1.	A/An ______________ attack attempts to learn or make use of information from the system but does not affect system resources.
Ans.	passive
2.	The ___________ attack is a variation of the brute force attack which narrows the field by selecting specific target accounts and using a list of commonly used passwords instead of random combinations.
Ans.	dictionary
3.	Risk can also be defined as: a) Risk = Vulnerability X Threat b) Risk = Threat + Vulnerability c) Risk = Threat X Exploit d) Risk = Exploit X Vulnerability
Ans.	a) Risk = Vulnerability X Threat
4.	Vulnerability refers to a new or newly discovered incident with the potential to do harm to a system or your overall organization. (True/False)
Ans.	False
5.	What are the three main security principles?
Ans.	1. Confidentiality 2. Integrity 3. Availability
6.	Laws are written and approved by governments while ethics comes from people's awareness of what is right and what is wrong. (True/False)
Ans.	True
7.	Which of the following strategies does not come under the risk control: a) Defend b) Mitigate c) Transfer d) Aggravate
Ans.	d) Aggravate
8.	As per the guideline of MeitY, the login password must be hashed using_________________.
Ans.	SHA2
9.	The ______________ methods can be used to pass the parameter as values from one page to another, as per the guideline of MeiTY.
Ans.	post
10.	A __________________ attack is a type of cyberattack where a malicious actor inserts him/herself into a conversation between two parties, impersonates both parties and gains access to information that the two parties were trying to send to each other.
Ans.	Man-In-The-Middle
11.	List the components of an Information System.
Ans.	Following are the components of an Information Systems: Software, Hardware, Data, People, Procedures, and Net
12.	Which of the following attack is likely to result in identity theft? a) Phishing attack b) DoS attack c) Virus infection d) None of these
Ans.	a) Phishing attack
13.	A _________ is a category of network attack in which an attacker detects a data transmission and fraudulently has it delayed or repeated. a) Replay attack b) Phishing attack c) MITM attack d) DoS attack
Ans.	a) Replay attack
14.	XSS can be used in which of the following languages/environments: a) ActiveX b) Javascript c) VB Script d) All of the Above
Ans.	d) All of the Above
15.	Risk management involves three major undertakings, what are they?
Ans.	Risk Identification, Risk Assessment, and Risk Control.
16.	A _________________ attack is a type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service.
Ans.	Denial-of-Service (DoS)
17.	A reflected XSS attack is also known as ________________.
Ans.	non-persistent XSS attack
18.	When there is an excessive amount of data flow, which the system cannot handle, the ________________ attack takes place. a) Database crash attack b) DoS (Denial of Service) attack c) Data overflow Attack d) Buffer Overflow attack
Ans.	d) Buffer Overflow attack
19.	Compromising a user's session for exploiting the user's data and do malicious activities or misuse user's credentials is called __________ a) Session Hijacking b) Session Fixation c) Cookie stuffing d) Session Spying
Ans.	a) Session Hijacking
20.	Stuxnet is a ________ a) Worm b) Virus c) Trojan d) Antivirus
Ans.	a) Worm

21.	Define information security.
Ans.	According to the SANS Institute “Information security refers to the processes and methodologies that are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification or disruption.”
22.	Differentiate between Information Security, Cyber Security and Network Security.
Ans.	Information Security refers to the processes and methodologies that are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification or disruption. Cyber Security, a subset of information security, is the practice of defending organization’s networks, computers and data from unauthorized digital access, attack or damage by implementing various processes, technologies and practices. Network Security is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure platform for computers, users and programs to perform their permitted critical functions within a secure environment.
23.	Define the following terms: a) Vulnerability b) Threat c) Exploit d) Risk
Ans.	a) Vulnerability: Vulnerability is a cyber-security term that refers to a flaw in a system that can leave it open to attack. Vulnerability may also refer to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat. b) Threat: A threat refers to a new or newly discovered incident with the potential to do harm to a system or your overall organization. There are three main types of threats – natural threats (e.g., floods or a tornado), unintentional threats (such as an employee mistakenly accessing the wrong information) and intentional threats. c) Exploit: The term exploit is commonly used to describe a software program that has been developed to attack an asset by taking advantage of vulnerability. The objective of many exploits is to gain control over an asset. d) Risk: Risk refers to the potential for loss or damage when a threat exploits vulnerability. Examples of risk include financial losses as a result of business disruption, loss of privacy, reputational damage, and legal implications and can even include loss of life.
24.	What do you mean by active attacks? What are the different types of active attacks?
Ans.	Active attacks involve some modification of the data stream or the creation of a false stream. The active attacks can be subdivided into four categories: 1. Masquerade 2. Replay 3. Modification of messages 4. Denial of service
25.	What do you mean by passive attacks? What are the different types of passive attacks?
Ans.	A Passive Attack attempts to learn or make use of information from the system but does not affect system resources. Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. There are two types of passive attacks: 1. Release of message contents 2. Traffic analysis.
26.	Differentiate between DOS and DDoS attack.
Ans.	A Denial-of-Service (DoS) is a type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service. A DoS attack can be done in a several ways. The basic types of DoS attack include: 1. Flooding the network to prevent legitimate network traffic. 2. Disrupting the connections between two machines, thus preventing access to a service 3. Preventing a particular individual from accessing a service. 4. Disrupting the state of information, such as resetting of TCP sessions A Distributed denial of service (DDoS) attacks represents the next step in the evolution of DoS attacks as a way of disrupting the Internet. Cyber criminals began using DDoS attacks around 2000. The attacks use large numbers of compromised computers, as well as other electronic devices — such as webcams and smart televisions that make up the ever-increasing Internet of Things — to force the shutdown of the targeted website, server or network. In contrast, a DoS attack generally uses a single computer and a single IP address to attack its target, making it easier to defend against.
27.	What do you mean by Zero Day Attack? Explain.
Ans.	The term “zero-day” refers to newly discovered software vulnerability. Because the developer has just learned of the flaw, it also means an official patch or update to fix the issue hasn’t been released. So, “zero-day” refers to the fact that the developers have “zero days” to fix the problem that has just been exposed — and perhaps already exploited by hackers. Once the vulnerability becomes publicly known, the vendor has to work quickly to fix the issue to protect its users. But the software vendor may fail to release a patch before hackers manage to exploit the security hole. That’s known as a zero-day attack.
28.	Define the security goals.
Ans.	There are three main security goals:

	Confidentiality: Confidentiality means keeping the secrets secret. Information has confidentiality when it is protected from disclosure or exposure to unauthorized individuals or systems. Confidentiality ensures that only those with the rights and privileges to access information are able to do so. Integrity: It can be achieved by - Identification, Authentication and Authorization. Integrity can apply to a stream of messages, a single message, or selected fields within a message. A connection-oriented integrity service, one that deals with a stream of messages, assures that messages are received as sent, with no duplication, insertion, modification, reordering, or replays. A connection-less integrity service, one that deals with individual messages without regard to any larger context, generally provides protection against message modification only. Availability: Availability enables authorized users—persons or computer systems—to access information without interference or obstruction and to receive it in the required format.
29.	What are the different components of Information System?
Ans.	An information system (IS) is much more than computer hardware; it is the entire set of software, hardware, data, people, procedures, and networks that make possible the use of information resources in the organization. These six critical components enable information to be input, processed, output, and stored. Each of these IS components has its own strengths and weaknesses, as well as its own characteristics and uses. Each component of the information system also has its own security requirements.
30.	Differentiate between authentication and authorization.
Ans.	In authentication process, the identity of users is checked for providing the access to the system. While in authorization process, person's or user's authorities are checked for accessing the resources. In authentication process, users or persons are verified. While in authorization process, users or persons are validated.
31.	What is Risk? What did you understand from Risk Management?
Ans.	Risk: Risk refers to the potential for loss or damage when a threat exploits vulnerability. Examples of risk include financial losses as a result of business disruption, loss of privacy, reputational damage, and legal implications and can even include loss of life. Risk management involves three major undertakings: risk identification, risk assessment, and risk control. Risk identification is the examination and documentation of the security posture of an organization's information technology and the risks it faces. Risk assessment is the determination of the extent to which the organization's information assets are exposed or at risk. Risk control is the application of controls to reduce the risks to an organization's data and information systems.
32.	What are the different types of security policies?
Ans.	There are four types of security policies: 1. General security policies 2. Program security policies 3. Issue-specific policies 4. Systems-specific policies
33.	What do you mean by Cyber Law? Explain.
Ans.	The virtual world of internet is known as cyberspace and the laws governing this area are known as Cyber laws and all the netizens of this space come under the ambit of these laws as it carries a kind of universal jurisdiction. Cyber law can also be described as that branch of law that deals with legal issues related to use of inter-networked information technology. In short, cyber law is the law governing computers and the internet.
34.	What do you mean Man In The Middle Attack? Explain.
Ans.	A man-in-the-middle attack is a type of cyberattack where a malicious actor inserts him/herself into a conversation between two parties, impersonates both parties and gains access to information that the two parties were trying to send to each other. A man-in-the-middle attack allows a malicious actor to intercept, send and receive data meant for someone else, or not meant to be sent at all, without either outside party knowing until it is too late.
35.	Define Nonrepudiation?
Ans.	Nonrepudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message.
36.	What is XSS attack? How it can be performed?
Ans.	Cross-site scripting (XSS) is a code injection attack that allows an attacker to execute malicious JavaScript in another user's browser. The attacker does not directly target his victim. Instead, he exploits vulnerability in a website that the victim visits, in order to get the website to deliver the malicious JavaScript for him. To the victim's browser, the malicious JavaScript appears to be a legitimate part of the website, and the website has thus acted as an unintentional accomplice to the attacker. There are three types of XSS attacks: Stored XSS – Stored XSS also known as persistent XSS, occurs when user input is stored on the target server such as database/message forum/comment field etc. Then the victim is able to retrieve the stored data from the web application. Reflected XSS – Reflected XSS also known as non-persistent XSS, occurs when user input is immediately returned by a web application in an error message/search result or the input provided by the user as part of the

request and without permanently storing the user provided data.

DOM Based XSS – DOM Based XSS is a form of XSS when the source of the data is in the DOM, the sink is also in the DOM, and the data flow never leaves the browser.

Cross Site Scripting attack means sending and injecting malicious code or script. Malicious code is usually written with client-side programming languages such as Javascript, HTML, VBScript, Flash, etc. However, Javascript and HTML are mostly used to perform this attack.

This attack can be performed in different ways. Depending upon the type of XSS attack, the malicious script may be reflected on the victim's browser or stored in the database and executed every time, when the user calls the appropriate function. The main reason for this attack is inappropriate user's input validation, where malicious input can get into the output. A malicious user can enter a script, which will be injected into the website's code. Then the browser is not able to know if the executed code is malicious or not. Therefore malicious script is being executed on the victim's browser or any faked form is being displayed for the users. There are several forms in which XSS attack can occur.
Main forms of Cross Site Scripting are as follows:
a) Cross Site Scripting can occur on the malicious script executed at the client side.
b) Fake page or form displayed to the user (where the victim types credentials or clicks a malicious link).
c) On the websites with displayed advertisements.
d) Malicious emails sent to the victim.
This attack occurs when the malicious user finds the vulnerable parts of the website and sends it as appropriate malicious input. Malicious script is being injected into the code and then sent as the output to the final user.

37. What is SQL injection attack? How it can be performed?

Ans. An SQL query is a request for some action to be performed on a database, most commonly on a web page that asks for a username or password. But since most websites don't monitor inputs other than usernames and passwords, a hacker can use the input boxes to send their own requests – that is, inject SQL into the database. This way, hackers can create, read, update, alter or delete data stored in the back-end database, usually to access sensitive information such as social security numbers and credit card data as well as other financial information. SQL injection usually occurs when you ask a user for input, like their username/userid, and instead of a name/id, the user gives you an SQL statement that you will unknowingly run on your database.

Consider the following example which creates a SELECT statement by adding a variable (txtUserId) to a select string. The variable is fetched from user input (getRequestString):
Example:

```
txtUserId = getRequestString("UserId");
txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;
```

The original purpose of the code was to create an SQL statement to select a user, with a given user id. If there is nothing to prevent a user from entering "wrong" input, the user can enter some "smart" input like this:

UserId: 105 OR 1=1

Then, the SQL statement will look like this: SELECT * FROM Users WHERE UserId = 105 OR 1=1;

The SQL above is valid and will return ALL rows from the "Users" table, since OR 1=1 is always TRUE.

38. What do you mean by Risk Assessment? Explain.

Ans. After identifying the information asset and threat & vulnerabilities, we evaluate the relative risk for each of the vulnerabilities. This process is called Risk Assessment. Risk assessment assigns a risk rating or score to each information asset. While this number does not mean anything in absolute terms, it is useful in gauging the relative risk to each vulnerable information asset and facilitates the development of comparative ratings later in the risk control process. Likelihood is the probability that a specific vulnerability will be the object of a successful attack. In risk assessment, we assign a numeric value to likelihood. The National Institute of Standards and Technology (NIST) recommends in Special Publication 800-30 assigning a number between 0.1 (low) and 1.0 (high).

39. What do you mean by Risk control? What are the different strategies to control the risk?

Ans. Once the project team for information security development has created the ranked vulnerability worksheet, the team must choose one of five basic strategies to control each of the risks that result from these vulnerabilities. The five strategies are: defend, transfer, mitigate, accept, and terminate.
1. Defend: The defend control strategy attempts to prevent the exploitation of the vulnerability. This is the preferred approach and is accomplished by means of countering threats, removing vulnerabilities from assets, limiting access to assets, and adding protective safeguards.
2. Transfer: The transfer control strategy attempts to shift risk to other assets, other processes, or other organizations. This can be accomplished by rethinking how services are offered, revising deployment models, outsourcing to other organizations, purchasing insurance, or implementing service contracts with providers.
3. Mitigate: The mitigate control strategy attempts to reduce the impact caused by the exploitation of

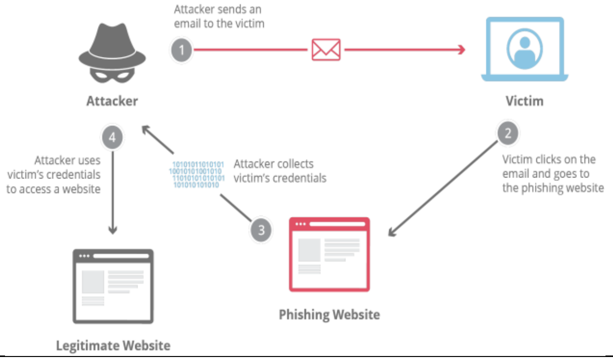
	vulnerability through planning and preparation. Mitigation begins with the early detection that an attack is in progress and a quick, efficient, and effective response. 4. Accept: The accept control strategy is the choice to do nothing to protect vulnerability and to accept the outcome of its exploitation. This may or may not be a conscious business decision. 5. Terminate: The terminate control strategy directs the organization to avoid those business activities that introduce uncontrollable risks.
40.	Explain the legal and ethical issues in computer security?
Ans.	Law: The law may be understood as the systematic set of universally accepted rules and regulation created by an appropriate authority such as government, which may be regional, national, international, etc. Ethics: Also described as moral philosophy, is a system of moral principles which is concerned with what is good for individuals and society. Nobody will be punished when they violate ethics; but whoever violates laws is going to receive punishment carried out by relevant authorities. Besides, an action can be illegal, but morally right. For example, in ancient China, some people rob properties from rich people, and give it to poor people, and it is considered to be morally right but be illegal. Similarly, an action that is legal can be morally wrong. For instance, some people spend thousands of dollars on their pets while some poor people on the street cannot have enough food. Ethics emphasizes more on positive aspects while laws are more concerned with negative actions. There are different types of laws: Civil law, Criminal law, Private law, Public law There are four types of security policies: 1. General security policies 2. Program security policies, 3. Issue-specific policies 4. Systems-specific policies.
41.	What is replay attack? How it works? Explain.
Ans.	A replay attack occurs when a cybercriminal eavesdrops on a secure network communication, intercepts it, and then fraudulently delays or resends it to misdirect the receiver into doing what the hacker wants. One of the best techniques to avert replay attacks is by using strong digital signatures with timestamps. A one-time password for each request also helps in preventing replay attacks and is frequently used in banking operations. Consider this real-world example of an attack. A staff member at a company asks for a financial transfer by sending an encrypted message to the company's financial administrator. An attacker eavesdrops on this message, captures it, and is now in a position to resend it. Because it's an authentic message that has simply been resent, the message is already correctly encrypted and looks legitimate to the financial administrator. In this scenario, the financial administrator is likely to respond to this new request unless he or she has a good reason to be suspicious. That response could include sending a large sum of money to the attacker's bank account.
42.	What do you mean by confidentiality in security goals? How it can be achieved?
Ans.	Confidentiality means keeping the secrets secret. Information has confidentiality when it is protected from disclosure or exposure to unauthorized individuals or systems. Confidentiality ensures that only those with the rights and privileges to access information are able to do so. When unauthorized individuals or systems can view information, confidentiality is breached. Confidentiality is the protection of transmitted data from passive attacks. With respect to the content of a data transmission, several levels of protection can be identified. The other aspect of confidentiality is the protection of traffic flow from analysis. This requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communication facility. The value of confidentiality of information is especially high when it is personal information about employees, customers, or patients. The confidentiality can be achieved by using the various cryptographic algorithms.
43.	What do you mean by integrity in security goals? How it can be achieved?
Ans.	Integrity can apply to a stream of messages, a single message, or selected fields within a message. A connection-oriented integrity service, one that deals with a stream of messages, assures that messages are received as sent, with no duplication, insertion, modification, reordering, or replays. A connection-less integrity service, one that deals with individual messages without regard to any larger context, generally provides protection against message modification only. The integrity of information is threatened when the information is exposed to corruption, damage, destruction, or other disruption of its authentic state. Corruption can occur while information is being stored or transmitted. Many computer viruses and worms are designed with the explicit purpose of corrupting data. Another key method of assuring information integrity is file hashing, in which a file is read by a special algorithm that uses the value of the bits in the file to compute a single large number called a hash value. The hash value for any combination of bits is unique. If a computer system performs the same hashing algorithm on a file and obtains a different number than the recorded hash value for that file, the file has been compromised and the integrity of the information is lost. Noise in the transmission media, for instance, can also cause data to

	lose its integrity. Transmitting data on a circuit with a low voltage level can alter and corrupt the data. Redundancy bits and check bits can compensate for internal and external threats to the integrity of information. During each transmission, algorithms, hash values, and the error-correcting codes ensure the integrity of the information. Data whose integrity has been compromised is retransmitted. It can be achieved by: Identification, Authentication, Authorization
44.	Describe about the Cyber Laws.
Ans.	The virtual world of internet is known as cyberspace and the laws governing this area are known as Cyber laws and all the netizens of this space come under the ambit of these laws as it carries a kind of universal jurisdiction. Cyber law can also be described as that branch of law that deals with legal issues related to use of inter-networked information technology. In short, cyber law is the law governing computers and the internet. Cyber law is important because it touches almost all aspects of transactions and activities on and involving the internet, World Wide Web and cyberspace. Every action and reaction in cyberspace has some legal and cyber legal perspectives. Cyber law encompasses laws relating to: 1. Cyber crimes 2. Electronic and digital signatures 3. Intellectual property 4. Data protection and privacy
45.	If an organization must evaluate the following three information assets for risk management, which vulnerability should be evaluated first for additional safety controls? Which should be evaluated last? a) Switch L47 connects a network to the Internet. It has two vulnerabilities: it is susceptible to hardware failure at a likelihood of 0.2, and it is subject to an SNMP buffer overflow attack at a likelihood of 0.1. This switch has an impact rating of 90 and has no current controls in place. You are 75% certain of the assumptions and data. b) Server WebSrv6 hosts a company Web site and performs e-commerce transactions. It has a Web server version that can be attacked by sending it invalid Unicode values. The likelihood of that attack is estimated at 0.1. The server has been assigned an impact value of 100, and a control has been implanted that reduces the impact of vulnerability by 75%. You are 80% certain of the assumptions and data. c) Operators use an MGMT45 control console to monitor operations in the server room. It has no passwords and is susceptible to unlogged misuse by the operators. Estimates show the likelihood of the misuse is 0.1. There are no controls in place on this asset; it has an impact rating of 5. You are 90% certain of the assumptions and data.
Ans.	First, we will calculate the risk of vulnerability by using the formula: Rr = (Lv x I)(1 – Rc + U) Switch L47 vulnerability 1 = (0.2 x 90)(1 – 0 + 0.25) = 22.5 Switch L47 vulnerability 2 = (0.1 x 90)(1 – 0 + 0.25) = 11.25 Server WebSrv6 vulnerability 3 = (0.1 x 100)(1 – 0.75 + 0.2) = 4.5 MGMT45 control console vulnerability 4 = (0.1 x 5)(1 – 0 + 0.1) = 0.55 Therefore, the vulnerability of Switch L47 would need to evaluated first because it has the highest risk rate (22.5) and the MGMT45 control console would be evaluated last because it has the lowest risk rate (0.55).
46.	Consider the information stored on your personal computer. For each of the terms listed, find an example and document it: threat, threat agent, vulnerability, exposure, risk, attack, and exploit.
Ans.	a. Threat: Theft of Media b. Threat Agent: Hacker c. Vulnerability: Unprotected system port d. Exposure: Using a website monitored by malicious hackers, reveals a vulnerability – i.e. Unprotected system port e. Risk: Low level risk – The probability that theft of media will occur is low. f. Attack: Hacker is made aware of system vulnerability (unprotected system port) by monitoring the website mediamadness.com. The hacker then navigates to and enters the exposed port; the hacker continues to steal media files from the user's computer. This results in the user experiencing a loss. g. Exploit: Hacker uses software tools to gain access to the unprotected system port; gaining access to the user's computer.
47.	What are the general guidelines for secure coding in an application as per Ministry of Electronics and Information Technology, Government of India?
Ans.	1. All your web-applications should be security Audited initially (for Web-application/mobile apps) • In every two years • Or whenever new module/page is added or modified or functionality is changed

2. In all web-applications/mobile-apps incorporate security requirements at the design and development phases.
3. Ensure that web-applications are deployed on hardened servers/infrastructures.
4. All components on server should be hardened and latest stable (non-vulnerable) versions should be upgraded.
5. All server environment/infrastructure should be configured for least privileged access, at all layers.
6. Effectively monitor system for any changes or intrusion.
7. Configure system logs on server [e.g.: Web-Access logs, Application Logs, Security Logs etc.]
8. Incorporate proper security advisories across all layers of infrastructure and servers.
9. Ensure proper backups of system/server/devices content/logs on a segregated server (preferable on disconnected server or storage devices)
10. Whenever any suspicious/intrusion incident is detected :
• Block the site for public access
• Report incident to Incident handling agency
• DO NOT CHANGE ARTIFACTS

48. What do you mean phishing attack? How it can be performed by attacker? Explain.

Ans. “Phishing” refers to an attempt to steal sensitive information, typically in the form of usernames, passwords, credit card numbers, bank account information or other important data in order to utilize or sell the stolen information. By masquerading as a reputable source with an enticing request, an attacker lures in the victim in order to trick them, similarly to how a fisherman uses bait to catch a fish.


Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
3
Attacker collects victim's credentials
10101011010101
10010101001010
11010101010101
101010101010
4
Attacker uses victim's credentials to access a website
Phishing Website
Legitimate Website

49. What are the possible results of an attack on a computer network?

Ans. There are some of the possible results of an attack on a computer network:
1. Loss or corruption of sensitive data that is essential for a company’s survival and success
2. Diminished reputation and trust among customers
3. The decline in value with shareholders
4. Reduced brand value
5. Reduction in profits

50. What are the types of password attacks? What can a systems administrator do to protect against them?

Ans. Following are the password attacks:
1. Brute force attack: In a brute force attack, a hacker uses a computer program to login to a user’s account with all possible password combinations. Moreover, brute force accounts don’t start at random; instead, they start with the easiest-to-guess passwords.
2. Dictionary Attack: Conversely, a dictionary attack allows hackers to employ a program which cycles through common words. A brute force attack goes letter by letter, whereas a dictionary attack only tries possibilities most likely to succeed. Also, dictionary attacks rely on a few key factors of users’ psychology. For example, users tend to pick short passwords and base their passwords off common words. So a dictionary attack starts with those words and variations (adding numbers at the end, replacing letters with numbers, etc.).
3. Keylogger Attack: Keylogger attacks install a program on users’ endpoints to track all of a users’ keystrokes. So as the user types in their usernames and passwords, the hackers record them for use later. This technically falls under the category of malware or a digital virus, so it must first infect the users’ endpoints (often through a phishing download).
4. Traffic interception: In this attack, the cybercriminal uses software such as packet sniffers to monitor network traffic and capture passwords as they’re passed. Similar to eavesdropping or tapping a phone line, the software monitors and captures critical information. Obviously, if that information—such as passwords—is unencrypted, the task is easier. But even encrypted information may be decryptable, depending on the strength of the encryption method used.
Strong passwords are usually the first defence against password attacks. The latest NIST guidelines recommend easy to remember/hard to guess passwords. A good mix of upper and lowercase characters, numbers, and special characters can help. Even better, avoid use of common words and common phrases. Definitely avoid site-specific words (including the name of the app you’re logging into in the password, for instance). NIST also recommends checking passwords against a dictionary of known poor passwords. Employee education is also important. One of the best defences against social engineering tactics is teaching users the techniques hackers use and how to recognize them.

51. The study of cryptography and cryptanalysis together are called______________.

Ans.	cryptology
52.	Which of the following algorithms are block ciphers: a) DES b) AES c) RSA d) All of these
Ans.	d) All of these
53.	In public key cryptography, both sender and receiver share a common secret key. (True/False)
Ans.	False
54.	The number of round functions in DES algorithm are_________.
Ans.	16
55.	The key length in 3DES algorithm is______________.
Ans.	192 bits
56.	AES algorithm uses ____________rounds and _______subkeys.
Ans.	10, 44
57.	The MD5 function is a cryptographic algorithm that takes an input of arbitrary length and produces a message digest that is __________ bits long.
Ans.	128
58.	What is the block size in SHA-512 algorithm?
Ans.	1024 bit
59.	Which of the following operation is NOT performed by AES: a) Left Circular Shift b) Mix Columns c) Substitute Bytes d) Add Round Key
Ans.	a) Left Circular Shift
60.	In MAC, two communicating parties, say X and Y, share the same secret key?(True/False)
Ans.	True
61.	Which of the following parameter is available in X.509 certificate format: a) Issuer Name b) Validity Period c) Public Key Info d) All of these
Ans.	d) All of these
62.	In RSA the ____________ key of a receiver is used to encrypt messages.
Ans.	public
63.	What are the numbers of possible keys for a key of length 128 bits?
Ans.	2^128
64.	Which among the following is an advantage of modern cryptography? a) Analyzed by best minds b) Low cost in implementation c) Can work over images, not just text d) All of the above
Ans.	d) All of the above
65.	When A wants to communicate with B using symmetric key algorithms, how many keys are needed?
Ans.	1
66.	What is the table size (in bits) to implement the S-Box? a) 8 b) 2^8 c) 2^11 d) 2^12
Ans.	c) 2^11
67.	Which among the following is true of 3DES (compared to DES)? a) Less secure b) slower c) Both a and b d) None of these
Ans.	b) slower
68.	In AES-128, a set contains how many words? a) 4 b) 8 c)12 d)16
Ans.	a) 4
69.	If the message size is 1000 bits, for a given hash value, how many messages in the message space map to this hash value? Note that the hash size is 160 bits. a) 2^1000 b) 2^840 c) 2^160 d) 840
Ans.	b) 2^840
70.	How many number of 64bit buffer registers are used in SHA-512 algorithm.
Ans.	8
71.	Define cryptography? Write the application of cryptography.
Ans.	Cryptography, which comes from the Greek words kryptos, meaning “hidden,” and graphein, meaning “to write,” is the process of making and using codes to secure the transmission of information. There are lots of benefits of cryptography in the modern world and a few of them are: 1. Chip based payment cards 2. Computer and other passwords 3. E-commerce 4. Defence communications 5. Digital Currencies 6. Designing protocols 7. Data authenticity
72.	Differentiate between the public key and secret key cryptography.
Ans.	In secret key cryptography, both sender and receiver share a common secret key; the same secret key is used for both encryption and decryption. This form of cryptography is also known as symmetric key cryptography. In public key cryptography algorithms, two distinct keys forming a key pair are used. The encryption key or public key and the decryption key or private key. The public key of a user is used to encrypt messages to that

	user. It is intended to be known to the outside world. The corresponding private key, however should not be revealed to anyone. It is the private key of the recipient that is used to decrypt the message. This form of cryptography is also known as Asymmetric Key Cryptography.
73.	Define the following terms: a) Encryption b) Decryption b. Decryption
Ans.	a) Encryption: The process of converting from plaintext to ciphertext is known as enciphering or encryption. b) Decryption: The process of restoring the plaintext from the ciphertext is known deciphering or decryption.
74.	Define the following terms: a) Plain text b) Cipher text
Ans.	An original message is known as the plaintext, while the coded message is called the ciphertext.
75.	What is substitution cipher? Write the name of different substitution cipher methods?
Ans.	A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols. If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns. Substitution cipher methods are Caesar cipher, Polyalphabetic cipher, Hill Cipher, One time pad.
76.	What is transposition cipher? Write the name of different transposition cipher methods?
Ans.	A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher. The simplest such cipher is the rail fence technique, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.
77.	Consider a Hill Cipher using a block size of 2(m=2). Let $K = \begin{matrix} 3 & 7 \\ 15 & 12 \end{matrix}$ The plaintext is [H I]. Calculate the corresponding cipher text?
Ans.	The numeric equivalent of the given plaintext block P is = [7 8] Encryption C = (P*K) mod 26 $P * K = \begin{matrix} 7 & 8 \end{matrix} * \begin{matrix} 3 & 7 \\ 15 & 12 \end{matrix}$ C = [141 145] mod 26 = [11 15] The corresponding cipher text C = [L P]
78.	Define message authentication? What are the different types of message authentication?
Ans.	Message authentication is a procedure to verify that received messages come from the alleged source and have not been altered. Types of message authentication: Message encryption: The ciphertext of the entire message serves as its authenticator. Message authentication code (MAC): A function of the message and a secret key that produces a fixed-length value that serves as the authenticator. Hash function: A function that maps a message of any length into a fixed-length hash value, which serves as the authenticator.
79.	What is digital signature? Write the types of digital signature?
Ans.	Message authentication protects two parties who exchange messages from any third party. However, it does not protect the two parties against each other. Several forms of dispute between the two are possible. In situations where there is not complete trust between sender and receiver, something more than authentication is needed. The most attractive solution to this problem is the digital signature. The digital signature is analogous to the handwritten signature. It must have the following properties: a. It must verify the author and the date and time of the signature. b. It must to authenticate the contents at the time of the signature. c. It must be verifiable by third parties, to resolve disputes. There are two approaches to digital signature: i. RSA Approach ii. DSS Approach
80.	What do you mean by X.509 standard? Explain.
Ans.	X.509 defines a framework for the provision of authentication services by the X.500 directory to its users. The directory may serve as a repository of public-key certificates. Each certificate contains the public key of a user and is signed with the private key of a trusted certification authority. In addition, X.509 defines alternative authentication protocols based on the use of public-key certificates. X.509 is an important standard because the certificate structure and authentication protocols defined in X.509 are used in a variety of contexts. For example, the X.509 certificate format is used in S/MIME, IP Security, and SSL/TLS and SET. The heart of the X.509 scheme is the public-key certificate associated with each user. These user certificates are assumed to be created by some trusted certification authority (CA) and placed in the directory by the CA or by the user. The directory server itself is not responsible for the creation of public keys or for the certification function; it merely provides an easily accessible location for users to obtain certificates.
81.	Explain the frame format of X.509 standard?
Ans.	The X.509 standard contains the following fields: Version: Differentiates among successive versions of the certificate format; the default is version 1. If the Issuer Unique Identifier or Subject Unique Identifier are present, the value must be version 2. If one or more extensions are present, the version must be version 3.

Serial number: An integer value, unique within the issuing CA, that is unambiguously associated with this certificate.

Signature algorithm identifier: The algorithm used to sign the certificate, together with any associated parameters. Because this information is repeated in the Signature field at the end of the certificate, this field has little, if any, utility.

Issuer name: X.500 name of the CA that created and signed this certificate.

Period of validity: Consists of two dates: the first and last on which the certificate is valid.

Subject name: The name of the user to whom this certificate refers. That is, this certificate certifies the public key of the subject who holds the corresponding private key.

Subject's public-key information: The public key of the subject, plus an identifier of the algorithm for which this key is to be used, together with any associated parameters.

Issuer unique identifier: An optional bit string field used to identify uniquely the issuing CA in the event the X.500 name has been reused for different entities.

Subject unique identifier: An optional bit string field used to identify uniquely the subject in the event the X.500 name has been reused for different entities.

Extensions: A set of one or more extension fields. Extensions were added in version 3.

Signature: Covers all of the other fields of the certificate; it contains the hash code of the other fields, encrypted with the CA's private key. This field includes the signature algorithm identifier.

82. Differentiate between SHA-1 and SHA-2.

Ans. The Secure Hash Algorithm (SHA) was developed by the National Institute of Standards and Technology (NIST) and published as a federal information processing standard (FIPS 180) in 1993; a revised version was issued as FIPS 180-1 in 1995 and is generally referred to as SHA-1. SHA-1 produces a hash value of 160 bits. In 2002, NIST produced a revised version of the standard, FIPS 180-2, that defined three new versions of SHA, with hash value lengths of 256, 384, and 512 bits, known as SHA-256, SHA-384, and SHA-512. These new versions have the same underlying structure and use the same types of modular arithmetic and logical binary operations as SHA-1.

83. What is Public Key Infrastructure (PKI)? Explain.

Ans. Public-key Infrastructure (PKI) is an integrated system of software, encryption methodologies, protocols, legal agreements, and third-party services that enables users to communicate securely. PKI systems are based on public-key cryptosystems and include digital certificates and certificate authorities (CAs). A typical PKI solution protects the transmission and reception of secure information by integrating the following components:

A certificate authority (CA), which issues, manages, authenticates, signs, and revokes users' digital certificates, which typically contain the user name, public key, and other identifying information.

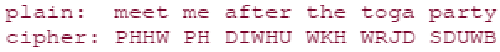
A registration authority (RA), which operates under the trusted collaboration of the certificate authority and can handle day-to-day certification functions, such as verifying registration information, generating end-user keys, revoking certificates, and validating user certificates.

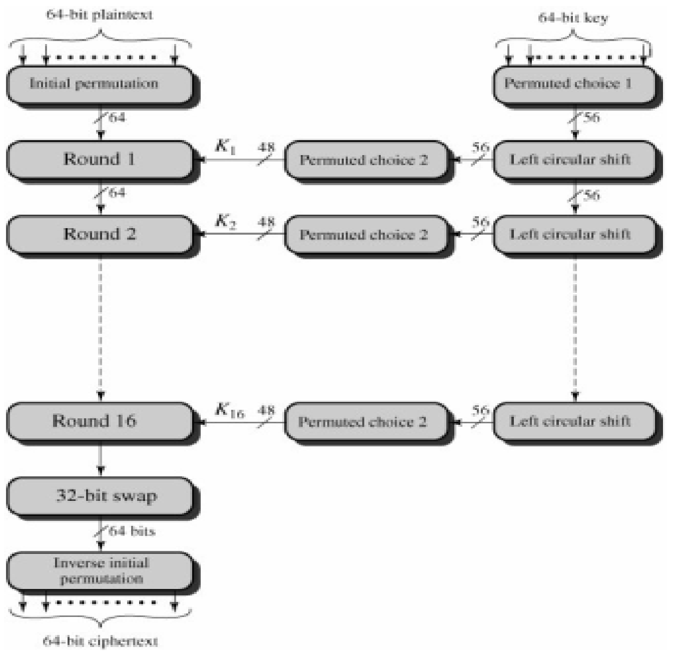
84. Differentiate between DES and Triple DES.

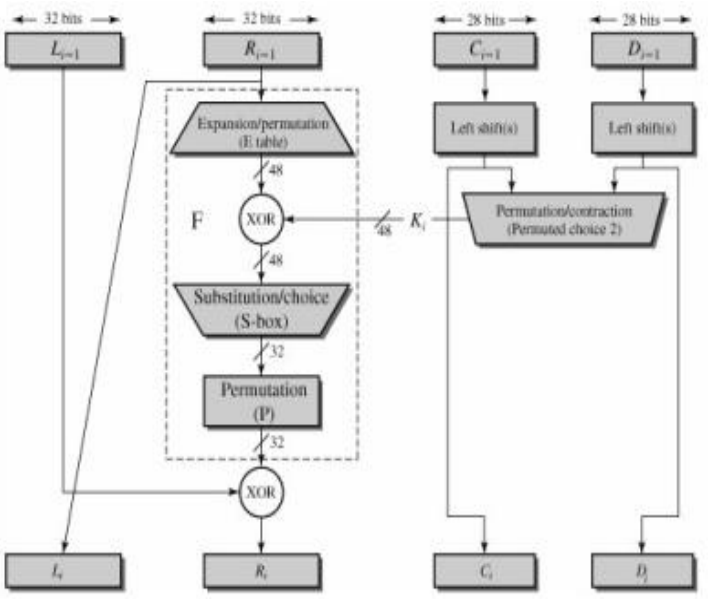
Ans. The most widely used encryption scheme is based on the Data Encryption Standard (DES) adopted in 1977 by the National Bureau of Standards, now the National Institute of Standards and Technology (NIST).
The algorithm itself is referred to as the Data Encryption Algorithm (DEA). For DES, data are encrypted in 64-bit blocks using a 64-bit key. The algorithm transforms 64-bit input in a series of steps into a 64-bit output. The same steps, with the same key, are used to reverse the encryption. DES works on bits, or binary numbers--the 0s and 1s common to digital computers. DES is a block cipher--meaning it operates on plaintext blocks of a given size (64-bits) and returns ciphertext blocks of the same size. Thus DES results in a permutation among the 264 possible arrangements of 64 bits, each of which may be either 0 or 1. Each block of 64 bits is divided into two blocks of 32 bits each.

3DES was created to provide a level of security far beyond that of standard DES. 3DES uses three 64-bit keys for an overall key length of 192 bits. 3DES encryption is the same as that of standard DES, repeated three times. 3DES can be employed using two or three keys and a combination of encryption or decryption for additional security. The most common implementations involve encrypting and/or decrypting with two or three different keys. 3DES employs forty-eight rounds in its encryption computation, generating ciphers that are approximately 256 times stronger than standard DES ciphers but require only three times longer to process.

85. What do you mean by Kerberos? Explain.

Ans.	Kerberos is an authentication service developed as part of Project Athena at MIT. The problem that Kerberos addresses is this: Assume an open distributed environment in which users at workstations wish to access services on servers distributed throughout the network. We would like for servers to be able to restrict access to authorized users and to be able to authenticate requests for service. In this environment, a workstation cannot be trusted to identify its users correctly to network services. In particular, the following three threats exist: i. A user may gain access to a particular workstation and pretend to be another user operating from that workstation. ii. A user may alter the network address of a workstation so that the requests sent from the altered workstation appear to come from the impersonated workstation. iii. A user may eavesdrop on exchanges and use a replay attack to gain entrance to a server or to disrupt operations. In any of these cases, an unauthorized user may be able to gain access to services and data that he or she is not authorized to access. Rather than building in elaborate authentication protocols at each server, Kerberos provides a centralized authentication server whose function is to authenticate users to servers and servers to users.
86.	How Caesar cipher works? Explain the encryption and decryption process of Caesar cipher?
Ans.	The earliest known use of a substitution cipher, and the simplest, was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet. For example:  plain: meet me after the toga party cipher: PHHW PH DIWHU WKH WRJD SDUWB A shift may be of any amount, so that the general Caesar algorithm is C = E(k, p) = (p + k) mod 26 where k takes on a value in the range 1 to 25. The decryption algorithm is simply p = D(k, C) = (C - k) mod 26 This type of substitution is based on a monoalphabetic substitution, because it only uses one alphabet. More advanced substitution ciphers use two or more alphabets, and are referred to as polyalphabetic substitutions.
87.	Differentiate between monoalphabetic and polyalphabetic cipher with suitable examples.
Ans.	The Caesar cipher substitution is based on a monoalphabetic substitution, because it only uses one alphabet. More advanced substitution ciphers use two or more alphabets, and are referred to as polyalphabetic substitutions. In polyalphabetic cipher, the ciphertext corresponding to a particular character in the plain text is not fixed. An advanced type of substitution cipher that uses a simple polyalphabetic code is the Vigenère cipher. The cipher is implemented using the Vigenère square (or table), which is made up of twenty-six distinct cipher alphabets.
88.	What do you mean by one time pad encryption process? Why it is unbreakable? Explain.
Ans.	Mauborgne suggested using a random key that is as long as the message, so that the key need not be repeated. In addition, the key is to be used to encrypt and decrypt a single message, and then is discarded. Each new message requires a new key of the same length as the new message. Such a scheme, known as a one-time pad, is unbreakable. It produces random output that bears no statistical relationship to the plaintext. Because the ciphertext contains no information whatsoever about the plaintext, there is simply no way to break the code. The security of the one-time pad is entirely due to the randomness of the key. If the stream of characters that constitute the key is truly random, then the stream of characters that constitute the ciphertext will be truly random. Thus, there are no patterns or regularities that a cryptanalyst can use to attack the ciphertext.
89.	Explain the DES algorithm encryption process with block diagram.
Ans.	The most widely used encryption scheme is based on the Data Encryption Standard (DES) adopted in 1977 by the National Bureau of Standards, now the National Institute of Standards and Technology (NIST). The algorithm itself is referred to as the Data Encryption Algorithm (DEA). For DES, data are encrypted in 64-bit blocks using a 64-bit key. The algorithm transforms 64-bit input in a series of steps into a 64-bit output. The same steps, with the same key, are used to reverse the encryption. DES works on bits, or binary numbers--the 0s and 1s common to digital computers. DES is a block cipher--meaning it operates on plaintext blocks of a given size (64-bits) and returns ciphertext blocks of the same size. Thus DES results in a permutation among the 264 possible arrangements of 64 bits, each of which may be either 0 or 1. Each block of 64 bits is divided into two blocks of 32 bits each.





90. How 3DES is more powerful than DES? Explain.

Ans. 3DES was created to provide a level of security far beyond that of standard DES. 3DES uses three 64-bit keys for an overall key length of 192 bits. 3DES encryption is the same as that of standard DES, repeated three times. 3DES can be employed using two or three keys and a combination of encryption or decryption for additional security. The most common implementations involve encrypting and/or decrypting with two or three different keys. 3DES employs forty-eight rounds in its encryption computation, generating ciphers that are approximately 256 times stronger than standard DES ciphers but require only three times longer to process.

91. What do you mean Advanced Encryption Standard algorithm? What are the different operations performed under AES algorithm?

Ans. The Advanced Encryption Standard (AES) was published by NIST (National Institute of Standards and Technology) in 2001. AES is a symmetric block cipher that is intended to replace DES as the approved standard for a wide range of applications. AES is a block cipher intended to replace DES for commercial applications. It uses a 128-bit block size and a key size of 128, 192, or 256 bits.

- No. of rounds: 10
- No. of subkeys:44
- Each sub key size: 32bit/1word/4 bytes
- Each round uses 4 sub-keys.
- Pre-round calculation uses 4 sub-keys.
- Size of one word is 32bits or 4bytes.

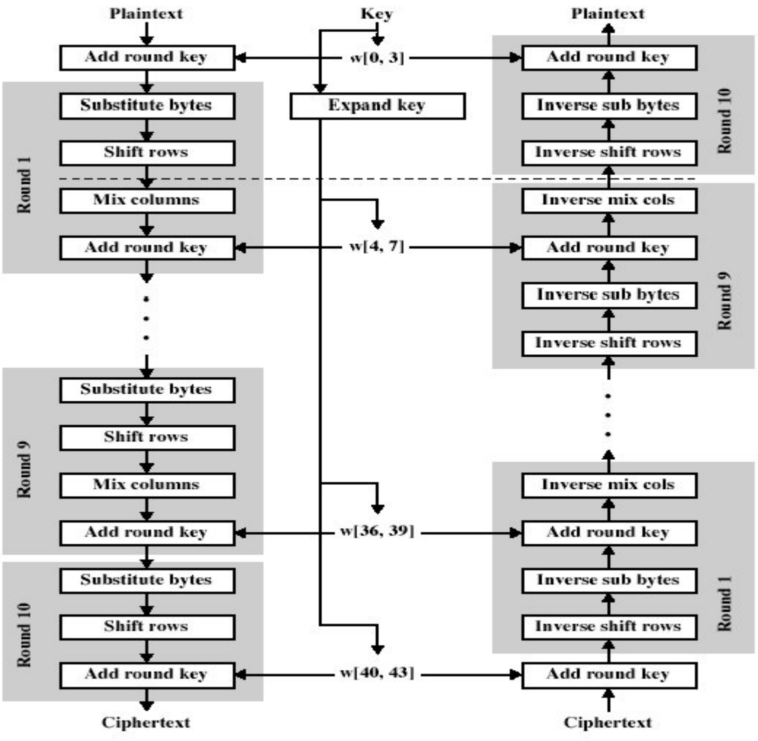
Four different stages are used, one of permutation and three of substitution:

1. Substitute bytes: Uses an S-box to perform a byte-by-byte substitution of the block
2. ShiftRows: A simple permutation

3. MixColumns: A substitution that makes use of arithmetic over GF(28)
4. AddRoundKey: A simple bitwise XOR of the current block with a portion of the expanded key

92. Explain the encryption and decryption process of AES algorithm with block diagram.

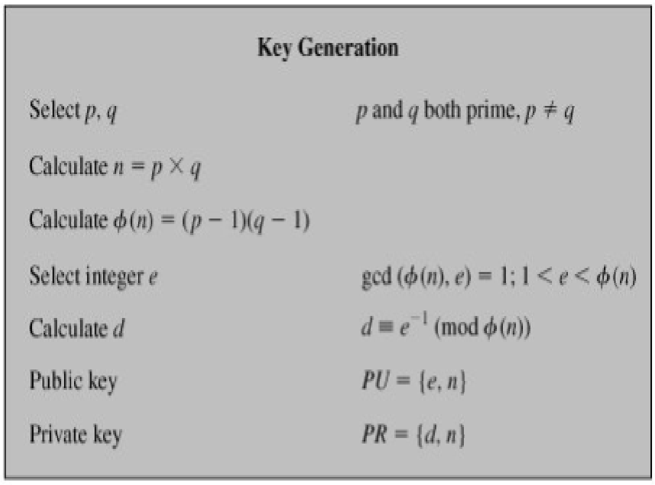
Ans.



(a) Encryption (b) Decryption

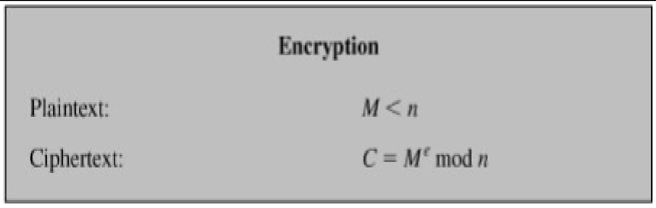
93. Explain the RSA algorithm with suitable example.

Ans. Developed in 1977 by Ron Rivest, Adi Shamir, and Len Adleman at MIT and first published in 1978. The Rivest-Shamir-Adleman (RSA) scheme has since that time reigned supreme as the most widely accepted and implemented general-purpose approach to public-key encryption. The RSA scheme is a block cipher in which the plaintext and ciphertext are integers between 0 and n-1 for some n.



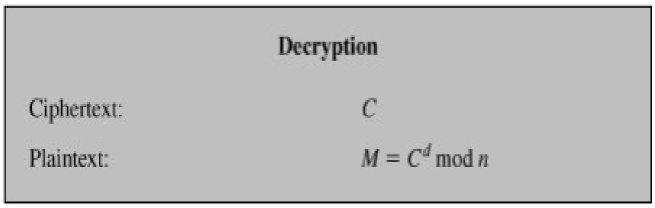
Key Generation

Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$



Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \bmod n$

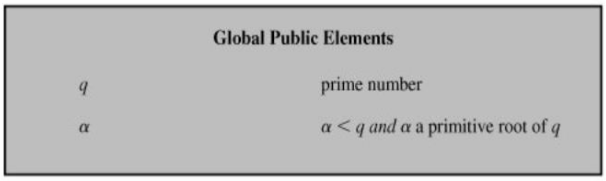


Decryption

Ciphertext:	C
Plaintext:	$M = C^d \bmod n$

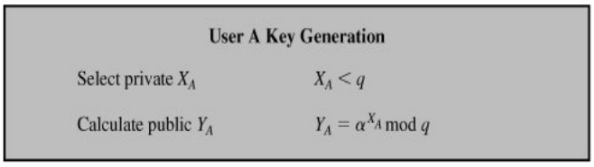
94. What is the purpose of Diffie Hellman key exchange algorithm? Write the process to generate the key using this algorithm. Explain.

Ans. The purpose of the algorithm is to enable two users to securely exchange a key that can then be used for subsequent encryption of messages. The algorithm itself is limited to the exchange of secret values



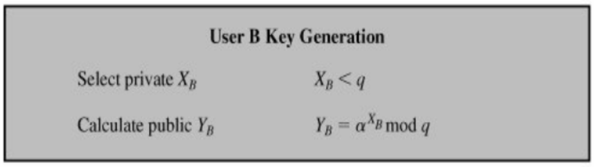
Global Public Elements

q	prime number
α	$\alpha < q$ *and* α a primitive root of q



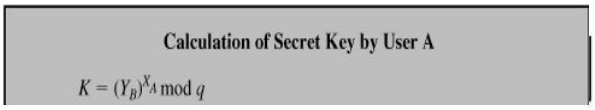
User A Key Generation

Select private X_A	$X_A < q$
Calculate public Y_A	$Y_A = \alpha^{X_A} \bmod q$



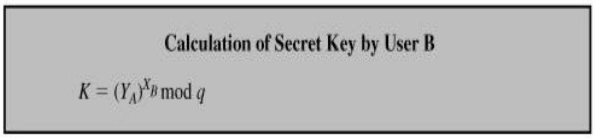
User B Key Generation

Select private X_B	$X_B < q$
Calculate public Y_B	$Y_B = \alpha^{X_B} \bmod q$



Calculation of Secret Key by User A

$K = (Y_B)^{X_A} \bmod q$



Calculation of Secret Key by User B

$K = (Y_A)^{X_B} \bmod q$

95. What is a hash function? How hash function is different from message authentication code? Explain.

Ans. A variation on the message authentication code is the one-way hash function. As with the message authentication code, a hash function accepts a variable-size message M as input and produces a fixed size output, referred to as a hash code H(M).

Unlike a MAC, a hash code does not use a key but is a function only of the input message. The hash code is also referred to as a message digest or hash value. The hash code is a function of all the bits of the message and provides an error-detection capability. A change to any bit or bits in the message results in a change to the hash code.

96. Explain the processing of single 512bit block using MD5 algorithm.

Ans. The MD5 function is a cryptographic algorithm that takes an input of arbitrary length and produces a message digest that is 128 bits long. MD5 was designed by well-known cryptographer Ronald Rivest in 1991.

The MD5 algorithm first divides the input in blocks of 512bits each.

Step 1: Append padding bits, starting from 1 then put 0's.(i.e. 10000……..)

Step 2: The remaining bits are filled up with 64 bits representing the length of the original message.

Step 3: Initialize the buffer. Each of size 32bits. Four buffers are required(A,B,C,D).

Step 4: Process each 512bits block.

Step 5: Output i.e. message digest stored in buffer.

The processing of a message block consists of four similar stages, termed rounds; each round is composed of 16 similar operations based on a non-linear function F, modular addition, and left rotation. There are four possible functions; a different one is used in each round:

$$F(B,C,D) = (B \wedge C) \vee (\neg B \wedge D)$$
$$G(B,C,D) = (B \wedge D) \vee (C \wedge \neg D)$$
$$H(B,C,D) = B \oplus C \oplus D$$
$$I(B,C,D) = C \oplus (B \vee \neg D)$$

97. Explain the working of SHA-512 algorithm.

Ans. The algorithm takes as input a message with a maximum length of less than 2128 bits and produces as output a 512-bit message digest. The input is processed in 1024-bit blocks.
Step 1: Append padding bits. The message is padded so that its length is congruent to 896 modulo 1024 . Padding is always added, even if the message is already of the desired length. Thus, the number of padding bits is in the range of 1 to 1024. The padding consists of a single 1-bit followed by the necessary number of 0-bits.

Step 2: Append length. A block of 128 bits is appended to the message. This block is treated as an unsigned 128-bit integer (most significant byte first) and contains the length of the original message (before the padding). The outcome of the first two steps yields a message that is an integer multiple of 1024 bits in length. The expanded message is represented as the sequence of 1024-bit blocks M1, M2,..., MN, so that the total length of the expanded message is N x 1024 bits.

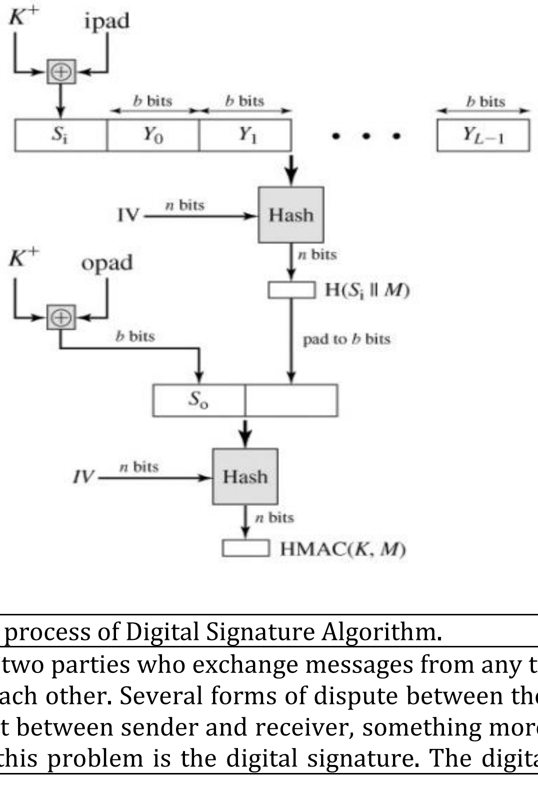
Step 3: Initialize hash buffer. A 512-bit buffer is used to hold intermediate and final results of the hash function. The buffer can be represented as eight 64-bit registers (a, b, c, d, e, f, g, h). These registers are initialized to the following 64-bit integers (hexadecimal values):
a = 6A09E667F3BCC908
b = BB67AE8584CAA73B
c = 3C6EF372FE94F82B
d = A54FF53A5F1D36F1
e = 510E527FADE682D1
f = 9B05688C2B3E6C1F
g = 1F83D9ABFB41BD6B
h = 5BE0CDI9137E2179

Step 4: Process message in 1024-bit (128-word) blocks. The heart of the algorithm is a module that consists of 80 rounds.

Step 5: Output. After all N 1024-bit blocks have been processed, the output from the Nth stage is the 512-bit message digest.

98. What is HMAC? Explain the HMAC structure with block diagram.

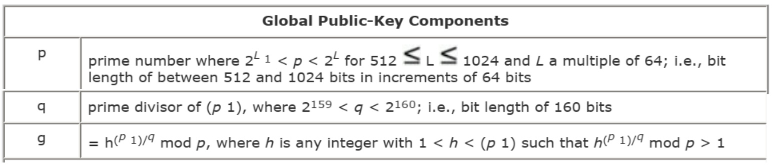
Ans. A hash function such as SHA was not designed for use as a MAC and cannot be used directly for that purpose because it does not rely on a secret key. There have been a number of proposals for the incorporation of a secret key into an existing hash algorithm. The approach that has received the most support is HMAC. HMAC has been issued as RFC 2104, has been chosen as the mandatory-to-implement MAC for IP security, and is used in other Internet protocols, such as SSL. HMAC has also been issued as a NIST standard. HMAC consists of twin benefits of Hashing and MAC, and thus is more secure than any other authentication codes.



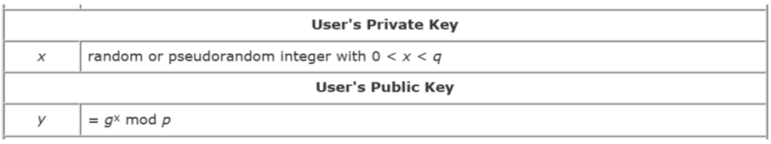
99. Explain the signing and verifying process of Digital Signature Algorithm.

Ans. Message authentication protects two parties who exchange messages from any third party. However, it does not protect the two parties against each other. Several forms of dispute between the two are possible. In situations where there is not complete trust between sender and receiver, something more than authentication is needed. The most attractive solution to this problem is the digital signature. The digital signature is analogous to the handwritten signature. It must have the following properties:

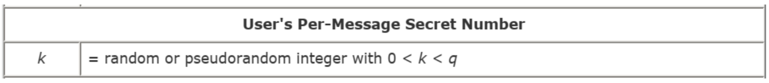
- It must verify the author and the date and time of the signature.
- It must to authenticate the contents at the time of the signature.
- It must be verifiable by third parties, to resolve disputes.



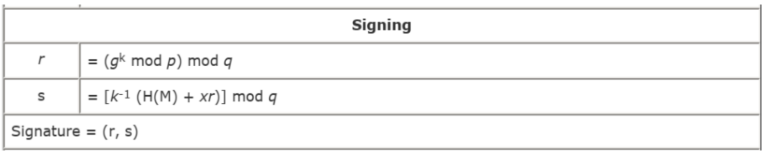
Global Public-Key Components	
p	prime number where $2^{L\ 1} < p < 2^L$ for $512 \leq L \leq 1024$ and L a multiple of 64; i.e., bit length of between 512 and 1024 bits in increments of 64 bits
q	prime divisor of (p 1), where $2^{159} < q < 2^{160}$; i.e., bit length of 160 bits
g	= $h^{(p\ 1)/q} \bmod p$, where h is any integer with $1 < h < (p\ 1)$ such that $h^{(p\ 1)/q} \bmod p > 1$



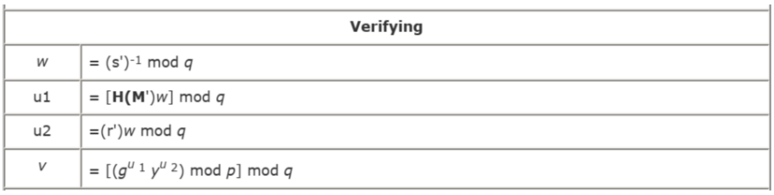
User's Private Key	
x	random or pseudorandom integer with $0 < x < q$
User's Public Key	
y	= $g^x \bmod p$



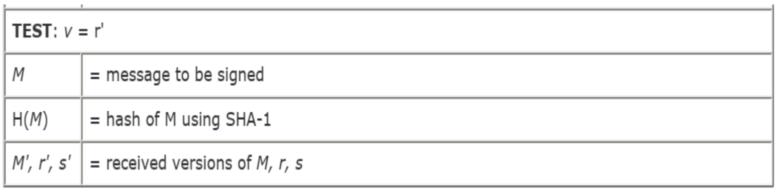
User's Per-Message Secret Number	
k	= random or pseudorandom integer with $0 < k < q$



Signing	
r	= $(g^k \bmod p) \bmod q$
s	= $[k^{-1} (H(M) + xr)] \bmod q$
Signature = (r, s)	



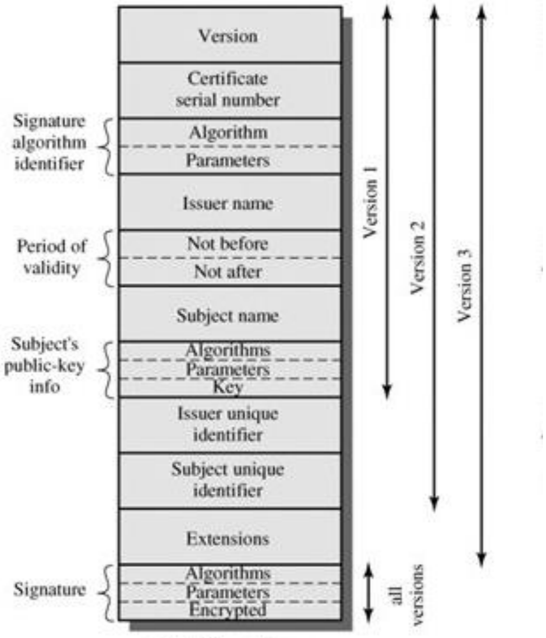
Verifying	
w	= $(s')^{-1} \bmod q$
u1	= $[\mathbf{H}(\mathbf{M}')w] \bmod q$
u2	=$(r')w \bmod q$
v	= $[(g^{u\ 1} y^{u\ 2}) \bmod p] \bmod q$



TEST: $v = r'$	
M	= message to be signed
H(M)	= hash of M using SHA-1
M', r', s'	= received versions of M, r, s

100. Explain the X.509 certificate format.

Ans.



(a) X.509 certificate

a) Version: Differentiates among successive versions of the certificate format; the default is version 1. If the Issuer Unique Identifier or Subject Unique Identifier are present, the value must be version 2. if one or more

	extensions are present, the version must be version 3. b) Serial number: An integer value, unique within the issuing CA, that is unambiguously associated with this certificate. c) Signature algorithm identifier: The algorithm used to sign the certificate, together with any associated parameters. Because this information is repeated in the Signature field at the end of the certificate, this field has little, if any, utility. d) Issuer name: X.500 name of the CA that created and signed this certificate. e) Period of validity: Consists of two dates: the first and last on which the certificate is valid. f) Subject name: The name of the user to whom this certificate refers. That is, this certificate certifies the public key of the subject who holds the corresponding private key. g) Subject's public-key information: The public key of the subject, plus an identifier of the algorithm for which this key is to be used, together with any associated parameters. h) Issuer unique identifier: An optional bit string field used to identify uniquely the issuing CA in the event the X.500 name has been reused for different entities. i) Subject unique identifier: An optional bit string field used to identify uniquely the subject in the event the X.500 name has been reused for different entities. j) Extensions: A set of one or more extension fields. Extensions were added in version 3. k) Signature: Covers all of the other fields of the certificate; it contains the hash code of the other fields, encrypted with the CA's private key. This field includes the signature algorithm identifier.
101.	The ___________ is actually an IETF version of________________ a)TLS;TSS b) SSL;TLS c) TLS;SSL d) SSL;SLT
Ans.	c) TLS;SSL
102.	The ___________ protocol provides security at transport layer.
Ans.	SSL and TLS
103.	SSL provides____________. a) message integrity b) confidentiality c) compression d) all of the above
Ans.	d) all of the above
104.	Protocol for the email security is__________
Ans.	PGP
105.	A ________________ protocol is a collection of protocols designed by IETF to provide security for a packet at the network layer. a) IPSec b) SSL c)PGP d)None of the above
Ans.	a) IPSec
106.	The __________________ mode is normally used when we need host-to-host protection of data. a) transport b) tunnel c) Both A and B d) Neither A and nor B
Ans	c)Both A and B
107.	In tunnel mode, IPSec protects the ______________ a) Entire IP packet b) IP header c) IP payload d) IP trailer
Ans.	a) Entire IP packet
108.	IPSec is designed to provide security at the ________ a) Transport layer b) Network layer c) Application layer d) Session layer
Ans.	b) Network layer
109.	Which component is included in IP security? a) Authentication Header (AH) b) Encapsulating Security Payload (ESP) c) Internet key Exchange (IKE) d) All of the mentioned
Ans.	d) All of the mentioned
110.	WPA2 is used for security in ___________.
Ans.	Wi-Fi
111.	PGP encrypts data by using a block cipher called _____ a) International data encryption algorithm b) Private data encryption algorithm c) Internet data encryption algorithm d) Local data encryption algorithm

Ans.	a) International data encryption algorithm
112.	Network layer firewall has two sub-categories as __________________.
Ans.	State full firewall and stateless firewall
113.	A proxy firewall filters at ________ . a) Physical layer b) Data link layer c) Network layer d) Application layer
Ans.	d) Application layer
114.	A stateful firewall maintains a __________ which is a list of active connections. a) Routing table b) Bridging table c) State table d) Connection table
Ans.	a) Routing table
115.	Which of the following is not a software firewall? a) Windows Firewall b) Outpost Firewall Pro c) Endian Firewall d) Linksys Firewall
Ans.	d) Linksys Firewall
116.	A firewall protects which of the following attacks? a) Phishing b) Dumpster diving c) Denial of Service (DoS) d) Shoulder surfing
Ans.	c) Denial of Service (DoS)
117.	Packet filtering firewalls are deployed on _______ a) routers b) switches c) hubs d) repeaters
Ans.	a)routers
118.	The _____________ protocol is an open encryption and security specification designed to protect credit card transactions on the Internet.
Ans.	SET
119.	The RFC ________________ Specification of key management capabilities.
Ans.	2408
120.	Both PGP and S/MIME make use of an encoding technique referred to as_________ conversion
Ans.	radix-64
121.	Which security protocols are predominantly used in Web-based electronic commerce?
Ans.	Many Web-based technologies make use of the S-HTTP, SET, SSL, SSH-2, and IPSec protocols.
122.	Which security protocols are used to protect e-mail?
Ans.	E-mail security is most often provided using the S/MIME, PEM, and PGP protocols.
123.	IPSec can be used in two modes. What are they?
Ans.	IPSec is provisioned using the transport and tunnel modes.
124.	What are the five principal services provided by PGP?
Ans.	The following are the services offered by PGP: 1. Authentication 2. Confidentiality 3. Compression 4. Email Compatibility 5. Segmentation
125.	What is the utility of a detached signature?
Ans.	A detached signature is useful in several contexts. A user may wish to maintain a separate signature log of all messages sent or received. A detached signature of an executable program can detect subsequent virus infection. Finally, detached signatures can be used when more than one party must sign a document, such as a legal contract. Each person's signature is independent and therefore is applied only to the document. Otherwise, signatures would have to be nested, with the second signer signing both the document and the first signature, and so on.
126.	Why does PGP generate a signature before applying compression?
Ans.	a) It is preferable to sign an uncompressed message so that one can store only the uncompressed message together with the signature for future verification. If one signed a compressed document, then it would be necessary either to store a compressed version of the message for later verification or to recompress the message when verification is required. b) Even if one were willing to generate dynamically a recompressed message for verification, PGP's compression algorithm presents a difficulty. The algorithm is not deterministic; various implementations of the algorithm achieve different tradeoffs in running speed versus compression ratio and, as a result, produce different compressed forms. However, these different compression algorithms are interoperable because any version of the algorithm can correctly decompress the output of any other version. Applying the hash function and signature after compression would constrain all PGP implementations to the same version of the compression algorithm.
127.	What is R64 conversion?
Ans.	R64 converts a raw 8-bit binary stream to a stream of printable ASCII characters. Each group of three octets of binary data is mapped into four ASCII characters.

128.	Why is the segmentation and reassembly function in PGP needed?
Ans.	E-mail facilities often are restricted to a maximum message length.
129.	What is S/MIME?
Ans.	Secure Multipurpose Internet Mail Extensions (S/MIME) builds on the encoding format of the Multipurpose Internet Mail Extensions (MIME) protocol and uses digital signatures based on public key cryptosystems to secure e-mail. S/MIME provides the following functions: Enveloped data, Signed data, Clear-signed data, Signed and enveloped data.
130.	Give examples of applications of IPSec.
Ans.	Secure branch office connection over the internet, Secure remote access over the internet, Establishing extranet and intranet connectivity with partners, Establishing electronic commerce security
131.	What parameters identify an SA and what parameters characterize the nature of a particular SA?
Ans.	Security Associations (SA) are identified by the following three parameters: 1. Security Parameter Index 2. IP Destination Address 3. Security Protocol Identifier The following parameters characterize the nature of a particular SA: 1. Secret Key 2. Encapsulation Mode
132.	What is the difference between transport mode and tunnel mode?
Ans.	Authentication Headers and Encapsulation Security Payloads support two modes of use: transport mode and tunnel mode. Transport mode provides protection, primarily, for upper-layer protocols whereas tunnel mode provides security for the entire IP Packet being transmitted.
133.	What is the difference between an SSL connection and an SSL session?
Ans.	A SSL connection is a transport that provides a suitable type of service. In the case of SSL, such a connection is peer-to-peer and the connections are transient. Furthermore, each connection is associated with one SSL session, which is defined as the association between a client and a server. A session is created by the Handshake Protocol, and it defines a set of cryptographic security parameters which can be shared among multiple connections.
134.	What services are provided by the SSL Record Protocol?
Ans.	The SSL Record Protocol provides two services for SSL connections: 1. Confidentiality: The Handshake Protocol defines a shared secret key that is used for conventional encryption of SSL payloads. 2. Message Integrity: The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC). In SSL Record Protocol application data is divided into fragments. The fragment is compressed and then encrypted MAC (Message Authentication Code) generated by algorithms like SHA (Secure Hash Protocol) and MD5 (Message Digest) is appended. After that encryption of the data is done and in last SSL header is appended to the data.
135.	Write the name of SET participants?
Ans.	SET includes the following participants: • Cardholder – customer • Issuer – customer financial institution • Merchant • Acquirer – Merchant financial • Certificate authority – Authority which follows certain standards and issues certificates (like X.509V3) to all other participants.
136.	What is the difference between digital signatures and digital certificates?
Ans.	A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. Key Generation Algorithms: Digital signature are electronic signatures, which assures that the message was sent by a particular sender. While performing digital transactions authenticity and integrity should be assured, otherwise the data can be altered or someone can also act as if he was the sender and expect a reply. Signing Algorithms: To create a digital signature, signing algorithms like email programs create a one-way hash of the electronic data which is to be signed. The signing algorithm then encrypts the hash value using the private key (signature key). This encrypted hash along with other information like the hashing algorithm is the digital signature. This digital signature is appended with the data and sent to the verifier. The reason for encrypting the hash instead of the entire message or document is that a hash function converts any arbitrary input into a much shorter fixed length value. This saves time as now instead of signing a long message a shorter hash value has to be signed and moreover hashing is much faster than signing. Signature Verification Algorithms: Verifier receives Digital Signature along with the data. It then uses Verification algorithm to process on the digital signature and the public key (verification key) and generates some value. It also applies the same hash function on the received data and generates a hash value. Then the hash value and the output of the verification algorithm are compared. If they both are equal, then the digital

signature is valid else it is invalid.

Digital certificate is issued by a trusted third party which proves sender's identity to the receiver and receiver's identity to the sender.

A digital certificate is a certificate issued by a Certificate Authority (CA) to verify the identity of the certificate holder. The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. Digital certificate is used to attach public key with a particular individual or an entity.

Digital certificate contains:-

- Name of certificate holder
- Serial number which is used to uniquely identify a certificate, the individual or the entity identified by the certificate
- Expiration dates
- Copy of certificate holder's public key.(used for decrypting messages and digital signatures)
- Digital Signature of the certificate issuing authority
- Digital certificate is also sent with the digital signature and the message

137. How to protect the electronic transaction over Internet? Explain.

Ans. Secure Electronic Transaction or SET is a system which ensures security and integrity of electronic transactions done using credit cards in a scenario. SET is not some system that enables payment but it is a security protocol applied on those payments. It uses different encryption and hashing techniques to secure payments over internet done through credit cards. SET protocol was supported in development by major organizations like Visa, Mastercard, Microsoft which provided its Secure Transaction Technology (STT) and NetScape which provided technology of Secure Socket Layer (SSL). SET protocol restricts revealing of credit card details to merchants thus keeping hackers and thieves at bay. SET protocol includes Certification Authorities for making use of standard Digital Certificates like X.509 Certificate.

SET functionalities :

Provide Authentication:

- Merchant Authentication – To prevent theft, SET allows customers to check previous relationships between merchant and financial institution. Standard X.509V3 certificates are used for this verification.
- Customer / Cardholder Authentication – SET checks if use of credit card is done by an authorized user or not using X.509V3 certificates.

Provide Message Confidentiality: Confidentiality refers to preventing unintended people from reading the message being transferred. SET implements confidentiality by using encryption techniques. Traditionally DES is used for encryption purpose.

Provide Message Integrity: SET doesn't allow message modification with the help of signatures. Messages are protected against unauthorized modification using RSA digital signatures with SHA-1 and some using HMAC with SHA-1.

138. How to secure the wireless networks? Explain.

Ans. There are some ways to secure the wireless networks:

a) Change default passwords: Most network devices, including wireless access points, are pre-configured with default administrator passwords to simplify setup. These default passwords are easily available to obtain online, and so provide only marginal protection. Changing default passwords makes it harder for attackers to access a device. Use and periodic changing of complex passwords is your first line of defense in protecting your device.

b) Restrict access: Only allow authorized users to access your network. Each piece of hardware connected to a network has a media access control (MAC) address. You can restrict access to your network by filtering these MAC addresses. Consult your user documentation for specific information about enabling these features. You can also utilize the "guest" account, which is a widely used feature on many wireless routers. This feature allows you to grant wireless access to guests on a separate wireless channel with a separate password, while maintaining the privacy of your primary credentials.

c) Encrypt the data on your network: Encrypting your wireless data prevents anyone who might be able to access your network from viewing it. There are several encryption protocols available to provide this protection. Wi-Fi Protected Access (WPA), WPA2, and WPA3 encrypt information being transmitted between wireless routers and wireless devices. WPA3 is currently the strongest encryption. WPA and WPA2 are still available; however, it is advisable to use equipment that specifically supports WPA3, as using the other protocols could leave your network open to exploitation.

d) Protect your Service Set Identifier (SSID): To prevent outsiders from easily accessing your network, avoid publicizing your SSID. All Wi-Fi routers allow users to protect their device's SSID, which makes it more difficult for attackers to find a network. At the very least, change your SSID to something unique. Leaving it as the manufacturer's default could allow a potential attacker to identify the type of router and possibly exploit any known vulnerabilities.

e) Install a firewall: Consider installing a firewall directly on your wireless devices (a host-based firewall), as well as on your home network (a router- or modem-based firewall). Attackers who can directly tap into your wireless network may be able to circumvent your network firewall—a host-based firewall will add a layer of protection to the data on your computer.

f) Maintain antivirus software: Install antivirus software and keep your virus definitions up to date. Many antivirus programs also have additional features that detect or protect against spyware and adware.

g) Use file sharing with caution: File sharing between devices should be disabled when not needed. You should always choose to only allow file sharing over home or work networks, never on public networks. You may want to consider creating a dedicated directory for file sharing and restrict access to all other directories. In addition, you should password protect anything you share. Never open an entire hard drive for file sharing.

h) Keep your access point software patched and up to date. The manufacturer of your wireless access point will periodically release updates to and patches for a device's software and firmware. Be sure to check the manufacturer's website regularly for any updates or patches for your device.

i) Check your internet provider's or router manufacturer's wireless security options: Your internet service provider and router manufacturer may provide information or resources to assist in securing your wireless network. Check the customer support area of their websites for specific suggestions or instructions.

j) Connect using a Virtual Private Network (VPN): Many companies and organizations have a VPN. VPNs allow employees to connect securely to their network when away from the office. VPNs encrypt connections at the sending and receiving ends and keep out traffic that is not properly encrypted. If a VPN is available to you, make sure you log onto it any time you need to use a public wireless access point.

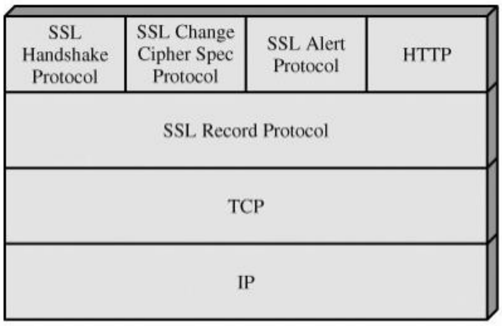
139. What do you mean by SSL protocol? How it works?

Ans. Netscape developed the Secure Sockets Layer (SSL) protocol to use public key encryption to secure a channel over the Internet, thus enabling secure communications. Most popular browsers, including Internet Explorer, use SSL. In addition to providing data encryption, integrity, and server authentication, SSL can, when properly configured, provide client authentication.

The SSL protocol works as follows: during a normal client/server HTTP session, the client requests access to a portion of the Web site that requires secure communications and the server sends a message to the client indicating that a secure connection must be established. The client sends its public key and security parameters. This handshaking phase is complete when the server finds a public key match and sends a digital certificate to the client in order to authenticate itself. Once the client verifies that the certificate is valid and trustworthy, the SSL session is established. Until the client or the server terminates the session, any amount of data can be transmitted securely.

140. Explain the SSL protocol stacks with diagram?

Ans. SSL is designed to make use of TCP to provide a reliable end-to-end secure service. SSL is not a single protocol but rather two layers of protocols.



The SSL Record Protocol provides basic security services to various higher-layer protocols. In particular, the Hypertext Transfer Protocol (HTTP), which provides the transfer service for Web client/server interaction, can operate on top of SSL. Three higher-layer protocols are defined as part of SSL: the Handshake Protocol, The Change Cipher Spec Protocol, and the Alert Protocol. These SSL-specific protocols are used in the management of SSL exchanges.

141. What do you mean by Secured HTTP? Explain.

Ans. Secure HTTP (S-HTTP) is an extended version of Hypertext Transfer Protocol that provides for the encryption of individual messages transmitted via the Internet between a client and server. S-HTTP is the application of SSL over HTTP, which allows the encryption of all information passing between two computers through a protected and secure virtual connection. Unlike SSL, in which a secure channel is established for the duration of a session, S-HTTP is designed for sending individual messages over the Internet and therefore a session for each individual exchange of data must be established. To establish a session, the client and server must have compatible cryptosystems and agree on the configuration. The S-HTTP client then must send the server its public key so that the server can generate a session key. The session key from the server is then encrypted with the client's public key and returned to the client. The client decrypts the key using its private key, and the client and server now possess identical session keys, which they can use to encrypt the messages sent between them. S-HTTP can provide confidentiality, authentication, and data integrity through a variety of trust models and cryptographic algorithms. In addition, this protocol is designed for easy integration with existing HTTP applications and for implementation in conjunction with HTTP.

142. Why is the segmentation and reassembly function in PGP needed?

Ans. E-mail facilities often are restricted to a maximum message length. For example, many of the facilities accessible through the Internet impose a maximum length of 50,000 octets. Any message longer than that must be broken up into smaller segments, each of which is mailed separately. To accommodate this restriction, PGP automatically subdivides a message that is too large into segments that are small enough to send via e-mail. The segmentation is done after all of the other processing, including the radix-64 conversion. Thus, the session key component and signature component appear only once, at the beginning of the first segment. Reassembly at the receiving end is required before verifying signature or decryption .

143. What do you mean by PGP? What are the functions or services provided by PGP? Explain.

Ans. PGP is a remarkable phenomenon. Largely the effort of a single person, Phil Zimmermann, PGP provides a confidentiality and authentication service that can be used for electronic mail and file storage applications. The actual operation of PGP, as opposed to the management of keys, consists of five services: authentication, confidentiality, compression, e-mail compatibility, and segmentation.

- Digital signature: A hash code of a message is created using SHA-1. This message digest is encrypted using DSS or RSA with the sender's private key and included with the message.
- Message encryption: A message is encrypted using CAST-128 or IDEA or 3DES with a one-time session key generated by the sender. The session key is encrypted using Diffie Hellman or RSA with the recipient's public key and included with the message.
- Compression: A message may be compressed, for storage or transmission, using ZIP.
- Email compatibility: To provide transparency for email applications, an encrypted message may be converted to an ASCII string using radix 64 conversions.
- Segmentation: To accommodate maximum message size limitations, PGP performs segmentation and reassembly.

144. Explain the parameters that define an SSL session state?

Ans. 1. Session identifier: This is an arbitrary byte sequence by the server to identify an active or resumable session state.
2. Peer certificate: This is an X509.v3 certificate of the peer. This element of the state may be null.
3. Compression method: This is the algorithm used to compress data prior to the encryption.
4. Cipher spec: This specifies the bulk data encryption (null, AES, etc.) and a hash algorithm (MD5 or SHA-1, etc.) sued for MAC calculation. This also defines cryptographic attributes such as the hash size.
5. Master secret: This is a 48-byte secret shared between the client and the server.
6. Is resumable: This is a flag indicating whether the session can be used to initiate new connections.

145. What are the limitations of existing mail transfer protocol SMTP?

Ans. MIME is an extension to the RFC 822 framework that is intended to address some of the problems and limitations of the use of SMTP (Simple Mail Transfer Protocol) or some other mail transfer protocol and RFC 822 for electronic mail. Following limitations of the SMTP/822 scheme:
1. SMTP cannot transmit executable files or other binary objects. A number of schemes are in use for converting binary files into a text form that can be used by SMTP mail systems, including the popular UNIX UUencode/UUdecode scheme. However, none of these is a standard or even a defacto standard.
2. SMTP cannot transmit text data that includes national language characters because these are represented by 8-bit codes with values of 128 decimal or higher, and SMTP is limited to 7-bit ASCII.
3. SMTP servers may reject mail message over a certain size.
4. SMTP gateways that translate between ASCII and the character code EBCDIC do not use a consistent set of mappings, resulting in translation problems.
5. SMTP gateways to X.400 electronic mail networks cannot handle non-textual data included in X.400 messages.
6. Some SMTP implementations do not adhere completely to the SMTP standards defined in RFC 821.
Common problems include:

- Deletion, addition, or reordering of carriage return and linefeed
- Truncating or wrapping lines longer than 76 characters
- Removal of trailing white space (tab and space characters)
- Padding of lines in a message to the same length
- Conversion of tab characters into multiple space characters

MIME is intended to resolve these problems in a manner that is compatible with existing RFC 822 implementations.

146. What do you mean by MIME? Explain the five header field defined in MIME?

Ans. MIME is an extension to the RFC 822 framework that is intended to address some of the problems and limitations of the use of SMTP (Simple Mail Transfer Protocol) or some other mail transfer protocol and RFC 822 for electronic mail.
The MIME specification includes the following elements:
1. Five new message header fields are defined, which may be included in an RFC 822 header. These fields provide information about the body of the message.
2. A number of content formats are defined, thus standardizing representations that support multimedia electronic mail.
3. Transfer encodings are defined that enable the conversion of any content format into a form that is protected from alteration by the mail system.

The five header fields defined in MIME are as follows:

- MIME-Version: Must have the parameter value 1.0. This field indicates that the message conforms to

RFCs 2045 and 2046.

- Content-Type: Describes the data contained in the body with sufficient detail that the receiving user agent can pick an appropriate agent or mechanism to represent the data to the user or otherwise deal with the data in an appropriate manner.
- Content-Transfer-Encoding: Indicates the type of transformation that has been used to represent the body of the message in a way that is acceptable for mail transport.
- Content-ID: Used to identify MIME entities uniquely in multiple contexts.
- Content-Description: A text description of the object with the body; this is useful when the object is not readable (e.g., audio data)

147. Explain the parameters that define an SSL session connection?

Ans. 1. Server and client random: These are byte sequences that are chosen by the server and client for each connection.

2. Server write MAC secret: This is the secret key used in MAC operations on data sent by the server.

3. Client write MAC secret: This is the secret key used in MAC operations on data sent by the client.

4. Server write key: This is the secret encryption key for data encrypted by the server and decrypted by the client.

5. Client write key: This is the symmetric encryption key for data encrypted by the client and decrypted by the server.

6. Initialization vectors: When a block cipher in CBC mode is used, an initialization vector (IV) is maintained for each key. This field is first initialized by the SSL Handshake Protocol. Thereafter, the final ciphertext block from each record is preserved for use as the IV with the following record.

7. Sequence numbers: Each party maintains separate sequence numbers for transmitted and received messages for each connection. When a party sends or receives a change cipher spec message, the appropriate sequence number is set to zero. Sequence numbers may not exceed 2^64-1.

148. What do you mean by WEP? What are the shortcomings of WEP protocol?

Ans. WEP was an early attempt to provide security with the 802.11 network protocol. It is now considered too cryptographically weak to provide any meaningful protection from eavesdropping, but for a time it did provide some measure of security for low-sensitivity networks. WEP uses the RC4 cipher stream to encrypt each packet using a 64-bit key. This key is created using a 24-bit initialization vector and a40-bit key value. The packets are formed using an XOR function to use the RC4 key value stream to encrypt the data packet. A 4-byte integrity check value (ICV) is calculated for each packet and then appended. According to many experts, WEP is too weak for use in most network settings because:

Key management is not effective since most networks use a single shared secret key value for each node. Synchronizing key changes is a tedious process, and no key management is defined in the protocol, so keys are seldom changed.

The initialization vector (IV) is too small, resulting in the recycling of IVs. An attacker can reverse engineer the RC4 cipher stream and decrypt subsequent packets, or can forge future packets. In 2007, this was accomplished in less than one minute.

In summary, an intruder who collects enough data can threaten a WEP network in just a few minutes by decrypting or altering the data being transmitted, or by forging the WEP key to gain unauthorized access to the network. WEP also lacks a means of validating user credentials to ensure that only those who should be on the network are allowed to access it.

149. What do you mean by TLS? How TLS is different from SSL? Explain.

Ans. TLS is an IETF standardization initiative whose goal is to produce an Internet standard version of SSL. TLS is defined as a Proposed Internet Standard in RFC 2246. RFC 2246 is very similar to SSLv3.

1. Version Number: The TLS Record Format is the same as that of the SSL Record Format, and the fields in the header have the same meanings. The one difference is in version values. For the current version of TLS, the Major Version is 3 and the Minor Version is 1.

2. Message Authentication Code: There are two differences between the SSLv3 and TLS MAC schemes: the actual algorithm and the scope of the MAC calculation. TLS makes use of the HMAC algorithm defined in RFC 2104. SSLv3 uses the same algorithm, except that the padding bytes are concatenated with the secret key rather than being XORed with the secret key padded to the block length. The level of security should be about the same in both cases. For TLS, the MAC calculation encompasses the fields indicated in the following expression:

HMAC_hash(MAC_write_secret, seq_num || TLSCompressed.type ||
TLSCompressed.version || TLSCompressed.length || TLSCompressed.fragment)

The MAC calculation covers all of the fields covered by the SSLv3 calculation, plus the field TLSCompressed.version, which is the version of the protocol being employed.

3. Pseudorandom Function: TLS makes use of a pseudorandom function referred to as PRF to expand secrets into blocks of data for purposes of key generation or validation. The objective is to make use of a relatively small shared secret value but to generate longer blocks of data in a way that is secure from the kinds of attacks made on hash functions and MACs.

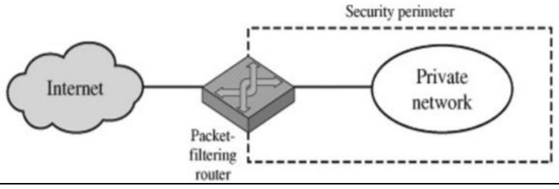
4. Alert Codes: TLS supports all of the alert codes defined in SSLv3 with the exception of no_certificate.

	5. Cipher Suites: There are several small differences between the cipher suites available under SSLv3 and under TLS: 6. Key Exchange: TLS supports all of the key exchange techniques of SSLv3 with the exception of Fortezza. 7. Symmetric Encryption Algorithms: TLS includes all of the symmetric encryption algorithms found in SSLv3, with the exception of Fortezza. 8. Padding: In SSL, the padding added prior to encryption of user data is the minimum amount required so that the total size of the data to be encrypted is a multiple of the cipher's block length. In TLS, the padding can be any amount that results in a total that is a multiple of the cipher's block length, up to a maximum of 255 bytes.
150.	How do viruses avoid basic pattern match of antivirus? a) They are encrypted b) They act with special permissions c) They modify themselves d) None of the mentioned
Ans.	c) They modify themselves
151.	How does an antivirus of today identify viruses? a) Previously known patterns b) It can detect unknown patterns c) It can take high priority to increase scanning speed d) None of the mentioned
Ans.	a) Previously known patterns
152.	What is known as a sandbox? a) It is a program which can be molded to do the desired task b) It is a program that is controlled or emulated section of OS c) It is a special mode of antivirus d) None of the mentioned
Ans.	b) It is a program that is controlled or emulated section of OS
153.	What are the different ways to intrude? a) Buffer overflows b) Unexpected combinations and unhandled input c) Race conditions d) All of the above
Ans.	d) All of the above
154.	What are the major components of the intrusion detection system? a) Analysis Engine b) Event provider c) Alert Database d) All of the above
Ans.	d) All of the above
155.	What are the characteristics of anomaly based IDS? a) It models the normal usage of network as a noise characterization b) It doesn’t detect novel attacks c) Anything distinct from the noise is not assumed to be intrusion activity d) It detects based on signature
Ans.	a) It models the normal usage of network as a noise characterization
156.	Who unleashed famous worm attack in 1988 which effected UNIX systems and caused losses in millions? a) Robert Morris b) Bob Milano c) Mark zuckerberg d) Bill Gates
Ans.	a) Robert Morris
157.	Which is not a port scan type? a) TCP scanning b) SYN scanning c) UDP scanning d) SYSTEM Scanning
Ans.	d) SYSTEM Scanning
158.	From the following, which is not a common file permission? a) Write b) Execute c) Stop d) Read
Ans.	c) Stop
159.	What does Light Directory Access Protocol (LDAP) doesn’t store? a) Users b) Address

	c) Passwords d) Security Keys
Ans.	b) Address
160.	Provide the security components of OS Security. a) User accounts Security b) BIOS Security c) Anti-virus Security d) All of these
Ans.	d) All of these
161.	Figure out the issues in Operating System Security. a) Authentication b) Malwares c) Software vulnerabilities d) All of these
Ans.	d) All of these
162.	An intrusion occurs when an attacker attempts to gain entry into or disrupt the normal operations of an information system.(True/False)
Ans.	True
163.	A network-based IDPS protects the server or host's information assets.(True/False)
Ans.	False
164.	A _____________ IDPS resides on a computer or appliance connected to a segment of an organization's network and monitors network traffic on that network segment, looking for indications of ongoing or successful attacks.
Ans.	network-based
165.	A ______________ IDPS resides on a particular computer or server, known as the host, and monitors activity only on that system.
Ans.	host-based
166.	During its lifetime, a typical virus goes through how much number of phases?
Ans.	4
167.	A ______ virus infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus.
Ans.	Boot sector
168.	A GFI LANguard is a __________ scanner tools.
Ans.	vulnerability
169.	A packet sniffer is a network tool that collects copies of packets from the network and analyses them. (True/False)
Ans.	True
170.	List and briefly define three classes of intruders.
Ans.	1. Masquerader: An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account. 2. Misfeasor: A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges. 3. Clandestine user: An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection.
171.	What are two common techniques used to protect a password file?
Ans.	1. One-way encryption: The system stores only an encrypted form of the user's password. When the user presents a password, the system encrypts that password and compares it with the stored value. In practice, the system usually performs a one-way transformation (not reversible) in which the password is used to generate a key for the encryption function and in which a fixed-length output is produced. 2. Access control: Access to the password file is limited to one or a very few accounts
172.	What are three benefits that can be provided by an intrusion detection system?
Ans.	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.
173.	What is a monitoring (or SPAN) port? What is it used for?
Ans.	A switched-port analysis port is a data port on a switched device that replicates all designated traffic from the switch device so that the traffic can be captured, stored or analyzed for IDS or other purposes.
174.	What is a honeypot? How is it different from a honeynet?
Ans.	A honeypot is a security mechanism that creates a virtual trap to lure attackers. An intentionally compromised computer system allows attackers to exploit vulnerabilities so we can study them to improve our security policies. We can apply a honeypot to any computing resource from software and networks to file servers and

	routers. Honeypots are a type of deception technology that allows us to understand attacker behavior patterns. Security teams can use honeypots to investigate cybersecurity breaches to collect intel on how cybercriminals operate. They also reduce the risk of false positives, when compared to traditional cybersecurity measures, because they are unlikely to attract legitimate activity. A honeynet is a decoy network that contains one or more honeypots. It looks like a real network and contains multiple systems but is hosted on one or only a few servers, each representing one environment. For example, a Windows honeypot machine, a Mac honeypot machine and a Linux honeypot machine.
175.	What is network footprinting? How are they related?
Ans.	An activity where the information about the organization along with their network activities and asserts are being gathered in called as network footprinting. It is a process where an organized research and investigations is made on internet address possessed by a targeted organization. Footprinting is a process where information that is available in public are gathered about a particular organization. The attackers generally collect information such as IP address of an organization to make organized attack. Footprinting is performed with the help of public internet data sources such as organizations webpage which can contain information about the internal systems.
176.	What is a vulnerability scanner? How is it used to improve security?
Ans.	Vulnerability scanners are automated tools that allow organizations to check if their networks, systems and applications have security weaknesses that could expose them to attacks. Vulnerability scanning is a common practice across enterprise networks and is often mandated by industry standards and government regulations to improve the organization's security posture.
177.	What is the difference between active and passive vulnerability scanners?
Ans.	Active Scanners: Active scanners send transmissions to the network's nodes, examining the responses they receive to evaluate whether a specific node represents a weak point within the network. A network administrator can also use an active scanner to simulate an attack on the network, uncovering weaknesses a potential hacker would spot, or examine a node following an attack to determine how a hacker breached security. Active scanners can take action to autonomously resolve security issues, such as blocking a potentially dangerous IP address. Passive Scanners: Passive scanners identify the active operating systems, applications and ports throughout a network, monitoring activity to determine the network's vulnerabilities. However, while passive scanners can provide information about weaknesses, they can't take action to resolve security problems. These scanners can check the current software and patch versions on networked devices, indicating which devices are using software that presents a potential gateway for hackers or trojan attacks, and reference this information against public databases containing lists of current patches. A network administrator can set passive scanners to run continuously or to operate at specified intervals.
178.	Define packet sniffing.
Ans.	When any data has to be transmitted over the computer network, it is broken down into smaller units at the sender's node called data packets and reassembled at receiver's node in original format. It is the smallest unit of communication over a computer network. It is also called a block, a segment, a datagram or a cell. The act of capturing data packet across the computer network is called packet sniffing. Packet sniffing is done by using tools called packet sniffer. It can be either filtered or unfiltered. Filtered is used when only specific data packets have to be captured and Unfiltered is used when all the packets have to be captured. WireShark, SmartSniff are examples of packet sniffing tools.
179.	Define open and close port.
Ans.	All communication that happens over the internet is exchanged via ports. Every IP address contains two kinds of ports, TCP and UDP, and there can be up to 65,535 of each for any given IP address. Services that connect to the internet (like web browsers, email clients, and file transfer services) use specific ports to receive information. In security parlance, the term open port is used to mean a TCP or UDP port number that is configured to accept packets. In contrast, a port which rejects connections or ignores all packets directed at it is called a closed port.
180.	Define the following terms: a) False negative b)False Positive c) Evasion d) Tuning
Ans.	a. False negative: The failure of an IDPS to react to an actual attack event. This is the most grievous failure, since the purpose of an IDPS is to detect and respond to attacks. b. False positive: An alert or alarm that occurs in the absence of an actual attack. A false positive can sometimes be produced when an IDPS mistakes normal system activity for an attack. False positives tend to make users insensitive to alarms and thus reduce their reactivity to actual intrusion events. c. Evasion: The process by which attackers change the format and/or timing of their activities to avoid being detected by the IDPS. d. Tuning: The process of adjusting an IDPS to maximize its efficiency in detecting true positives, while minimizing both false positives and false negatives.
181.	What are the different types of IDPS?
Ans.	There are two types of IDPS: 1. Network-based IDPS (NIDPS): A network-based IDPS is focused on protecting network information assets. 2. Host-based IDPS (HIDPS): A host-based IDPS protects the server or host's information assets. It monitors both network connection activity and current information states on host servers.

182.	Differentiate between virus and worm.
Ans.	A virus is a piece of software that can "infect" other programs by modifying them; the modification includes a copy of the virus program, which can then go on to infect other programs. A worm is a program that propagates copies of itself to other computers.
183.	What is firewall? What are the different types of firewall?
Ans.	A firewall forms a barrier through which the traffic going in each direction must pass. A firewall security policy dictates which traffic is authorized to pass in each direction. A firewall may be designed to operate as a filter at the level of IP packets, or may operate at a higher protocol layer. There are three types of firewall: 1. Packet Filtering Firewall 2. Application Level Gateway 3. Circuit Level Gateway
184.	What do you mean by port scanning? Explain.
Ans.	Port scanning utilities, or port scanners, are tools used by both attackers and defenders to identify (or fingerprint) the computers that are active on a network, as well as the ports and services active on those computers, the functions and roles the machines are fulfilling, and other useful information. A port is a network channel or connection point in a data communications system. There are 65,536 port numbers in use for TCP and another 65,536 port numbers for UDP. Services using the TCP/IP protocol can run on any port; however, services with reserved ports generally run on ports 1–1023. Port 0 is not used. Ports greater than 1023 are typically referred to as ephemeral ports and may be randomly allocated to server and client processes. An open port can be used by an attacker to send commands to a computer, potentially gain access to a server, and possibly exert control over a networking device. The general rule of thumb is to remove from service or secure any port not absolutely necessary to conducting business. For example, if a business doesn't host Web services, there is no need for port 80 to be available on its servers.
185.	How does a network-based IDPS differ from a host-based IDPS? Explain.
Ans.	Network-Based IDPS: A network-based IDPS (NIDPS) resides on a computer or appliance connected to a segment of an organization's network and monitors network traffic on that network segment, looking for indications of ongoing or successful attacks. When the NIDPS identifies activity that it is programmed to recognize as an attack, it responds by sending notifications to administrators. When examining incoming packets, an NIDPS looks for patterns within network traffic such as large collections of related items of a certain type—which could indicate that a denial-of-service attack is underway—or the exchange of a series of related packets in a certain pattern—which could indicate that a port scan is in progress. An NIDPS can detect many more types of attacks than a host-based IDPS, but it requires a much more complex configuration and maintenance program. A NIDPS is installed at a specific place in the network (such as on the inside of an edge router) from where it is possible to monitor the traffic going into and out of a particular network segment. Host-Based IDPS: While a network-based IDPS resides on a network segment and monitors activities across that segment, a host-based IDPS (HIDPS) resides on a particular computer or server, known as the host, and monitors activity only on that system. HIDPSs are also known as system integrity verifiers because they benchmark and monitor the status of key system files and detect when an intruder creates, modifies, or deletes monitored files. An HIDPS has an advantage over an NIDPS in that it can access encrypted information traveling over the network and use it to make decisions about potential or actual attacks. Also, since the HIDPS works on only one computer system, all the traffic it examines traverses that system. An HIDPS is also capable of monitoring system configuration databases, such as windows registries, in addition to stored configuration files like .ini, .cfg, and .dat files. Most HIDPSs work on the principle of configuration or change management, which means that they record the sizes, locations, and other attributes of system files.
186.	How does a signature-based IDPS differ from a behavior-based IDPS? Explain.
Ans.	A signature-based system looks for patterns of behavior that match a library of known behaviors. A behavior-based system watches for activities that suggest an alert-level activity is occurring based on sequences of actions or the timing between otherwise unrelated events.
187.	What kind of data and information can be found using a packet sniffer?
Ans.	A packet sniffer (sometimes called a network protocol analyzer) is a network tool that collects copies of packets from the network and analyzes them. It can provide a network administrator with valuable information for diagnosing and resolving networking issues. In the wrong hands, however, a sniffer can be used to eavesdrop on network traffic. An excellent free, client-based network protocol analyzer is Wireshark, formerly known as Ethereal. Wireshark allows the administrator to examine data from both live network traffic and captured traffic. Wireshark has several features, including a language filter and TCP session reconstruction utility.
188.	What is a virus? Explain the different phases of virus?
Ans.	A virus is a piece of software that can "infect" other programs by modifying them; the modification includes a copy of the virus program, which can then go on to infect other programs. A virus can do anything that other programs do. The only difference is that it attaches itself to another program and executes secretly when the host program is run. Once a virus is executing, it can perform any function, such as erasing files and programs. Parasitic virus: The traditional and still most common form of virus. A parasitic virus attaches itself to executable files and replicates, when the infected program is executed, by finding other executable files to infect. 1. Memory-resident virus: Lodges in main memory as part of a resident system program. From that point on, the virus infects every program that executes.

	2. Boot sector virus: Infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus. 3. Stealth virus: A form of virus explicitly designed to hide itself from detection by antivirus software. 4. Polymorphic virus: A virus that mutates with every infection, making detection by the "signature" of the virus impossible. 5. Metamorphic virus: As with a polymorphic virus, a metamorphic virus mutates with every infection. The difference is that a metamorphic virus rewrites itself completely at each iteration, increasing the difficulty of detection. Metamorphic viruses my change their behavior as well as their appearance.
189.	Differentiate between application level gateway and circuit level gateway firewall.
Ans.	An application-level gateway, also called a proxy server, acts as a relay of application-level traffic. The user contacts the gateway using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed. When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints. If the gateway does not implement the proxy code for a specific application, the service is not supported and cannot be forwarded across the firewall. Application-level gateways tend to be more secure than packet filters. Rather than trying to deal with the numerous possible combinations that are to be allowed and forbidden at the TCP and IP level, the application-level gateway need only scrutinize a few allowable applications. In addition, it is easy to log and audit all incoming traffic at the application level. A prime disadvantage of this type of gateway is the additional processing overhead on each connection. A circuit-level gateway can be a stand-alone system or it can be a specialized function performed by an application-level gateway for certain applications. A circuit-level gateway does not permit an end-to-end TCP connection; rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host. Once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents. The security function consists of determining which connections will be allowed.
190.	What is packet filtering firewall? Explain
Ans.	A packet-filtering router applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet. The router is typically configured to filter packets going in both directions (from and to the internal network). Filtering rules are based on information contained in a network packet.  Security perimeter Internet Private network Packet-filtering router
191.	What do you mean by Memory and Address Protection?
Ans.	Memory protection includes protection for the memory that the OS itself uses as well as the memory of user processes. Major challenge in multi-programming system is to prevent one program from affecting the data and programs in the memory space of other users.
192.	What is the difference between rule-based anomaly detection and rule-based penetration identification?
Ans.	With rule-based anomaly detection, historical audit records are analyzed to identify usage patterns and to generate automatically rules that describe those patterns. Rules may represent past behavior patterns of users, programs, privileges, time slots, terminals, and so on. Current behavior is then observed, and each transaction is matched against the set of rules to determine if it conforms to any historically observed pattern of behavior. Rule-based penetration identification uses rules for identifying known penetrations or penetrations that would exploit known weaknesses. Rules can also be defined that identify suspicious behavior, even when the behavior is within the bounds of established patterns of usage. Typically, the rules used in these systems are specific to the machine and operating system. Also, such rules are generated by "experts" rather than by means of an automated analysis of audit records.
193.	What is a salt in the context of UNIX password management?
Ans.	The salt is combined with the password at the input to the one-way encryption routine.
194.	What is the difference between statistical anomaly detection and rule-based intrusion detection?
Ans.	Statistical anomaly detection involves the collection of data relating to the behavior of legitimate users over a period of time. Then statistical tests are applied to observed behavior to determine with a high level of confidence whether that behavior is not legitimate user behavior. Rule-Based Detection involves an attempt to define a set of rules that can be used to decide that a given behavior is that of an intruder.
195.	What is an Intrusion Detection System? Explain.
Ans.	An intrusion occurs when an attacker attempts to gain entry into or disrupt the normal operations of an information system, almost always with the intent to do harm. Intrusion detection consists of procedures and systems that identify system intrusions. An IDS works like a burglar alarm in that it detects a violation (some system activity analogous to an opened or broken window) and activates an alarm. This alarm can be audible and/or visual (producing noise and lights, respectively), or it can be silent (an e-mail message or pager alert).

	With almost all IDSs, system administrators can choose the configuration of the various alerts and the alarm levels associated with each type of alert.
196.	What is the difference between stateful firewall and stateless firewall?
Ans.	A stateful firewall is a firewall that monitors the full state of active network connections. This means that stateful firewalls are constantly analyzing the complete context of traffic and data packets, seeking entry to a network rather than discrete traffic and data packets in isolation. Once a certain kind of traffic has been approved by a stateful firewall, it is added to a state table and can travel more freely into the protected network. Traffic and data packets that don't successfully complete the required handshake will be blocked. By taking multiple factors into consideration before adding a type of connection to an approved list, such as TCP stages, stateful firewalls are able to observe traffic streams in their entirety. However, this method of protection does come with a few vulnerabilities. For example, stateful firewalls can fall prey to DDoS attacks due to the intense compute resources and unique software-network relationship necessary to verify connections. Stateless firewalls are designed to protect networks based on static information such as source and destination. Whereas stateful firewalls filter packets based on the full context of a given network connection, stateless firewalls filter packets based on the individual packets themselves. To do so, stateless firewalls use packet filtering rules that specify certain match conditions. If match conditions are met, stateless firewall filters will then use a set of preapproved actions to guide packets into the network. If match conditions are not met, unidentified or malicious packets will be blocked. Because stateless firewalls do not take as much into account as stateful firewalls, they're generally considered to be less rigorous. For example, stateless firewalls can't consider the overall pattern of incoming packets, which could be useful when it comes to blocking larger attacks happening beyond the individual packet level.
197.	What are the different ways for memory and address protection of Operating System? Explain.
Ans.	Memory protection includes protection for the memory that the OS itself uses as well as the memory of user processes. Major challenge in multi-programming system is to prevent one program from affecting the data and programs in the memory space of other users. The various methods for memory and address protection are: i. Fence: A fence or fence address is simplest form of memory protection which can be used only for single user operating system. A fence is a particular address that users and their processes cannot cross. Only the OS can operate on one side of the fence and users are restricted to the other side. A fence could be static, in which case there is a fixed fence address. Alternatively, a dynamic fence can be used, which can be implemented using a fence register to specify the current fence address. ii. Base and Bounds registers: This type of protection can be used in multi- user environment where one users program needs to be protected from the other. Each user has a base register which is the lower address and a Bound register which is the upper address limit. The base and bounds register approach implicitly assumes that the user or process space is contiguous in memory. The OS must determine what protection to apply to a specific memory location. In some cases it might be sufficient to apply the same protection to all of a user's memory. The disadvantage is that the registers confine access to consecutive range of addresses. iii. Tagging: This specifies the protection for each individual address. In this method of protection every word of machine memory has one or more extra bits to identify the access rights to that word. Only privileged instructions can set these access bits. While this is as fine-grained protection as possible, it introduces significant overhead. The overhead can be reduced by tagging sections of the address space instead of each individual address. Another drawback to tagging is compatibility, since tagging schemes are not in common use. iv. Segmentation: This method divides the memory into logical units such as individual procedures or the data in one array. Once they are divided, appropriate access control can be enforced on each segment. A benefit of segmentation is that any segment can be placed in any memory location provided the location is large enough to hold it. The OS must keep track of the locations of all segments, which is accomplished using <segment,offset> pairs, where the named segment specifies the segment, and the offset is the starting address of the specified segment. With segmentation, all address references must go through the OS, so the OS can, in this respect, achieve complete mediation. Depending on the access control applied to particular segments, users can share access to some segments or users can be restricted to specific segments. v. Paging: Paging discards the disadvantage of segmentation. In paging all segments are of a fixed size called as pages and the memory divided is known as page frames. In paging a particular page can be accessed using a pair of the form <page, offset=""> where page is the page number and offset is location within a page. The advantages of paging over segmentation include no fragmentation, improved efficiency, and the fact that there are no variable sizes to worry about. The disadvantages are that there is, in general, no logical unity to pages, which makes it more difficult to determine the proper access control to apply to a given page.
198.	What do you mean by Intrusion Prevention Systems? Explain. Why IDPS is required?
Ans.	An intrusion occurs when an attacker attempts to gain entry into or disrupt the normal operations of an information system, almost always with the intent to do harm. Intrusion prevention consists of activities that deter an intrusion. Some important intrusion prevention activities are writing and implementing good enterprise information security policy, planning and executing effective information security programs, installing and testing technology-based information security countermeasures (such as firewalls and intrusion

	detection systems), and conducting and measuring the effectiveness of employee training and awareness activities. According to the NIST documentation on industry best practices, there are several compelling reasons to acquire and use an IDPS: 1. To prevent problem behaviors by increasing the perceived risk of discovery and punishment for those who would attack or otherwise abuse the system. 2. To detect attacks and other security violations that are not prevented by other security measures. 3. To detect and deal with the preambles to attacks (commonly experienced as network probes and other "doorknob rattling" activities). 4. To document the existing threat to an organization. 5. To act as quality control for security design and administration, especially in large and complex enterprises. 6. To provide useful information about intrusions that do take place, allowing improved diagnosis, recovery, and correction of causative factors.
199.	What are the different types of viruses? Explain,
Ans.	Parasitic virus: The traditional and still most common form of virus. A parasitic virus attaches itself to executable files and replicates, when the infected program is executed, by finding other executable files to infect. Memory-resident virus: Lodges in main memory as part of a resident system program. From that point on, the virus infects every program that executes. Boot sector virus: Infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus. Stealth virus: A form of virus explicitly designed to hide itself from detection by antivirus software. Polymorphic virus: A virus that mutates with every infection, making detection by the "signature" of the virus impossible. Metamorphic virus: As with a polymorphic virus, a metamorphic virus mutates with every infection. The difference is that a metamorphic virus rewrites itself completely at each iteration, increasing the difficulty of detection. Metamorphic viruses my change their behavior as well as their appearance.
200.	The EISP is based on and directly supports the ________________ of the organization and sets the strategic direction, scope, and tone for all security efforts. a) Vision b) Mission c)Direction d)All of these
Ans.	d)All of these
201.	Which of the following thing/s comes under the issue specific security policy: a) Use of phone b) Use of photocopy equipment c) Use of pen drive d) All of these
Ans.	d) All of these
202.	Information leakage is one of the threats of computer system specifically distributed systems where sensitive information can easily be revealed to unauthorized users that results to lack of integrity. (True/False)
Ans.	False
203.	Authorization is a prerequisite for authentication.
Ans.	False
204.	Lack of access control policy is a __________. a) Bug b) Threat c) Vulnerability d) Attack
Ans.	c) Vulnerability
205.	Security features that control that can access resources in the OS. a) Authentication b) Identification c) Validation d) Access control
Ans.	d) Access control
206.	A ________ is a plan or course of action that conveys instructions from an organization's senior management to those who make decisions, take actions, and perform other duties.
Ans.	policy
207.	Information security safeguards provide three levels of controls; what are they?
Ans.	managerial, operational, and technical
208.	A buffer against outside attacks is frequently referred to as a_______________.
Ans.	demilitarized zone (DMZ)
209.	Which direction access cannot happen using DMZ zone by default? a) Company computer to DMZ b) Internet to DMZ

	c) Internet to company computer d) Company computer to internet
Ans.	c) Internet to company computer
210.	The ACL that consists of a list related to an object that states all the subjects that can be allowed to access the object, as well as the rights to the object. (True/False)
Ans.	True
211.	Access control is the method by which systems determine whether and how to admit a user into a trusted area of the organization(True/False)
Ans.	True
212.	Nondiscretionary access controls (MACs) use data classification schemes; they give users and data owners limited control over access to information resources. (True/False)
Ans.	False
213.	A variation of Mandatory access controls is called_____________, in which users are assigned a matrix of authorizations for particular areas of access.
Ans.	lattice-based access control
214.	Discretionary controls are a strictly-enforced version of MACs that are managed by a central authority in the organization and can be based on an individual's role.(True/False)
Ans.	False
215.	An information security policy provides rules for the protection of the information assets of the organization.(True/False)
Ans.	True
216.	Issue specific security policies often function as standards or procedures to be used when configuring or maintaining systems.(True/False)
Ans.	False
217.	A ____________ might describe the configuration and operation of a network firewall.
Ans.	System Specific Security Policy
218.	Indicate the security standard that specifies a management system to bring information security under management control. a) ISO 27002 b) ISO 27001 c) ISO 3200 d) ISO 3201
Ans.	b) ISO 27001
219.	Which of the following threat may occur in the distributed system? a) Denial of Service b)Information Leakage c) Unauthorized Access d)All of these
Ans.	d) All of these
220.	What do you mean by access control?
Ans.	Access control is the method by which systems determine whether and how to admit a user into a trusted area of the organization—that is, information systems, restricted areas such as computer rooms, and the entire physical location. Access control is achieved by means of a combination of policies, programs, and technologies.
221.	What are the different types of access control?
Ans.	Access controls can be of three types: 1. Mandatory Access Control 2. Nondiscretionary Access Control 3. Discretionary Access Control
222.	What are the different methods for logical access control?
Ans.	Logical access control is done via access control lists (ACLs), group policies, passwords, and account restrictions.
223.	What did you understand from information security policies?
Ans.	A policy is a plan or course of action that conveys instructions from an organization's senior management to those who make decisions, take actions, and perform other duties. Policies are organizational laws in that they dictate acceptable and unacceptable behavior within the organization. An information security policy provides rules for the protection of the information assets of the organization.
224.	What are the different types of information security policies?
Ans.	There are three types of security policy, according to the National Institute of Standards and Technology's: 1. Enterprise information security policies 2. Issue-specific security policies 3. Systems-specific security policies
225.	Write the name of different threats to the distributed system?
Ans.	There are different threats when distributed system is concerned, as any networked computer system can face it. It is important to implement countermeasures for all expected threats for the purpose of the system to remain constant and cost effective. Those threats can be distinguished depending on their interaction as follows below: 1. Denial of service

	2. Information leakage 3. Unauthorized access
226.	What are the major design issues in building secure distributed system?
Ans.	The major design issues in building secure distributed systems are: 1. Focus of control 2. Layering of security mechanism Focus of control: There are three approaches that can be followed to protect a distributed application: a. Protection against invalid operations on secure data b. Protection against unauthorized invocations c. Protection against unauthorized users Layering of security mechanism: One of the important aspect of designing secure systems is to decide which level the security mechanism should be placed. Security mechanism is normally placed in middleware in a distributed system.
227.	What do you mean by database security? Explain.
Ans.	All systems have ASSETS and security is about protecting assets. The first thing, then, is to know your assets and their value. The second thing to know is what THREATs are putting your assets at risk. These include things such as power failure and employee fraud. Note that threats are partly hypothetical, always changing and always imperfectly known. Security activity is directed at protecting the system from perceived threats.
228.	Write the names of the different threats to database security?
Ans.	• Unauthorised modification • Unauthorised disclosure • Loss of availability • Commercial sensitivity • Personal privacy and data protection • Computer misuse
229.	What do you mean by database security models?
Ans.	A security model establishes the external criteria for the examination of security issues in general, and provides the context for database considerations, including implementation and operation. There are two database security models: 1. Authentication 2. Authorization
230.	What is a distributed denial-of-service attack? Explain.
Ans.	A distributed denial of-service (DDoS) is an attack in which a coordinated stream of requests is launched against a target from many locations at the same time. Most DDoS attacks are preceded by a preparation phase in which many systems, perhaps thousands, are compromised. The compromised machines are turned into zombies, machines that are directed remotely (usually by a transmitted command) by the attacker to participate in the attack. DDoS attacks are the most difficult to defend against, and there are presently no controls that any single organization can apply.
231.	Write the name of modules exist in the ORACLE DBSAT?
Ans.	The DBSAT tool contains three modules: 1. Collector 2. Reporter 3. Discoverer Collector and Reporter work together to discover any risk areas and will produce reports regarding those risk areas – the Database Security Assessment report. The Discoverer is a stand-alone module used to locate and report on sensible data – and will produce the Database Sensitive Data Assessment report.
232.	What is the ISO 27000 series of standards?
Ans.	The ISO 27000 family of information security management standards is a series of mutually supporting information security standards that can be combined to provide a globally recognised framework for best-practice information security management.
233.	What are the differences between a policy, a standard, and a practice?
Ans.	Policy - Written instructions that describe proper behavior. Standard - Detailed statement of what must be done to comply with policy. Practice - Examples of actions that would comply with policy.
234.	Where can a security administrator find information on established security frameworks?
Ans.	ISO/IEC 27002 gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s). It is designed to be used by organizations that intend to: • select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001; • implement commonly accepted information security controls; • develop their own information security management guidelines.

235. Write about the worst-case assumptions and design guidelines for secure Distributed Systems.

Ans. Interfaces are exposed: Distributed systems are composed of processes that offer services or share information. Their communication interfaces are necessarily open (to allow new clients to access them) - an attacker can send a message to any interface.

Networks are insecure: For example, message sources can be falsified - messages can be made to look as though they came from Alice when they were actually sent by Mallory. Host addresses can be `spoofed' - Mallory can connect to the network with the same address as Alice and receive copies of messages intended for her.

Limit the lifetime and scope of each secret: When a secret key is first generated we can be confident that it has not been compromised. The longer we use it and the more widely it is known, the greater the risk. The use of secrets such as passwords and shared secret keys should be time-limited, and sharing should be restricted.

Algorithms and program code are available to attackers: The bigger and the more widely distributed a secret is, the greater the risk of its disclosure. Secret encryption algorithms are totally inadequate for today's large-scale network environments. Best practice is to publish the algorithms used for encryption and authentication, relying only on the secrecy of cryptographic keys. This helps to ensure that the algorithms are strong by throwing them open to scrutiny by third parties.

Attackers may have access to large resources: The cost of computing power is rapidly decreasing. We should assume that attackers will have access to the largest and most powerful computers projected in the lifetime of a system, then add a few orders of magnitude to allow for unexpected developments.

Minimize the trusted base: The portions of a system that are responsible for the implementation of its security, and all the hardware and software components upon which they rely, have to be trusted - this is often referred to as the trusted computing base. Any defect or programming error in this trusted base can produce security weaknesses, so we should aim to minimize its size. For example, application programs should not be trusted to protect data from their users.

236. Compare Nondiscretionary Access Control and Discretionary Access Control.

Ans. Nondiscretionary controls are a strictly-enforced version of MACs that are managed by a central authority in the organization and can be based on an individual's role—role-based controls—or a specified set of tasks (subject- or object-based)—task-based controls.

Role-based controls are tied to the role a user performs in an organization, and task-based controls are tied to a particular assignment or responsibility. The role and task controls make it easier to maintain the controls and restrictions associated with a particular role or task, especially if the individual performing the role or task changes often. Instead of constantly assigning and revoking the privileges of individuals who come and go, the administrator simply assigns the associated access rights to the role or task, and then whenever individuals are associated with that role or task, they automatically receive the corresponding access. When their turns are over, they are removed from the role or task and the access is revoked.

Discretionary access controls (DACs) are implemented at the discretion or option of the data user. The ability to share resources in a peer-to-peer configuration allows users to control and possibly provide access to information or resources at their disposal. The users can allow general, unrestricted access, or they can allow specific individuals or sets of individuals to access these resources. For example, a user has a hard drive containing information to be shared with office co-workers. This user can elect to allow access to specific individuals by providing access, by name, in the share control function.

237. Write about the enterprise information security policies?

Ans. An enterprise information security policy (EISP) is also known as a general security policy, organizational security policy, IT security policy, or information security policy. The EISP is based on and directly supports the mission, vision, and direction of the organization and sets the strategic direction, scope, and tone for all security efforts. The EISP is an executive level document, usually drafted by or in cooperation with the chief information officer of the organization. This policy is usually two to ten pages long and shapes the philosophy of security in the IT environment. The EISP usually needs to be modified only when there is a change in the strategic direction of the organization. The EISP guides the development, implementation, and management of the security program. It sets out the requirements that must be met by the information security blueprint or framework. It defines the purpose, scope, constraints, and applicability of the security program. It also assigns responsibilities for the various areas of security, including systems administration, maintenance of the information security policies, and the practices and responsibilities of the users. Finally, it addresses legal compliance.

According to the National Institute of Standards and Technology (NIST), the EISP typically addresses compliance in the following two areas:

1. General compliance to ensure meeting the requirements to establish a program and the responsibilities assigned therein to various organizational components.
2. The use of specified penalties and disciplinary action.

238. Write about the issues specific security policies?

Ans. As an organization executes various technologies and processes to support routine operations, it must instruct employees on the proper use of these technologies and processes. In general, the issue-specific security policy, or ISSP,

- addresses specific areas of technology as listed below,
- requires frequent updates, and
- contains a statement on the organization’s position on a specific issue.

An ISSP may cover the following topics, among others:

- E-mail
- Use of the Internet
- Specific minimum configurations of computers to defend against worms and viruses
- Prohibitions against hacking or testing organization security controls
- Home use of company-owned computer equipment
- Use of personal equipment on company networks
- Use of telecommunications technologies (fax and phone)
- Use of photocopy equipment

239. Write about the system specific security policies?

Ans. System Specific Security Policies (SysSPs) often function as standards or procedures to be used when configuring or maintaining systems. For example, a SysSP might describe the configuration and operation of a network firewall. This document could include a statement of managerial intent; guidance to network engineers on the selection, configuration, and operation of firewalls; and an access control list that defines levels of access for each authorized user. SysSPs can be separated into two general groups, managerial guidance and technical specifications, or they can be combined into a single policy document.

240. What is ORACLE DBSAT? What does DBSAT check? Explain.

Ans. The Oracle Database Security Assessment Tool is a stand-alone command line tool that accelerates the assessment and regulatory compliance process by collecting relevant types of configuration information from the database and evaluating the current security state to provide recommendations on how to mitigate the identified risks. DBSAT enables customers to quickly find:

- Security configuration issues, and how to remediate them
- Users and their entitlements
- Location, type, and quantity of sensitive data

DBSAT analyses information on the database and listener configuration to identify configuration settings that may unnecessarily introduce risk. DBSAT goes beyond simple configuration checking, examining user accounts, privilege and role grants, authorization control, separation of duties, fine-grained access control, data encryption and key management, auditing policies, and OS file permissions. DBSAT applies rules to quickly assess the current security status of a database and produce findings in all the areas above. For each finding, DBSAT recommends remediation activities that follow best practices to reduce or mitigate risk. DBSAT also scans the database for sensitive data using customizable regular expression patterns, and reports on the amount and type of sensitive data found. Besides providing the ability to search for sensitive data on English based data dictionaries (column names and comments) it also includes support for additional major European languages such as Dutch, French, Italian, German, Portuguese and Spanish. This provides organizations with a deeper insight on how much sensitive data they have and where it resides, enabling them to then protect their databases through appropriate access controls, auditing, masking, and encryption.

241. Write a short note on Cluster Computing Security?

Ans. Clustering security is one of the most important factors that needs to be considered during clustering. Connectivity, especially when they are implemented through the internet, is susceptible to any type of attack. The attacks to clustering of nodes could come in different forms – it could be as simple as a virus wherein its sole purpose is to destroy files or could be a very powerful spyware that can easily hijack the controls of nodes for malicious purposes.

It only takes a single security flaw to destroy the entire clustering configuration. Whenever a network opens up a connection to its administrator, it automatically opens itself to different forms of attacks. This is also possible for users who try to access the nodes and stores data.

In gist, there is always a possibility of attack whenever an interaction happens with the client and the server. This is practically the “security nightmare” in clustering since interaction will always happen which means the nodes are always susceptible to different attacks.

For domain based security for clusters, administrator could easily control the clusters since security is based online. It does not even matter where the administrator implements security and troubleshooting as long as there is a strong connection between the clusters and the administrator.

However, domain based security could be easily hacked. Anything that is done online could be monitored and used against the administrator’s will. Local security on the other hand boasts of optimal security by localizing administrator credentials for access.

Most of the network tools for clustering today are using this form of security measure. But this type of security protocol is not easy. It requires a lot of resources especially when they are configured for the first time. Access to local nodes will also be challenging especially when the administrator tries to access them through online connectivity.

242. Compare managerial, operational, and technical levels of controls.

Ans. Managerial Control: Managerial controls are security processes that are designed by strategic planners and implemented by the security administration of the organization. Management controls set the direction and

	scope of the security process and provide detailed instructions for its conduct, as well as addressing the design and implementation of the security planning process and security program management. They also address risk management and security control reviews, describe the necessity and scope of legal compliance, and set guidelines for the maintenance of the entire security life cycle. Operational Controls: Operational controls are management and lower-level planning functions that deal with the operational functionality of security in the organization, such as disaster recovery and incident response planning. Operational controls address personnel security, physical security, and the protection of production inputs and outputs. In addition, operational controls guide the development of education, training, and awareness programs for users, administrators, and management. Finally, they address hardware and software systems maintenance and the integrity of data. Technical Controls: Technical controls are the tactical and technical implementations of security in the organization. While operational controls address specific operational issues, such as developing and integrating controls into the business functions, technical controls are the components put in place to protect an organization's information assets. They include logical access controls, such as identification, authentication, authorization, accountability (including audit trails), cryptography, and the classification of assets and users.
243.	What do you mean by Access Control Lists (ACL)? Explain.
Ans.	Access control lists (ACLs) consist of the user access lists, matrices, and capability tables that govern the rights and privileges of users. ACLs can control access to file storage systems, software components, or network communications devices. A capabilities table specifies which subjects and objects users or groups can access; in some systems, capabilities tables are called user profiles or user policies. These specifications frequently take the form of complex matrices, rather than simple lists or tables. The access control matrix includes a combination of tables and lists, such that organizational assets are listed along the column headers, while users are listed along the row headers. The resulting matrix contains ACLs in columns for a particular device or asset, and capability tables in rows for a particular user. ACLs can restrict access for a particular user, computer, time, duration—even a particular file. This specificity provides powerful control to the administrator. In general, ACLs regulate the following: • Who can use the system • What authorized users can access • When authorized users can access the system • Where authorized users can access the system from The who of ACL access may be determined by a person's identity or by a person's membership in a group. Restricting what authorized users are permitted to access—whether by type (printers, files, communication devices, or applications), name, or location—is achieved by adjusting the resource privileges for a person or group to one of Read, Write, Create, Modify, Delete, Compare, or Copy. To control when access is allowed, some organizations implement time-of-day and/or day-of-week restrictions for some network or system resources. To control where resources can be accessed from, many network-connected assets block remote usage and also have some levels of access that are restricted to locally connected users. When these various ACL options are applied concurrently, the organization can govern how its resources can be used.
244.	Explain the mandatory access control?
Ans.	Mandatory access controls (MACs) use data classification schemes; they give users and data owners limited control over access to information resources. In a data classification scheme, each collection of information is rated, and each user is rated to specify the level of information that user may access. These ratings are often referred to as sensitivity levels, and they indicate the level of confidentiality the information requires. A variation of this form of access control is called lattice-based access control, in which users are assigned a matrix of authorizations for particular areas of access. The level of authorization may vary between levels, depending on the classification authorizations individuals possess for each group of information or resources. The lattice structure contains subjects and objects, and the boundaries associated with each pair are demarcated. Lattice-based control specifies the level of access each subject has to each object. With this type of control, the column of attributes associated with a particular object (such as a printer) is referred to as an access control list (ACL). The row of attributes associated with a particular subject (such as a user) is referred to as a capabilities table.
245.	Explain the authentication and authorization Database security models?
Ans.	A security model establishes the external criteria for the examination of security issues in general, and provides the context for database considerations, including implementation and operation. Authentication: The client has to establish the identity of the server and the server has to establish the identity of the client. This is done often by means of shared secrets (either a password/user-id combination, or shared biographic and/or biometric data). It can also be achieved by a system of higher authority which has previously established authentication. In client-server systems where data (not necessarily the database) is distributed, the authentication may be acceptable from a peer system. Note that authentication may be transmissible from system to system. The result, as far as the DBMS is concerned, is an authorisation identifier. Authentication does not give any privileges for particular tasks. It only establishes that the DBMS trusts that the user is who he/she claimed to be and that the user trusts that the DBMS is also the intended system. Authentication is a prerequisite for authorisation.

	Authorization: Authorisation relates to the permissions granted to an authorised user to carry out particular transactions, and hence to change the state of the database (write item transactions) and/or receive data from the database (read-item transactions). The result of authorisation, which needs to be on a transactional basis, is a vector: Authorisation (item, auth-id, operation). A vector is a sequence of data values at a known location in the system. How this is put into effect is down to the DBMS functionality. At a logical level, the system structure needs an authorisation server, which needs to co-operate with an auditing server. There is an issue of server-to-server security and a problem with amplification as the authorisation is transmitted from system to system. Amplification here means that the security issues become larger as a larger number of DBMS servers are involved in the transaction. Audit requirements are frequently implemented poorly. To be safe, you need to log all accesses and log all authorisation details with transaction identifiers. There is a need to audit regularly and maintain an audit trail, often for a long period.
246.	Explain the distributed system security mechanisms?
Ans.	a. Cryptography: The security of information transmitted from one node to another is questionable, therefore there is a need of using a proper method of transforming it into unreadable formats (secrets writing) through cryptography. The use of a single key or public key cryptographic algorithm which is suitable for protecting message content by hiding information carried by a packet during the transmission process. This can be accomplished using RSA or AES algorithms. b. Authentication protocol: Provides a series of communication procedures between users of the system and the server for the purpose of securing the communication process. c. Access control mechanism: This can be done using access control lists (ACL) that consists of a list related to an object that states all the subjects that can be allowed to access the object, as well as the rights to the object. ACL normally are implemented directly or as an approximation in recent Operating systems.
247.	What do you mean by security to distributed system? What are the different threats to the distributed system? Explain.
Ans.	Today, computers are not stand alone units. Several computers are being networked together to form large computer systems. Not only are computers being network, but they are being networked into large distributed systems where each individual computer, node if you will, can make use of the applications distributed throughout the system. There are different threats when distributed system is concerned, as any networked computer system can face it. It is important to implement countermeasures for all expected threats for the purpose of the system to remain constant and cost effective. Those threats can be distinguished depending on their interaction as follows below: 1. Denial of service: Involves attacks that affect the availability of information from the system to the user resulting to paralysation of the entire operation of an organization or part of activities depending on the attack. The use of resource control mechanism can help in solving the above problem by applying timing responses, sizing responses, and connection control. Also problem detection by timing latency in system can easily be done if there is a dramatic increase of latency then denial of service (DoS) can be detected as well as addressed. 2. Information leakage: is one of the threats of computer system specifically distributed systems where sensitive information can easily be revealed to unauthorized users that results to lack of confidentiality. 3. Unauthorized access: This can occur due to the reason that the physical configuration is not strong enough to protect such threats from accessing the system (distributed system). This is known as inter process communication threats. Access control policies will enable organizations to be able to specify different ways that will lead to proper management of access to resources as well as information which are the valuable assets of an organization.
248.	What are the different threats to the database security? Explain.
Ans.	a. Unauthorised modification: Changing data values for reasons of sabotage, crime or ignorance which may be enabled by inadequate security mechanisms, or sharing of passwords or password guessing, for example. b. Unauthorised disclosure: When information that should not have been disclosed has been disclosed. A general issue of crucial importance, which can be accidental or deliberate. c. Loss of availability: Sometimes called denial of service. When the database is not available it incurs a loss (otherwise life is better without the system!). So any threat that gives rise to time offline, even to check whether something has occurred, is to be avoided. d. Commercial sensitivity: Most financial losses through fraud arise from employees. Access controls provide both protection against criminal acts and evidence of attempts (successful or otherwise) to carry out acts detrimental to the organisation, whether fraud, extraction of sensitive data or loss of availability. e. Personal privacy and data protection: Internationally, personal data is normally subject to legislative controls. Personal data is data about an identifiable individual. Often the individual has to be alive but the method of identification is not prescribed. So a postal code for a home may in some cases identify an individual, if only one person is living at an address with the postal code. Such data needs careful handling and control.

	f. Computer misuse: There is also generally legislation on the misuse of computers. Misuse includes the violation of access controls and attempts to cause damage by changing the database state or introducing worms and viruses to interfere with proper operation. These offences are often extraditable. So an unauthorised access in Hong Kong using computers in France to access databases in Germany which refer to databases in America could lead to extradition to France or Germany or the USA. g. Audit requirements: These are operational constraints built around the need to know who did what, who tried to do what, and where and when everything happened. They involve the detection of events (including CONNECT and GRANT transactions), providing evidence for detection, assurance as well as either defence or prosecution. There are issues related to computer-generated evidence not covered here.
249.	How to protect the database from various security threats? Explain.
Ans.	To protect the database system from various threats. Here are some countermeasures which are as follows: a. Access Control: A database for an organization contains a great deal of information and usually has several users. Most of them need to access only a small part of the database. A policy defines the requirements that are to be implemented within hardware and software and those that are external to the system, including physical, personal, and procedural controls. b. Flow Control: Flow control provides the flow of information among accessible objects. Flow controls check that information contained in objects does not flow explicitly or implicitly into less protected objects. c. Encryption: An encryption algorithm should be applied to the data, using a user-specified encryption key. The output of the algorithm is the encrypted version. There is also a decryption algorithm, which takes the encrypted data and a decryption key as input and then returns the original data. d. RAID: Redundant Array of Independent Disks which protect against data loss due to disk failure. e. Authentication: Access to the database is a matter of authentication. It provides the guidelines how the database is accessed. Every access should be monitored. f. Backup: At every instant, backup should be done. In case of any disaster, Organizations can retrieve their data.