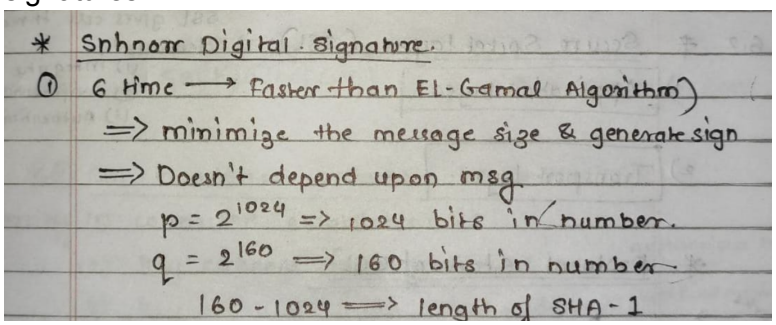
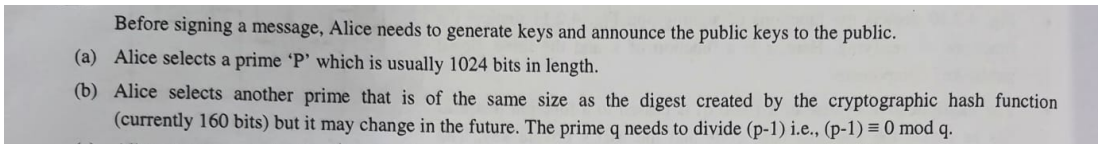
Yellow - remaining to read.

1. What are the steps of Schorr Digital Signature?
Ans)
It is a digital signature scheme known for its simplicity, and efficiency and generates short signatures.



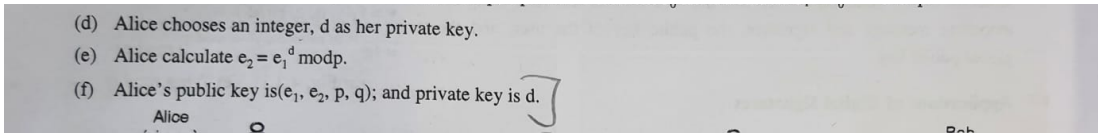
The steps of Schorr Digital Signature are as follows:

1. Key Generation:


Before signing a message, Alice needs to generate keys and announce the public keys to the public.

(a) Alice selects a prime 'P' which is usually 1024 bits in length.

(b) Alice selects another prime that is of the same size as the digest created by the cryptographic hash function (currently 160 bits) but it may change in the future. The prime q needs to divide (p-1) i.e., (p-1) ≡ 0 mod q.

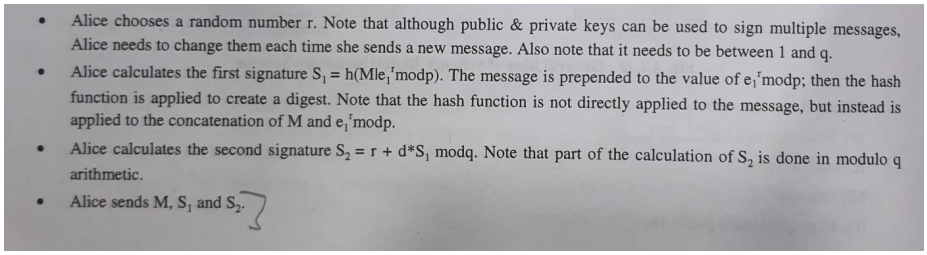

(d) Alice chooses an integer, d as her private key.

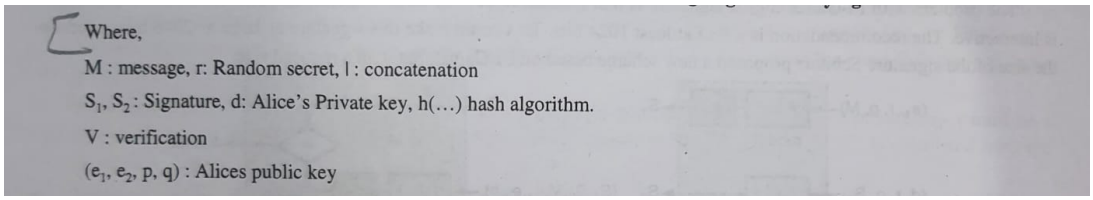
(e) Alice calculate $e_2 = e_1^{\,d} \bmod p$.

(f) Alice's public key is(e_1, e_2, p, q); and private key is d.

Alice

2. Signing:


- Alice chooses a random number r. Note that although public & private keys can be used to sign multiple messages, Alice needs to change them each time she sends a new message. Also note that it needs to be between 1 and q.
- Alice calculates the first signature $S_1 = h(M|e_1^{\,r} \bmod p)$. The message is prepended to the value of $e_1^{\,r} \bmod p$; then the hash function is applied to create a digest. Note that the hash function is not directly applied to the message, but instead is applied to the concatenation of M and $e_1^{\,r} \bmod p$.
- Alice calculates the second signature $S_2 = r + d*S_1 \bmod q$. Note that part of the calculation of S_2 is done in modulo q arithmetic.
- Alice sends M, S_1 and S_2.


Where,

M : message, r: Random secret, | : concatenation

S_1, S_2 : Signature, d: Alice's Private key, h(…) hash algorithm.

V : verification

(e_1, e_2, p, q) : Alices public key

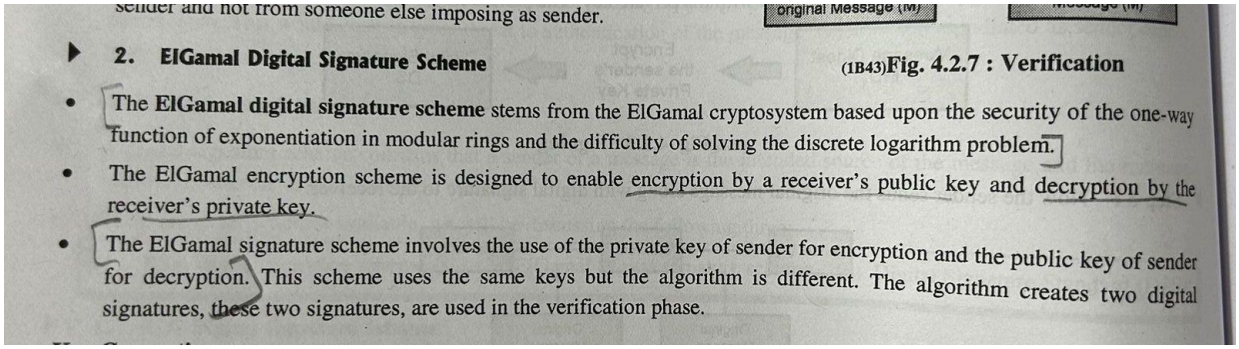
3. Verifying Message:

- Assume that the receiver Bob, receives M, S_1 and S_2.
- Bob calculates $V = h(Mle_1^{S}{}_2e_2^{-S}{}_1 \text{mod} p)$

If S_1 is congruent to V modulo p, the message is accepted otherwise rejected.

2. Write the Working process of El Gamal algorithm.

Ans)



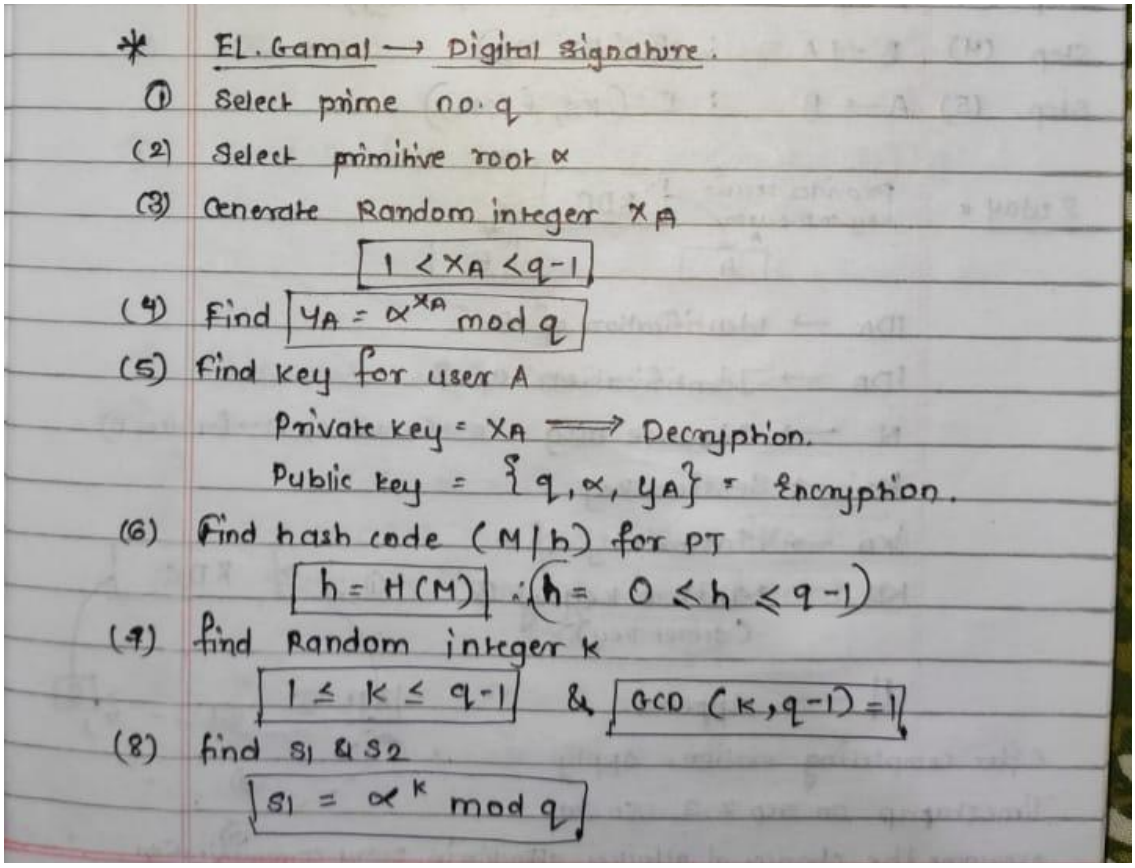
sender and not from someone else imposing as sender.

original Message (M)

2. ElGamal Digital Signature Scheme

(1B43)**Fig. 4.2.7 : Verification**

- The **ElGamal digital signature scheme** stems from the ElGamal cryptosystem based upon the security of the one-way function of exponentiation in modular rings and the difficulty of solving the discrete logarithm problem.
- The ElGamal encryption scheme is designed to enable encryption by a receiver's public key and decryption by the receiver's private key.
- The ElGamal signature scheme involves the use of the private key of sender for encryption and the public key of sender for decryption. This scheme uses the same keys but the algorithm is different. The algorithm creates two digital signatures, these two signatures, are used in the verification phase.



* EL. Gamal → Digital Signature.

(1) Select prime no. q

(2) Select primitive root α

(3) Generate Random integer X_A

$1 < X_A < q-1$

(4) Find $Y_A = \alpha^{X_A} \text{ mod } q$

(5) Find key for user A

Private key = X_A ⟹ Decryption.

Public key = $\{q, \alpha, Y_A\}$ = Encryption.

(6) Find hash code (M/h) for PT

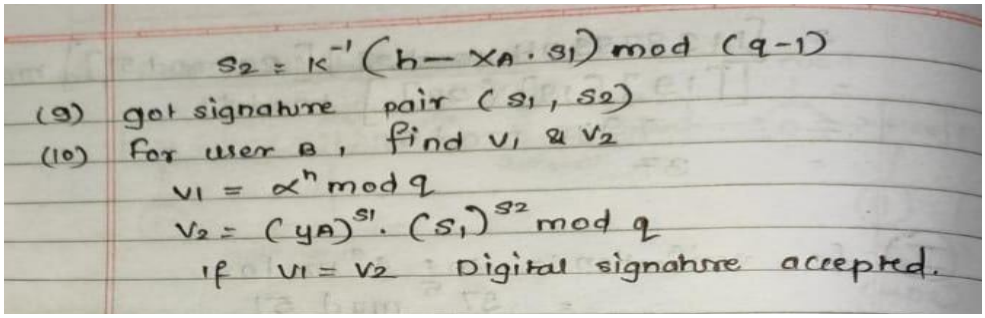
$h = H(M)$ ∴ $(h = 0 \leq h \leq q-1)$

(7) find Random integer k

$1 \leq K \leq q-1$ & $GCD(K, q-1) = 1$

(8) find S_1 & S_2

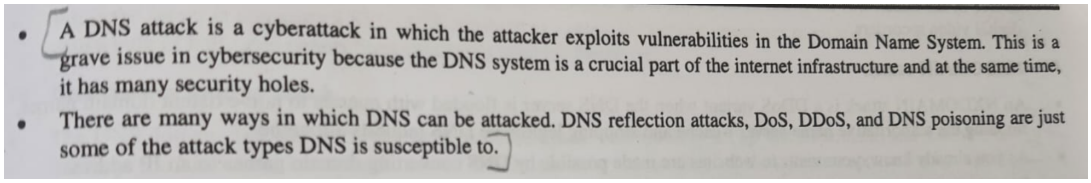
$S_1 = \alpha^K \text{ mod } q$



3. Define DNS attack and web Browser Attack with examples.

Ans)

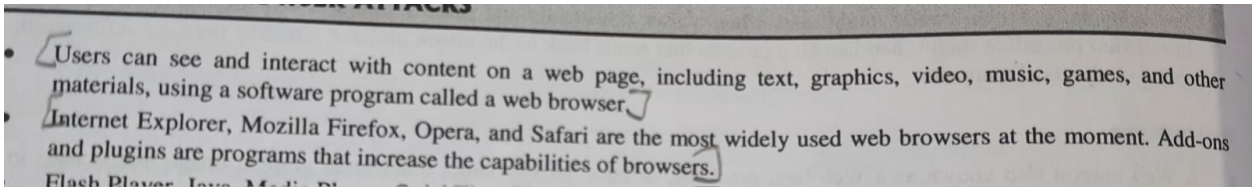
DNS Attack:



Denial of Service (DOS): The denial-of-service attack is an attack in which a system is attacked by a lot of requests to the system at one time that it is not able to handle. The attacker sends multiple requests to the server at the same time and the server is not able to handle such requests. However, this attack is easily identifiable as these loads of requests come from a single sender (the attacker) and it is easy to identify the source of the attack.

● **Distributed Denial of Service (DDOS):** As we saw, in the denial-of-service attack, the source of the attack can be easily identified. Now, there is a modified version of this attack i.e., DDOS i.e., distributed version of the DOS attack. In this attack, the attacker first observes the details of a lot of authorized users. Then, the attacker uses these authorized users at the same time to send requests to the system. Now, thousands (or even more) of requests at the same time are sent to the system and the system cannot recognize the source of attack as there is each request from a different user, and all the users are authorized. So, the attacker is using the authorized users as victims too. The primary victim is the system, and the secondary victims are the authorized users. The authorized users are called Zombie PCs.

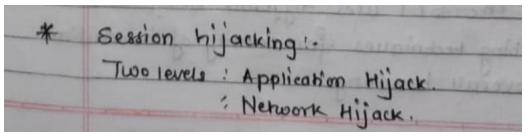
Web Browser Attack:



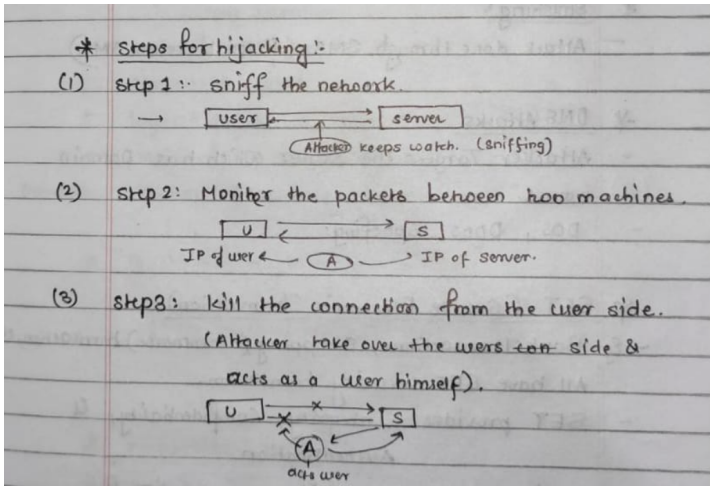
- Web browsers are susceptible to attack or exploitation, much like other software, if the proper security patches aren't installed.
- If the browser plug-ins are not fully patched, a fully patched web browser may still be open to attack or exploit. It's crucial to keep in mind that plug-ins may not always get updated when the browser does.
- Historically, malicious websites were the source of browser-based attacks. However, attackers have recently been successful in breaching a significant number of reliable websites in order to disseminate dangerous payloads to unwary users as a result of weak security coding in web apps or flaws in the software that supports websites.
- Hackers add scripts without altering the look of the website. These scripts could surreptitiously reroute your browser to another website without your knowledge.
- It's possible that your computer will download malicious software as a result of this redirect to another website. These programs are typically made to provide remote access to your computer by the attacker and to collect personal data, frequently in the form of credit card and banking information as well as other information that can be used to commit identity theft.

4. Define Session Hijacking with all hacking steps.

Ans)
Session hijacking is a type of attack where an attacker tries to take control of a legitimate user's session in order to gain unauthorized access to sensitive information or perform malicious activities. The attacker can intercept and manipulate the communication between the user and the server, and use this to take over the user's session.



Application hijacking, also known as app hijacking, is a type of cyber attack where an attacker gains unauthorized access to an application by exploiting vulnerabilities in the application or the underlying system. The attacker may use this access to steal sensitive data, modify or delete files, or execute malicious code on the compromised device.
Network Hijacking is a type of organizational hijacking that involves the unauthorized use of groups of IP addresses, known as ranges. Network hijacking includes IP hijacking or Route Hijacking.



In the above figure, it can be seen that the attacker captures the victim's session ID to gain access to the server by using some packet sniffers.

Session hijacking example: Aditya is sitting in a coffee shop sipping a latte and checking his bank balance. A hijacker at the next table uses "session sniffing", one of the techniques to grab the session cookie, take over the session, and access his bank account.

5. Define working steps of Digital Signature Standard.

Ans) Digital Signature is a way to validate the authenticity and integrity of the message or digital or electronic documents. Authenticity means to check whether the data is coming from a valid source or not to the receiver i.e. to verify the identity of the sender and integrity means to check that the data or message should not be altered during the transmission.

The working steps of DSS are as follows:

1. Generation of a global public key component
   - Find a prime number p such that 2^L-1 < p < 2^L, where L is an integer between 512 and 1024 i.e., 512 <= L <= 1024.
   - Find another number q which is a prime divisor of (p-1).
   - Compute g = h^(p-1)/q mod p, where h is an integer between 1 < h < p-1 and g should be greater than 1 or h^(p-1)/q mod p>1.

2. Finding the user's private and public keys
   - The private key, x is any random number such that 0 < x< q.
   - The public key, y = g^x mod p

3. Generating the Signature
   - Finding the components of signature s and r.
   - r = (gk mod p) mod q
   - s = [k^ -1 {H(M) + x*r}] mod q where k is an integer such that 0 < k <q.
   - Signature= (r, s)

4. Verifying the signature

Let M', r', and s' be the message and signature components respectively received corresponding to M, r, and s.
To verify whether the signature is valid or not, first, the following condition needs to be checked:
$0 < r' < q$ and $0 < s' < q$
If any of the above conditions are not met, the signature is considered invalid and is therefore discarded; otherwise, if both conditions are met, the following parameters are computed:
$v = [(g^{u1} y^{u2}) \bmod p] \bmod q$
$u1 = [H(M)w] \bmod q$
$u2 = (r') w \bmod q$
$w = (s')^{-1} \bmod q$
Test: $v = r'$
If $v = r'$, the signature is correct; otherwise, the data or message has been altered.

6. What is meant by the Multilevel Security Model in System Security.

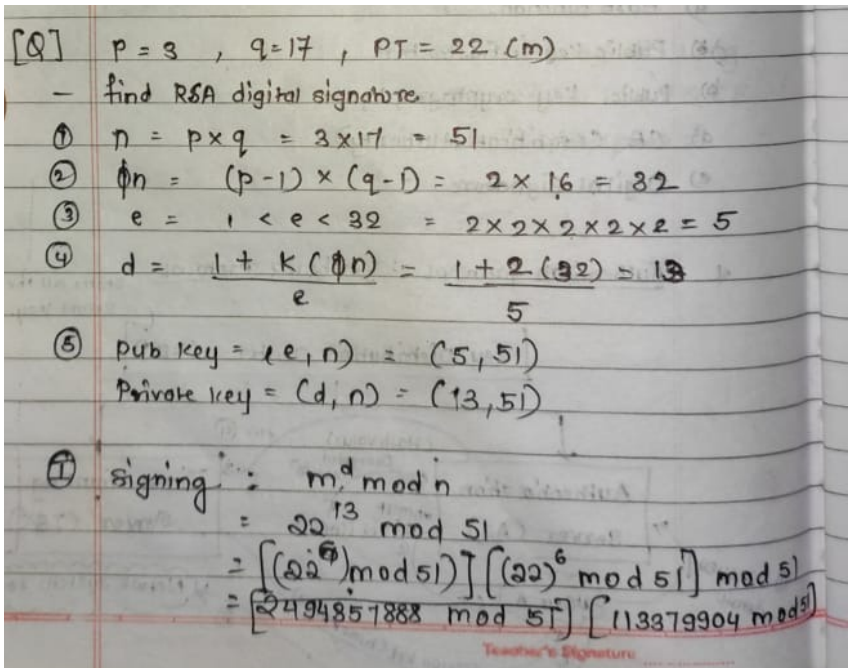
Ans) The Multilevel Security Model (MLS) is a security model that allows for the protection of sensitive information by controlling access to it based on the security clearance level of the user. It is commonly used in environments where multiple users with different levels of clearance need to access the same system, such as government or military organizations.
In the MLS model, information is classified into different levels, each of which is associated with a specific level of clearance. Access to information at a particular security level is granted only to users with an equal or higher level of clearance. This ensures that sensitive information is only accessible to authorized personnel.
To ensure the confidentiality, integrity, and availability of information, the MLS model employs various security mechanisms.
Authentication is used to verify the identity of users and ensure that only authorized users can access the system. Authorization controls are used to determine what actions a user is allowed to perform on the system, based on their security clearance level.
Encryption is used to protect data at rest and in transit, so that even if it is intercepted by an unauthorized party, it cannot be read.
The MLS model also uses techniques such as mandatory access control (MAC) and discretionary access control (DAC) to provide an additional layer of security. MAC is a security mechanism that enforces a strict set of rules regarding which users can access specific resources, based on their security clearance level. DAC, on the other hand, allows users to determine who can access resources they own, and to what extent.

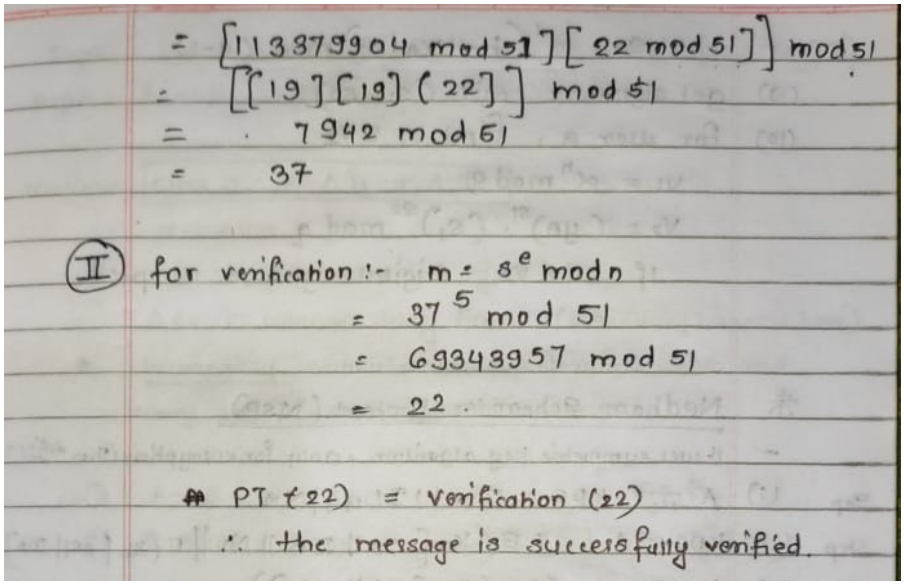
7. What are the steps of RSA Digital Signature?

Ans)

- Select two large prime numbers, p and q.
- Multiply these numbers to find $n = p \times q$, where n is called the modulus for encryption and decryption.
- $\varphi(n) = (p - 1) \times (q - 1)$

- Choose a number e less than n, such that n is relatively prime to φ (n). It means that e and have no common factor except 1. Choose "e" such that 1<e < φ (n), e is prime to φ (n), gcd (e,d(n)) =1
- Public key is <e, n>.
  Private key is <d, n>
- Signing: $s = m^d \bmod n$
- Verification : $m = s^e \bmod n$

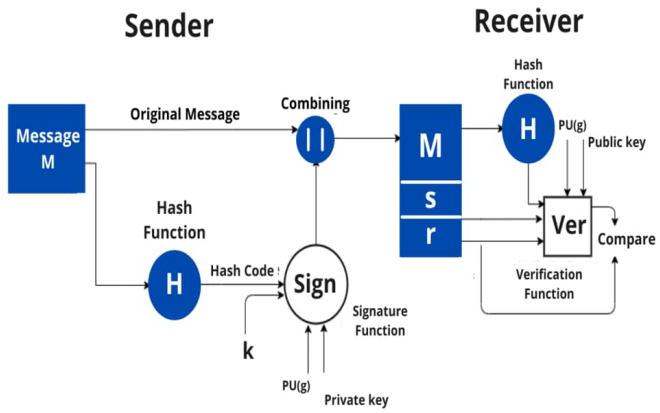




8. Define what is meant by Digital Signature with its process.

Ans)

Digital Signature is a way to validate the authenticity and integrity of the message or digital or electronic documents. Authenticity means to check whether the data is coming from a valid source or not to the receiver i.e. to verify the identity of the sender and integrity means to check that the data or message should not be altered during the transmission.



A hash code is generated from the message and given as input to the signature function on the sender side. The other inputs to a signature function include a unique random number k for the signature, the private key of sender PR(a), and the global public key i.e., PU(g).

The output of the signature function consists of two components: s & r, which are concatenated with the input message and then sent to the receiver.

Signature = {s, r}.

On the receiver side, the hash code for the message sent is generated by the receiver by applying a hash function. The verification function is used for verifying the message and signature sent by the sender. The verification function takes the hash code generated, signature components s and r, the public key of the sender (PU(a)), and the global public key.

The signature function is compared with the output of the verification function and if both the values match, the signature is valid because A valid signature can only be generated by the sender using its private key.

steps involved in DSS in Cryptography are,

- Generation of keys i.e., public and private keys for the source.
- Creation of digital signature by the source for a message.
- The receiver verifies the digital signature.

9. What is meant by CrossSite Request Forgery.

Ans)

- Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated.
- With a little help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing.
- If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth. If the victim is an administrative account, CSRF can compromise the entire web application.

For most sites, browser requests automatically include any credentials associated with the site, such as the user's session cookie, IP address, Windows domain credentials, and so forth. Therefore, if the user is currently authenticated to the site, the site will have no way to distinguish between the forged request sent by the victim and a legitimate request sent by the victim.

☞ **Preventing CSRF Vulnerabilities**

- Security experts propose many CSRF prevention mechanisms. This includes, for example, using a referer header, using the HttpOnly flag, sending an X-Requested-With custom header using jQuery, and more.

10. Define Firewall and its types.

Ans)

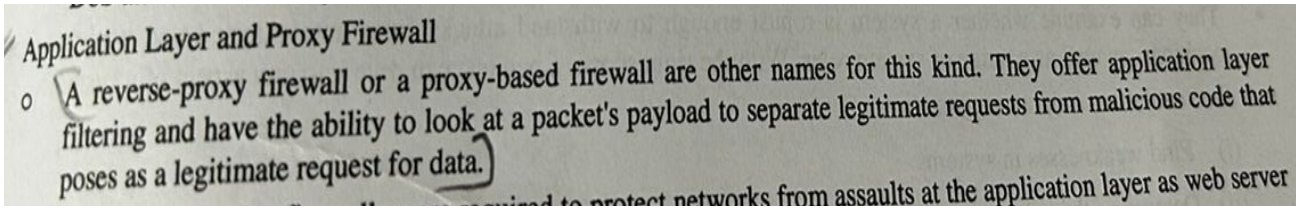
⏭ 6.19 FIREWALLS

- A firewall is a piece of software or firmware that guards against unauthorized network access. To find and stop threats, it examines incoming and outgoing communications using a set of criteria.
- Firewalls are utilized in both home and business environments, and many devices, including Mac, Windows, and Linux PCs, already have one built in. They are frequently regarded as a crucial element of network security.

Types of Firewalls

- Packet Filtering Firewall
  - A packet-filtering firewall verifies a packet's source and destination addresses, protocol, and destination port number as it passes through. If a packet does not adhere to the firewall's rule set, it is dropped, which prevents it from being routed to its intended location.
  - For instance, if a firewall is set up with a rule that prevents Telnet access, the firewall will reject packets that are headed for TCP port 23, which is where a Telnet server

- Stateful inspection firewalls
  - Stateful inspection firewalls have mostly superseded packet-filtering firewalls since they process each packet individually and can be subject to IP spoofing attacks.
  - Stateful inspection firewalls, sometimes referred to as dynamic packet-filtering firewalls, continuously track and analyse communication packets, both incoming and outgoing.
  - This type keeps a database that lists all active connections. It detects whether incoming packets are a part of an


Application Layer and Proxy Firewall

- A reverse-proxy firewall or a proxy-based firewall are other names for this kind. They offer application layer filtering and have the ability to look at a packet's payload to separate legitimate requests from malicious code that poses as a legitimate request for data.

protect networks from assaults at the application layer as web server

12. What is Inference Attacks in System Security.

Ans)

Inference attacks are a type of attack in system security that involves extracting sensitive information from a system by analyzing the patterns in non-sensitive data. A real-world example of an inference attack is as follows:

Let's say that a healthcare organization has a database of patient records that includes their medical histories, diagnoses, and treatments. The database is encrypted to ensure the confidentiality of the data. However, the organization also provides researchers with access to some non-sensitive data, such as demographic information, without encryption.

An attacker who gains access to this non-sensitive data could use statistical analysis techniques to infer sensitive information about individual patients. For example, they could use clustering algorithms to group patients based on their age, gender, and zip code. By analyzing the medical histories of the patients in each cluster, the attacker could infer information about the prevalence of certain diseases in each group. This could reveal sensitive information about individual patients, such as their medical conditions, without directly accessing the encrypted data.

In this example, the attacker is able to use non-sensitive data to infer sensitive information about the patients, highlighting the need for organizations to carefully manage and protect all data, even if it is not directly sensitive.

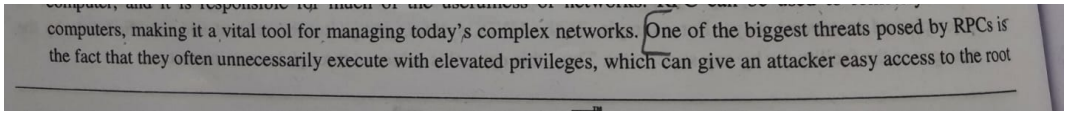
To protect against inference attacks, there are several ways to ensure that sensitive information is not inadvertently disclosed:

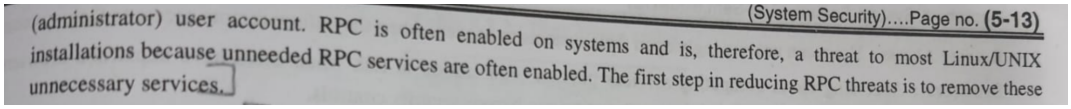
1. Data anonymization: The organization can remove or encrypt all identifying information from the non-sensitive data, such as names, addresses, or social security numbers. This can prevent attackers from being able to link non-sensitive data to sensitive data.
2. Differential privacy: This technique involves adding noise or random data to the non-sensitive data before releasing it to researchers. This makes it more difficult for attackers to identify individual records.
3. Access control: Limiting access to the non-sensitive data can prevent unauthorized users from being able to use it to infer sensitive information.
4. Data segmentation: The organization can segment the data into different subsets, with different access levels based on the sensitivity of the data. This can limit the amount of non-sensitive data that is accessible to any individual user.
5. Regular monitoring: The organization can regularly monitor access to the non-sensitive data, and analyze patterns of access to identify any potential inference attacks.

13. How Multilevel Database Security will work in Web Security. Illustrate with Diagram and examples.
Ans)

14. Illustrate Vulnerability in Linux and Windows Operating systems. Also Explain File System Security with examples.
Ans) Vulnerability in linux are as follows:

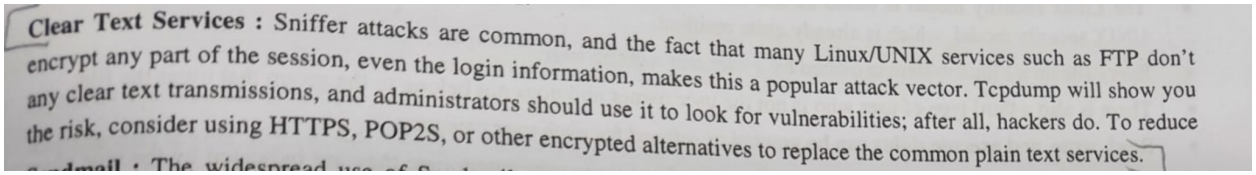
1. Remote Procedure Call:


computers, making it a vital tool for managing today's complex networks. One of the biggest threats posed by RPCs is the fact that they often unnecessarily execute with elevated privileges, which can give an attacker easy access to the root

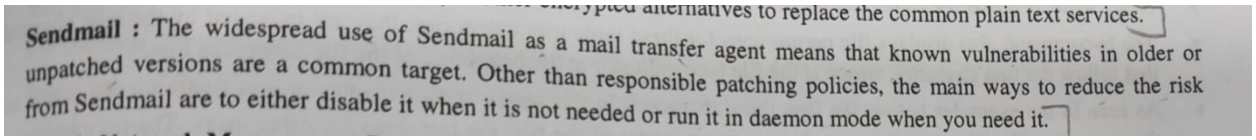


(administrator) user account. RPC is often enabled on systems and is, therefore, a threat to most Linux/UNIX installations because unneeded RPC services are often enabled. The first step in reducing RPC threats is to remove these unnecessary services.

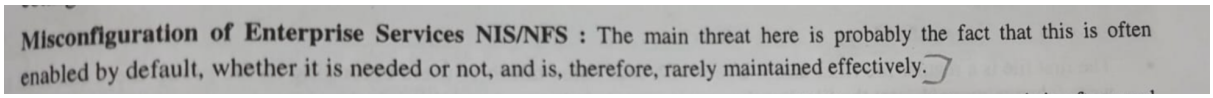
2. Clear Text Services:


Clear Text Services : Sniffer attacks are common, and the fact that many Linux/UNIX services such as FTP don't encrypt any part of the session, even the login information, makes this a popular attack vector. Tcpdump will show you any clear text transmissions, and administrators should use it to look for vulnerabilities; after all, hackers do. To reduce the risk, consider using HTTPS, POP2S, or other encrypted alternatives to replace the common plain text services.

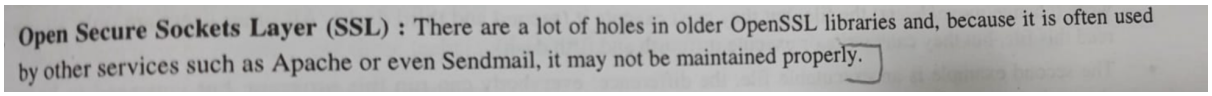
3. Sendmail:

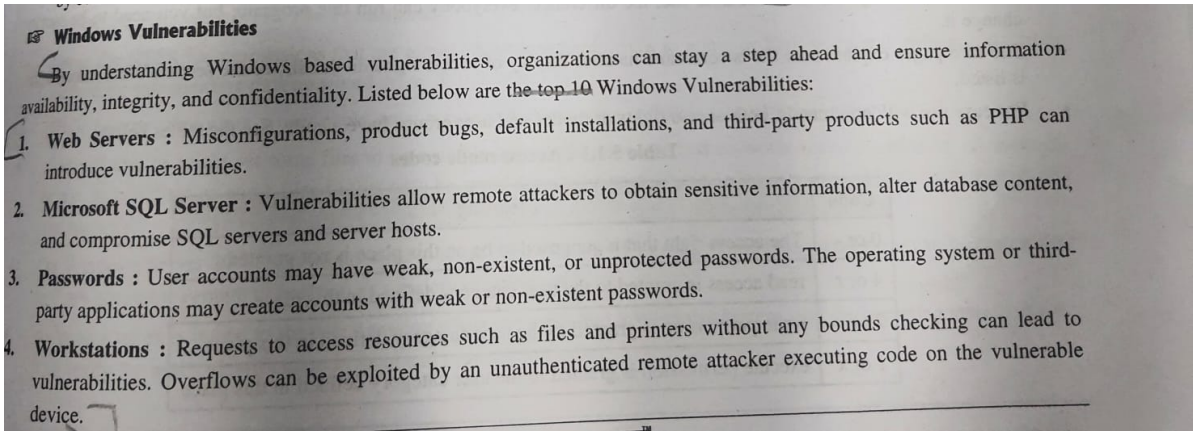

Sendmail : The widespread use of Sendmail as a mail transfer agent means that known vulnerabilities in older or unpatched versions are a common target. Other than responsible patching policies, the main ways to reduce the risk from Sendmail are to either disable it when it is not needed or run it in daemon mode when you need it.

4. Misconfiguration of Enterprise Services NIS/NFS:


Misconfiguration of Enterprise Services NIS/NFS : The main threat here is probably the fact that this is often enabled by default, whether it is needed or not, and is, therefore, rarely maintained effectively.

5. Open Secure Sockets Layer (SSL):


Open Secure Sockets Layer (SSL) : There are a lot of holes in older OpenSSL libraries and, because it is often used by other services such as Apache or even Sendmail, it may not be maintained properly.


☞ **Windows Vulnerabilities**

By understanding Windows based vulnerabilities, organizations can stay a step ahead and ensure information availability, integrity, and confidentiality. Listed below are the top 10 Windows Vulnerabilities:

1. **Web Servers :** Misconfigurations, product bugs, default installations, and third-party products such as PHP can introduce vulnerabilities.
2. **Microsoft SQL Server :** Vulnerabilities allow remote attackers to obtain sensitive information, alter database content, and compromise SQL servers and server hosts.
3. **Passwords :** User accounts may have weak, non-existent, or unprotected passwords. The operating system or third-party applications may create accounts with weak or non-existent passwords.
4. **Workstations :** Requests to access resources such as files and printers without any bounds checking can lead to vulnerabilities. Overflows can be exploited by an unauthenticated remote attacker executing code on the vulnerable device.

8. **E-mail :** By opening a message a recipient can activate security threats such as viruses, spyware, Trojan horse programs, and worms.

Linux File System Security

Access rights : Linux's first line of defense

- The Linux security model is based on the one used on UNIX systems and is as strict (and sometimes more) than the UNIX security model, which is already quite resilient.
- Every file on a Linux system is owned by a user and a group user.
- There is also a third type of user who is not the user owner and does not belong to the group that owns the file.
- Read, write, and execute rights can be granted or refused for each user category.
- The ls-command also displays file permissions for these three user categories; they are indicated by the nine characters

- As seen in the examples below, the first three characters in this series of nine display access rights for the actual user that owns the file. The next three are for the group owner of the file, the last three for other users. The permissions are always in the same order: read, write, execute for the user, the group and the others. Some examples:

```
nilesh:~>ls -l To_Do
-rw-rw-r--   1 nilesh  users     5 Jan 15 12:39 To_Do
nilesh:~>ls -l /bin/ls
-rwxr-xr-x   1 root    root   45948 Aug  9 15:01 /bin/ls*
```

- The first file is a regular file (first dash). Users with user name nilesh or users belonging to the group users can read and write (change/move/delete) the file, but they can't execute it (second and third dash). All other users are only allowed to read this file, but they can't write or execute it (fourth and fifth dash).

Windows File System Security

- Anytime data is kept on a physical medium, it could end up being hacked.
- For instance, compromised confidential notes between Napoleon and his generals contributed to his loss.
- Secret letters from Napoleon were written on paper or leather and sent by swift riders.
- Those confidential notes are kept in a computing environment on a hard drive and are either utilized locally or sent over a network to a friend, co-worker, website, or other destination outside of your server or organization.
- Long-term computer data storage provides several advantages, but it also creates a specific security concern for the system administrator: how do you safeguard data such that only the intended user has access while yet assuring some

- Using the NTFS file permissions that are already built into hard drives to allow or limit users and groups is the basic method for safeguarding data on a hard drive.
- While barring other users, a user could grant access to his user account for his own personal research data.
- Additionally, he might set some files to be writable by only his manager and co-workers and readable by all users. At home, he could set up some files so that only he could access the contents while leaving other folders open to both him and his wife.
- On Windows Server 2003, you might want to share files with the HR group alone. File permissions can be customized and are adaptable enough to function in a variety of situations.

15. The message" The meeting is Delayed "is to be Securely communicated to the receiver. apply the knowledge of SSH and show the steps to communicating this message.

Ans) To securely communicate the message "The meeting is delayed" using SSH, you can follow these steps:

1. Open a terminal on your local computer and type the following command:

ssh user@remotehost
Replace "user" with the username on the remote host and "remotehost" with the hostname or IP address of the remote host.

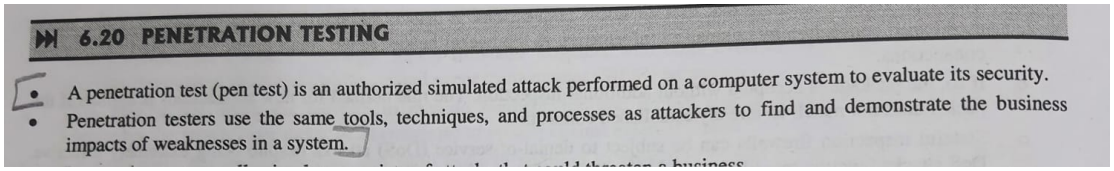
1. Enter your password when prompted. This will establish a secure SSH connection to the remote host.
2. Type the following command to send the message:

echo "The meeting is delayed" | ssh user@remotehost 'cat > message.txt'
This will send the message "The meeting is delayed" to the remote host and save it to a file named "message.txt".

1. Close the SSH connection by typing:

exit
This will close the SSH connection and return you to your local terminal.
By using SSH, the message is encrypted and transmitted securely over the network, preventing unauthorized access or interception of the message.

16. Explain how data is protected during and after Penetration Testing. Illustrate its Phases and Methods.
Ans)


6.20 PENETRATION TESTING

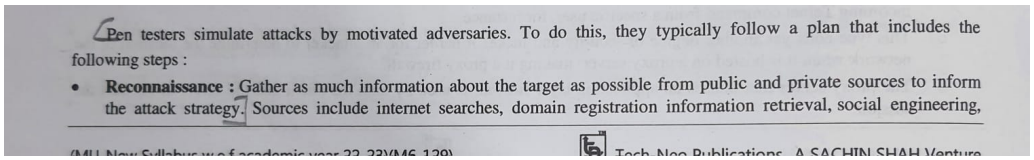
- A penetration test (pen test) is an authorized simulated attack performed on a computer system to evaluate its security.
- Penetration testers use the same tools, techniques, and processes as attackers to find and demonstrate the business impacts of weaknesses in a system.

To protect the data during and after penetration testing, various measures can be taken.
During Penetration Testing:

1. Non-Disclosure Agreements (NDAs): An NDA can be signed between the penetration testing team and the organization to ensure that all sensitive information and data found during testing remains confidential.
2. Scope Limitation: The scope of the testing can be limited to certain systems, networks, or applications to ensure that only authorized areas are being tested and that sensitive data is not exposed.
3. Use of Test Data: The penetration testing team can use test data that is representative of the actual data to ensure that real data is not exposed or modified during the testing process.
4. Data Encryption: Data encryption can be used during testing to ensure that sensitive data remains protected while it is being used by the penetration testing team.

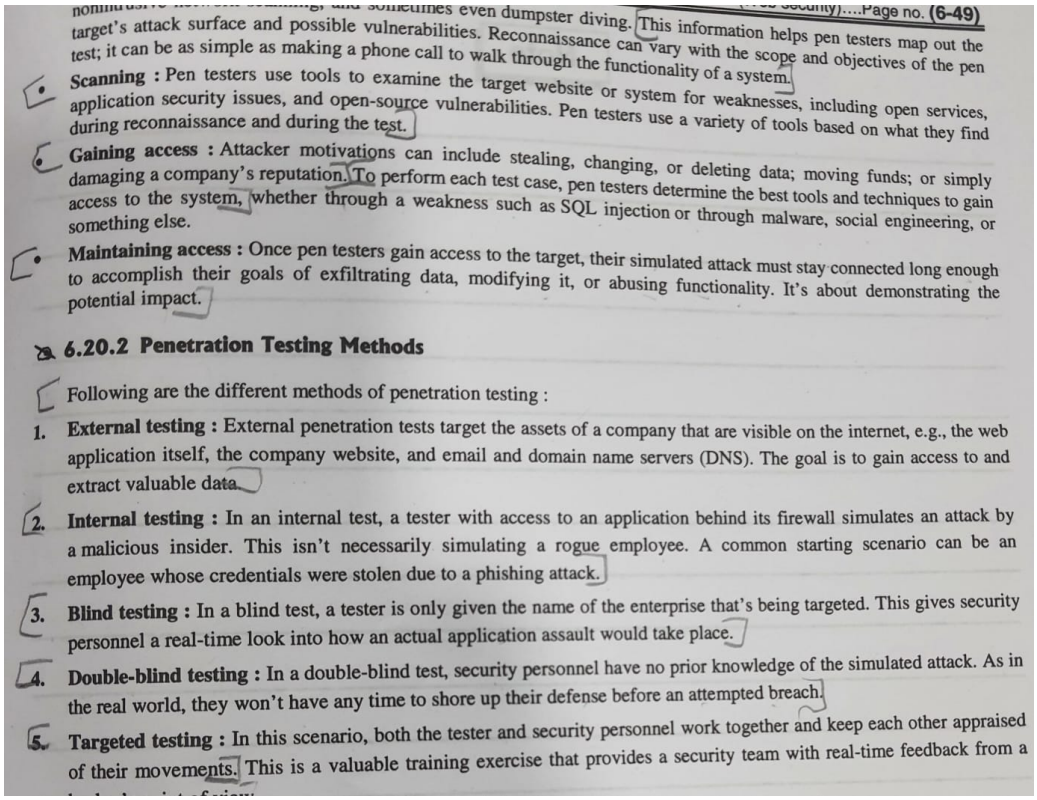
After Penetration Testing:

1. Data Deletion: All data used during testing should be securely deleted and removed from the testing environment to ensure that it is not accessible to unauthorized users.
2. Reporting and Remediation: The penetration testing team should provide a report that includes all vulnerabilities found during testing and recommendations for remediation. The organization should then take steps to address the identified vulnerabilities.



Pen testers simulate attacks by motivated adversaries. To do this, they typically follow a plan that includes the following steps :

- **Reconnaissance :** Gather as much information about the target as possible from public and private sources to inform the attack strategy. Sources include internet searches, domain registration information retrieval, social engineering,



target's attack surface and possible vulnerabilities. Reconnaissance can vary with the scope and objectives of the pen test; it can be as simple as making a phone call to walk through the functionality of a system.

- **Scanning :** Pen testers use tools to examine the target website or system for weaknesses, including open services, application security issues, and open-source vulnerabilities. Pen testers use a variety of tools based on what they find during reconnaissance and during the test.
- **Gaining access :** Attacker motivations can include stealing, changing, or deleting data; moving funds; or simply damaging a company's reputation. To perform each test case, pen testers determine the best tools and techniques to gain access to the system, whether through a weakness such as SQL injection or through malware, social engineering, or something else.
- **Maintaining access :** Once pen testers gain access to the target, their simulated attack must stay connected long enough to accomplish their goals of exfiltrating data, modifying it, or abusing functionality. It's about demonstrating the potential impact.

6.20.2 Penetration Testing Methods

Following are the different methods of penetration testing :

1. **External testing :** External penetration tests target the assets of a company that are visible on the internet, e.g., the web application itself, the company website, and email and domain name servers (DNS). The goal is to gain access to and extract valuable data.
2. **Internal testing :** In an internal test, a tester with access to an application behind its firewall simulates an attack by a malicious insider. This isn't necessarily simulating a rogue employee. A common starting scenario can be an employee whose credentials were stolen due to a phishing attack.
3. **Blind testing :** In a blind test, a tester is only given the name of the enterprise that's being targeted. This gives security personnel a real-time look into how an actual application assault would take place.
4. **Double-blind testing :** In a double-blind test, security personnel have no prior knowledge of the simulated attack. As in the real world, they won't have any time to shore up their defense before an attempted breach.
5. **Targeted testing :** In this scenario, both the tester and security personnel work together and keep each other appraised of their movements. This is a valuable training exercise that provides a security team with real-time feedback from a

17. How memory and address protection is implemented in system security. Illustrate with an example.
Ans)

18. How file protection mechanism works in software security. Illustrate with an example.
Ans)
File protection mechanism is an essential aspect of software security that aims to ensure the confidentiality, integrity, and availability of sensitive data stored in files. The file protection mechanism uses various techniques to prevent unauthorized access, modification, and deletion

of files by attackers or malicious users. Here's an example of how file protection mechanism works in software security.

Let's consider a scenario where a company has developed an application for storing and managing customer data, including personal and financial information. To protect this sensitive data, the application uses a file protection mechanism that includes the following measures:

1. Access Control: The file protection mechanism restricts access to the customer data files to authorized users only. Access control can be implemented using various techniques, such as password authentication, biometric authentication, or role-based access control. For instance, the application can require users to enter a valid username and password before allowing access to the customer data files.
2. Encryption: The file protection mechanism uses encryption to protect the customer data files from unauthorized access and interception during transmission. Encryption can be implemented using various algorithms, such as AES, RSA, or DES. For example, the application can encrypt the customer data files using AES-256 encryption before transmitting them over the internet.
3. Backup and Recovery: The file protection mechanism ensures that customer data files are backed up regularly and can be recovered in case of data loss or corruption. Backup and recovery can be implemented using various techniques, such as cloud backup, tape backup, or disk imaging. For instance, the application can store the customer data files in a secure cloud-based backup system that allows quick and easy recovery in case of a disaster.
4. File Integrity Checking: The file protection mechanism uses file integrity checking to detect any unauthorized changes to the customer data files. File integrity checking can be implemented using various techniques, such as checksums, digital signatures, or file permissions. For example, the application can use digital signatures to verify the authenticity and integrity of the customer data files before allowing access to them.

In summary, the file protection mechanism is a critical component of software security that aims to protect sensitive data stored in files. It uses various measures such as access control, encryption, backup and recovery, and file integrity checking to ensure the confidentiality, integrity, and availability of data. By implementing a robust file protection mechanism, companies can safeguard their customer data from unauthorized access, modification, and deletion, and protect their reputation and credibility.

19. The message" The meeting is canceled "is to be Securely communicated to the receiver.apply the knowledge of SSL and show the steps for communicating this message.

Ans) To securely communicate the message "The meeting is canceled" to the receiver, we can use the SSL (Secure Sockets Layer) protocol. Here are the steps to communicate the message securely using SSL:

1. The sender initiates a connection request to the receiver's server using the SSL protocol. The sender's computer sends a "Client Hello" message to the receiver's server, indicating that it wants to establish a secure connection.
2. The receiver's server responds with a "Server Hello" message, which includes information about the SSL version, cipher suite, and other details required for establishing a secure connection.
3. The sender and receiver computers then engage in a "handshake" process, during which they negotiate the parameters of the SSL connection, including the encryption algorithm to be used and the keys for encrypting and decrypting messages.
4. Once the handshake process is complete, the sender's computer can send the message "The meeting is canceled" to the receiver's server over the secure SSL connection.
5. The receiver's server receives the message and decrypts it using the shared encryption key negotiated during the handshake process.
6. If the message is intended for a specific recipient, the receiver's server can use access control mechanisms such as user authentication to ensure that only authorized users can read the message.
7. Finally, the receiver's server sends an acknowledgment message back to the sender's computer over the SSL connection, confirming that the message has been received and securely decrypted.

Overall, the SSL protocol provides a secure and reliable method for transmitting sensitive information such as the message "The meeting is canceled" over the internet, protecting it from interception or tampering by unauthorized parties.

20. How Email Attacks can be done by an attacker in Web Security. Illustrate its types with examples.

Ans) Many people rely on the Internet for many of their professional, social and personal activities. But there are also people who attempt to damage our Internet-connected computers, violate our privacy and render inoperable Internet services. Email is a universal service used by over a billion people worldwide. As one of the most popular services, email has become a major vulnerability to users and organizations. Below are some of the most common types of Attacks:

- Phishing: Phishing is a form of fraud. Cyber criminals use email, instant messaging, or other social media to try to gather information such as login credentials by masquerading as a reputable person. Phishing occurs when a malicious party sends a fraudulent email disguised as being from an authorized, trusted source. The message’s intent is to trick the recipient into installing malware on his or her device or into sharing personal or financial information.
- Vishing: Vishing is phishing using voice communication technology. Criminals can spoof calls from authorized sources using voice-over IP technology. Victims may also receive a recorded message that appears authorized. Criminals want to obtain credit card numbers or other information to steal the victim’s identity. Vishing takes advantage of the fact that people trust the telephone network.

- Pharming: Pharming is the impersonation of an authorized website in an effort to deceive users into entering their credentials. Pharming misdirects users to a fake website that appears to be official. Victims then enter their personal information thinking that they are connected to a legitimate site.
- Adware: Adware typically displays annoying pop-ups to generate revenue for its authors. The malware may analyze user interests by tracking the websites visited. It can then send pop-up advertising relevant to those sites. Some versions of software automatically install Adware.
- Spam: Spam (also known as junk mail) is unsolicited email. In most cases, spam is a method of advertising. However, spam can send harmful links, malware, or deceptive content. The end goal is to obtain sensitive information such as a social security number or bank account information. Most spam comes from multiple computers on networks infected by a virus or worm. These compromised computers send out as much bulk email as possible.

There are many other type of email attacks like Smishing,Whaling,Spyware,Scareware,etc.