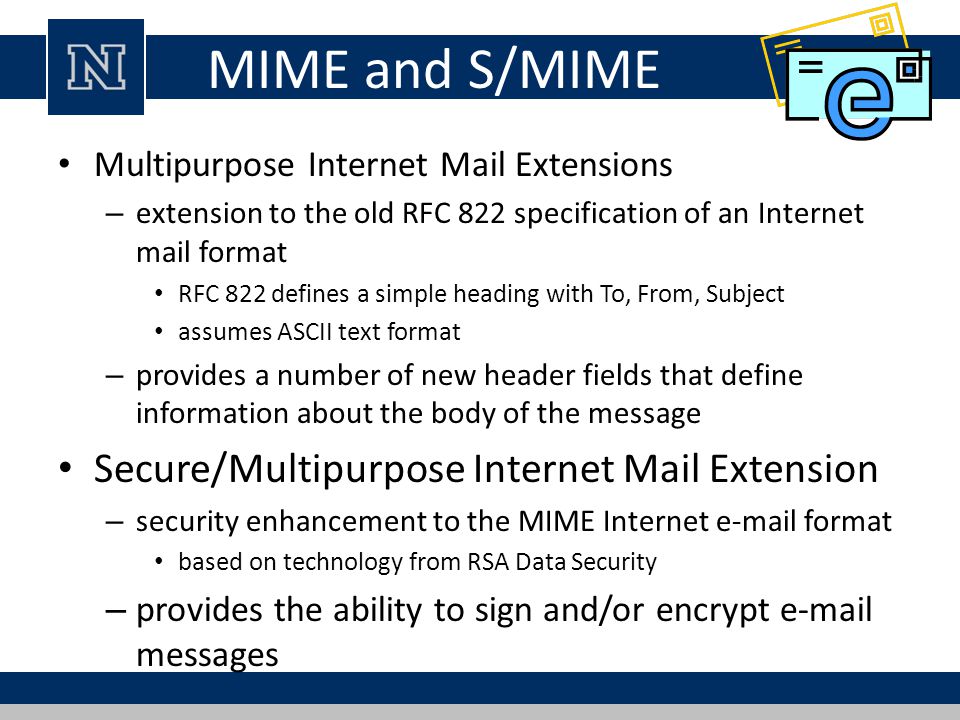
1. The client sends a request to the server for a secure session. The server responds by sending its X.509 digital certificate to the client.
2. The client receives the server's X.509 digital certificate.
3. The client authenticates the server, using a list of known certificate authorities.
4. The client generates a random symmetric key and encrypts it using server's public key.
5. The client and server now both know the symmetric key and can use the SSL encryption process to encrypt and decrypt the information contained in the client request and the server response.

2. Difference between MIME and SMIME.

<https://www.geeksforgeeks.org/difference-between-pgp-and-s-mime/>







3. Explain Pretty Good Privacy.

* PGP was designed to provide all four aspects of security, i.e., privacy, integrity, authentication, and non-repudiation in the sending of email.
* PGP uses a digital signature (a combination of hashing and public key encryption) to provide integrity, authentication, and non-repudiation. PGP uses a combination of secret key encryption and public key encryption to provide privacy. Therefore, we can say that the digital signature uses one hash function, one secret key, and two private-public key pairs.
* PGP is an open source and freely available software package for email security.
* PGP provides authentication through the use of Digital Signature.
* It provides confidentiality through the use of symmetric block encryption.
* It provides compression by using the ZIP algorithm, and EMAIL compatibility using the radix-64 encoding scheme.

4. Difference between SSL and TLS.

|  |  |  |
| --- | --- | --- |
| S.NO | SSL | TLS |
| 1. | SSL stands for Secure Socket Layer. | TLS stands for Transport Layer Security. |
| 2. | SSL (Secure Socket Layer) supports **Fortezza** algorithm. | TLS (Transport Layer Security) does not supports **Fortezza** algorithm. |
| 3. | SSL (Secure Socket Layer) is the 3.0 version. | TLS (Transport Layer Security) is the 1.0 version. |
| 4. | In SSL( Secure Socket Layer), Message digest is used to create master secret. | In TLS(Transport Layer Security), Pseudo-random function is used to create master secret. |
| 5. | In SSL( Secure Socket Layer), Message Authentication Code protocol is used. | In TLS(Transport Layer Security), Hashed Message Authentication Code protocol is used. |
| 6. | SSL (Secure Socket Layer) is complex than TLS(Transport Layer Security). | TLS (Transport Layer Security) is simple. |
| 7. | SSL (Secure Socket Layer) is less secured as compared to TLS(Transport Layer Security). | TLS (Transport Layer Security) provides high security. |

5. Difference between IPV4 and IPV6.

| **IPv4** | **IPv6** |
| --- | --- |
| IPv4 has a 32-bit address length | IPv6 has a 128-bit address length |
| It Supports Manual and DHCP address configuration | It supports Auto and renumbering address configuration |
| In IPv4 end to end, connection integrity is Unachievable | In IPv6 end to end, connection integrity is Achievable |
| It can generate 4.29×109 address space | Address space of IPv6 is quite large it can produce 3.4×1038 address space |
| The Security feature is dependent on application | IPSEC is an inbuilt security feature in the IPv6 protocol |
| Address representation of IPv4 is in decimal | Address Representation of IPv6 is in hexadecimal |
| Fragmentation performed by Sender and forwarding routers | In IPv6 fragmentation performed only by the sender |
| In IPv4 Packet flow identification is not available | In IPv6 packet flow identification are Available and uses the flow label field in the header |
| In IPv4 checksum field is available | In IPv6 checksum field is not available |
| It has broadcast Message Transmission Scheme | In IPv6 multicast and anycast message transmission scheme is available |
| In IPv4 Encryption and Authentication facility not provided | In IPv6 Encryption and Authentication are provided |
| IPv4 has a header of 20-60 bytes. | IPv6 has header of 40 bytes fixed |

6. Explain the working of Secure Electronic Transaction.

Secure electronic transaction (SET) was an early communications protocol used by e-commerce websites to secure electronic debit and credit card payments. Secure electronic transaction was used to facilitate the secure transmission of consumer card information via electronic portals on the internet. Secure electronic transaction protocols were responsible for blocking out the personal details of card information, thus preventing merchants, hackers, and electronic thieves from accessing consumer information.

participants who are involved in the SET process:

**Cardholder**

**Merchant**

**Issuer**

**Acquirer**

**Payment Gateway**

**Certification Authority**

Secure Electronic Transaction works as follows:

#### Step 1: Customer Open an Account

The customer opens a credit card account like a master card or visa with a bank, i.e. issuer that supports electronic payment transactions and the secure electronic transaction protocol.

#### Step 2: Customer Receive a Certificate

Once the customer identity is verified (Verification can be done by using a passport, business documents or other documents), it receives a digital certificate which is issued by CA (Certificate Authority). This certificate contains customer details like name, public key, expiry date, certificate number, etc.

#### Step 3: Merchant Receives a Certificate

The merchant who wants to accept certain credit card brands must process a digital certificate for trustworthiness.

#### Step 4: Customer Place an Order

It is a shopping cart process where customers borrow an item from the available list, search for the specific item according to requirements, and place the order. Once the customer places the orders, the merchant, in return, sends the details of the order, such as a list of items selected, their quantity and price, total bill, etc., to maintain a record of the order at the customer site.

#### Step 5: Merchant is Verified

Merchant also sends a digital certificate to the customer to ensure the customers that they are dealing with an authorized or valid merchant.

#### Step 6: The Order and Payment Details Are Sent

Along with the customer’s digital certificate customer also sends an order and payment details to the merchant. The order part is used to confirm the transaction with the reference of items that are mentioned in the order form. The payment part contains the credit card( master card or visa) details. This payment information is in encrypted form; even the merchant cannot read it. The customer certificate ensures the merchant of a customer’s identity.

#### Step 7: Merchant Requests Payment Authorization

Once the merchant gets the customer’s payment details, it transfers them to the payment gateway via the acquirer and requests the payment gateway to authorize the payment details. This process ensures start the customer credit card is valid, and the credit limit is not breached.

#### Step 8: Payment Gateway Authorizes the Payment

Using the credit card information received from the merchant, the payment gateway cross verify the customer’s credit card with the help of the issuer. Based on the verification result, it either authorizes the payment or rejects the payment.

#### Step 9: Merchant Confirm the Order

Assuming that the payment gateway authorizes the payment, merchants send confirmation of the order to the customer.

#### Step 10: Merchant Provides a Goods and Services

Now the merchant provides goods and services according to the customer’s order.

#### Step 11: Merchant Request Payment

The merchant sends a request to the payment gateway for making payment. After that, the payment gateway interacts with various financial organizations such as the issuer, acquirer and the clearinghouse to effect the payment from the customer’s account to the merchant’s account.

7. What is Firewall ? Explain different type of Firewall? What are the benefits and limitations of firewall?

* Firewalls are used to prevent unauthorized Internet users from accessing private networks connected to the Internet. All data entering or leaving the intranet pass through the firewall, which examines each packet and blocks those that do not meet the specified security criteria.
* Firewall is a software program (or a hardware) that protects the network of computers from being compromised with hacker initiated cyber-attacks. It works as the first line of defense in network security with efficient monitoring of private network’s traffic. It prevents unauthorized access to the network and can block messages linking to unwanted content.

**Capabilities**:

* A firewall defines a single choke point that blocks malicious traffic. The use of a single choke point simplifies security management because security capabilities are consolidated on a few points.
* A firewall is an excellent location for monitoring security-related events. Audits and alarms can be implemented on the firewall system.
* A firewall is a convenient platform for several internet functions that are not security related. 4. A firewall can serve as a platform for IPSEC.

**Limitations**

* It cannot protect against attacks that by-pass the firewall.
* It may not protect against internal threats when an insider collaborates with an outside adversary. An attacker may be able to break into network by completely bypassing the firewall, if he can find a ``helpful'' insider who can be fooled into giving access to a modem pool.
* Firewalls cannot protect against tunneling over most application protocols. For example, firewall cannot protect against the transfer of virus-infected programs or files.

Types:

1. Packet Filtering Firewalls
2. Circuit Level Gateways
3. Application Level Gateways
4. Stateful Multilayer Inspection

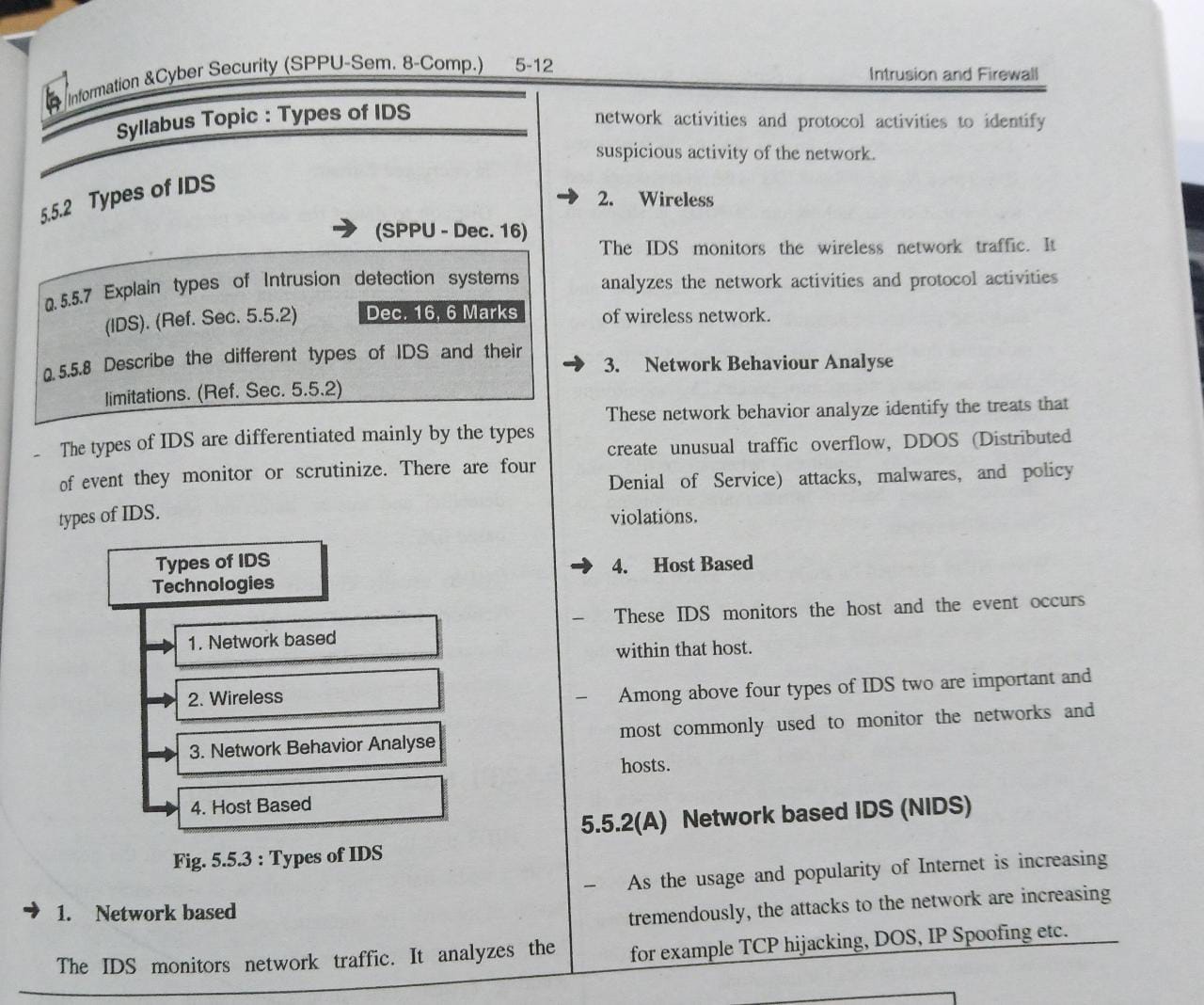
8. What is IDS?

An **Intrusion Detection System (IDS)** is a system that monitors **network traffic** for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for the harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.

Although intrusion detection systems monitor networks for potentially malicious activity, they are also disposed to false alarms. Hence, organizations need to fine-tune their IDS products when they first install them. It means properly setting up the intrusion detection systems to recognize what normal traffic on the network looks like as compared to malicious activity.

Intrusion prevention systems also monitor network packets inbound the system to check the malicious activities involved in it and at once send the warning notifications.

9. Explain different types of IDS.



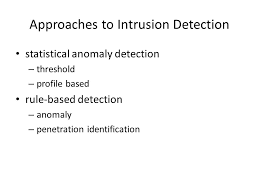
10. What are three benefits that can be provided by an intrusion detection system?

* **Fewer security incidents.** While connected units typically do not notice any changes, the IPS ensures less disruption for university systems and a reduced number of security incidents.
* **Selective logging.** The IPS only records network activity when it takes action, maintaining the privacy of network users.
* **Privacy protection.** The IPS compares network traffic against a list of known malicious traffic and does not store or view content.
* **Reputation-managed protection.** The IPS subscribes to a reputation-based list of known malicious sites and domains, which it uses to proactively protect the university.
* **Multiple threat protection.** The IPS offers zero-day threat protection, mitigates brute force password attempts, and provides protection against availability threats, such as DDoS and DoS attempts. **Dynamic threat response.** The IPS can be fine-tuned to recognize and respond to particular threats, allowing the university to react to identified threats to university business.

11. What is difference between statistically anomaly detection and rule based intrusion detection.

In a Rule-based intrusion detection system, **an attack can either be detected if a rule is found in the rule base or goes undetected if not found**. If this is combined with FIDS, the intrusions went undetected by RIDS can further be detected.

Anomaly detection is **the identification of rare events, items, or observations which are suspicious because they differ significantly from standard behaviors or patterns**. Anomalies in data are also called standard deviations, outliers, noise, novelties, and exceptions.



1. If an intrusion is detected quickly enough, the intruder can be identified and ejected from the system before any damage is done or any data are compromised. Even if the detection is not sufficiently timely to preempt the intruder, the sooner that the intrusion is detected, the less the amount of damage and the more quickly that recovery can be achieved. 2. An effective intrusion detection system can serve as a deterrent, so acting to prevent intrusions. 3. Intrusion detection enables the collection of information about intrusion techniques that can be used to strengthen the intrusion prevention facility

12. List and briefly define four techniques used avoid guessable passwords.

User education: Users can be told the importance of using hard-to-guess passwords and can be provided with guidelines for selecting strong passwords

Computer-generated passwords: Users are provided passwords generated by a computer algorithm.

Reactive password checking: the system periodically runs its own password cracker to find guessable passwords. The system cancels any passwords that are guessed and notifies the user.

Proactive password checking: a user is allowed to select his or her own password. However, at the time of selection, the system checks to see if the password is allowable and, if not, reiects it.

13. Explain PII (Personally Identifiable Information).

Personally Identifiable Information (PII) is a legal term pertaining to information security environments. While PII has several formal definitions, generally speaking, it is information that can be used by organizations on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

Personally identifiable information, or PII, is any data that could potentially be used to identify a particular person. Examples include a full name, Social Security number, driver’s license number, bank account number, passport number, and email address.

14. What is Cyber Stalking?

Cyberstalking refers to the use of the internet and other technologies to harass or stalk another person online, and is potentially a crime in the United States. This online harassment, which is an extension of [cyberbullying](https://www.verywellmind.com/the-psychology-of-cyberbullying-5086615) and in-person stalking, can take the form of e-mails, text messages, social media posts, and more and is often methodical, deliberate, and persistent.

Most of the time, the interactions do not end even if the recipient expresses their displeasure or asks the person to stop. The content directed at the target is often inappropriate and sometimes even disturbing, which can leave the person feeling fearful, distressed, anxious, and worried.

Here are some examples of things people who cyberstalk might do:

* Post rude, offensive, or suggestive [comments online](https://www.verywellmind.com/mental-health-effects-of-reading-negative-comments-online-5090287)
* Follow the target online by joining the same groups and forums
* Send threatening, controlling, or lewd messages or emails to the target
* Use technology to threaten or blackmail the target
* Tag the target in posts excessively, even if they have nothing to do with them
* Comment on or like everything the target posts online
* Create fake accounts to follow the target on [social media](https://www.verywellmind.com/social-media-and-depression-5085354)
* Message the target repeatedly

15. Difference between PIA and SORN.

16. Give few examples of PII data.

* Full name
* [Social Security Number](https://www.investopedia.com/terms/s/ssn.asp) (SSN)
* Driver’s license
* [Mailing address](https://www.investopedia.com/terms/t/taxhome.asp)
* Credit card information
* Passport information
* Financial information
* Medical records

17. Explain PII confidentiality impact level with example.

PII confidentiality impact levels range from low, moderate or high to indicate the potential harm that could result to an individual or organization if the data was accessed, used or disclosed.

Each organization needs to decide on what factors it will use to determine impact levels and then create and operationalize the appropriate policies, procedures and controls. That said, there are six general factors:

1. **Identifiability:**How easy can the PII be used to identify a specific individual?
2. **Quantity of PII:**How many people would be exposed in a data breach?
3. **Data field sensitivity:**How sensitive is each individual PII data element?
4. **Context of use:**How is the PII being collected, stored, used, processed, disclosed or disseminated?
5. **Obligations to protect confidentiality:**Does your organization have any legal or regulatory obligations to protect PII? Obligations include laws, regulations or other mandates like the Privacy Act, General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA) and OMB guidance
6. **Access to and location of PII:**Who can access the PII and where can they access it from?

18. Explain few cybercrimes against organization

Cybercrime against organization and society mainly includes **unauthorized access of computer, password sniffing, denial of service attacks, malware attacks, crimes emanating from usenet group, industrial spying/espionage, network intrusions, forgery, web-jacking** etc.

A password sniffer is **a software application that scans and records passwords that are used or broadcasted on a computer or network interface**. It listens to all incoming and outgoing network traffic and records any instance of a data packet that contains a password.

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.

A network intrusion refers to **any unauthorized activity on a digital network**. Network intrusions often involve stealing valuable network resources and almost always jeopardize the security of networks and/or their data.

**Illegally seeking control of a website by taking over a domain** is know as Web Jacking. In web jacking attack method hackers compromises with the domain name system (DNS) that resolves website URL to IP address but the actual website is never touched.

19. What are the activities of cyber forensic.

Cyber forensics is a process of extracting data as proof for a crime (that involves electronic devices) while following proper investigation rules to nab the culprit by presenting the evidence to the court. Cyber forensics is also known as computer forensics. The main aim of cyber forensics is to maintain the thread of evidence and documentation to find out who did the crime digitally. Cyber forensics can do the following:

* It can recover deleted files, chat logs, emails, etc
* It can also get deleted SMS, Phone calls.
* It can get recorded audio of phone conversations.
* It can determine which user used which system and for how much time.
* It can identify which user ran which program.
* **Identification:** The first step of cyber forensics experts are to identify what evidence is present, where it is stored, and in which format it is stored.
* **Preservation:**After identifying the data the next step is to safely preserve the data and not allow other people to use that device so that no one can tamper data.
* **Analysis:**After getting the data, the next step is to analyze the data or system. Here the expert recovers the deleted files and verifies the recovered data and finds the evidence that the criminal tried to erase by deleting secret files. This process might take several iterations to reach the final conclusion.
* **Documentation:**Now after analyzing data a record is created. This record contains all the recovered and available(not deleted) data which helps in recreating the crime scene and reviewing it.
* **Presentation:**This is the final step in which the analyzed data is presented in front of the court to solve cases.