Information Security and Cyber Laws PYQ 2020

Q1. What are the security issues of Windows XP operating system? Suppose IT chief security officer of an organization purchase a highly secure system "Alarm Logic" to meet their security needs. This system works as a gateway to the Organization from outside network by sending alert to the security portal of that organization. What type of system is "Alarm Logic"? Describe the functioning of this "Alarm logic" security system.

Ans1. Windows XP, which was released by Microsoft in 2001, is an outdated operating system that is no longer supported by Microsoft. As a result, it is vulnerable to several security issues, including:

Lack of security updates: Since Windows XP is no longer supported by Microsoft, it does not receive regular security updates, leaving the system exposed to known vulnerabilities and exploits that can be exploited by hackers.

Malware and viruses: Windows XP does not have the latest security features and defenses against malware and viruses, making it more susceptible to attacks from malicious software.

Weak authentication and encryption: Windows XP uses outdated authentication and encryption protocols, which can be easily exploited by attackers to gain unauthorized access to the system or intercept sensitive data.

Hardware and software compatibility issues: Many modern hardware and software applications are not compatible with Windows XP, which can result in security vulnerabilities due to lack of updates and patches.

Social engineering attacks: Windows XP does not have advanced security features to protect against social engineering attacks, which involve manipulating users into revealing sensitive information or performing actions that can compromise the security of the system.

In order to meet their security needs, the IT chief security officer of the organization has purchased a security system called "Alarm Logic". Based on the given information, "Alarm Logic" appears to be a security gateway system that acts as a protective barrier between the organization's internal network and the external network. It monitors incoming and outgoing traffic to detect and alert the organization about potential security threats.

The functioning of the "Alarm Logic" security system likely involves the following steps:

Gateway functionality: "Alarm Logic" acts as a gateway, filtering and analyzing incoming and outgoing network traffic to identify potential security threats, such as malware, viruses, or suspicious activities.

Alert generation: When a security threat is detected, "Alarm Logic" generates alerts in real-time and sends them to the organization's security portal, providing information about the nature of the threat, its severity, and the affected systems.

Centralized monitoring and management: The organization's security portal is likely a centralized management console where security administrators can monitor and manage security alerts generated by "Alarm Logic". This allows for quick response and mitigation of security threats.

Customizable rules and policies: "Alarm Logic" may allow the organization to define customizable rules and policies based on their specific security requirements, such as blocking certain types of traffic, enforcing encryption protocols, or restricting access to certain websites or applications.

Integration with other security tools: "Alarm Logic" may be integrated with other security tools, such as firewalls, intrusion detection systems, or antivirus software, to provide a layered security approach and enhance the overall security posture of the organization.

Regular updates and maintenance: "Alarm Logic" may require regular updates and maintenance to ensure that it remains effective in detecting and mitigating new and emerging security threats.

In summary, "Alarm Logic" is likely a security gateway system that provides real-time monitoring, alert generation, and centralized management of security threats to help organizations protect their internal network from external security risks. It works by analyzing incoming and outgoing network traffic, generating alerts, and allowing for customizable rules and policies to enhance the security posture of the organization.

Q2. Describe various stages and tools of Hacking . Distinguish between Hacking and Phishing. Suppose, you have created a website. Some vulnerabilities are reported by exposing and exploiting that website in order to discover its weaknesses. What types of vulnerabilities can be there? List them and explain various ways to fix these vulnerabilities in order to make the website more secure?

Ans2. Hacking is the act of gaining unauthorized access to a computer system or network, typically for malicious purposes. It involves various stages and tools, which can vary depending on the specific type of attack and the skill level of the attacker. Some common stages and tools of hacking include:

Reconnaissance: This stage involves gathering information about the target system or network, such as identifying potential vulnerabilities, finding open ports, or determining the operating system and software versions in use. Tools used in this stage may include port scanners, network scanners, and information gathering techniques like social engineering.

Exploitation: Once vulnerabilities are identified, the attacker may use various tools to exploit them and gain unauthorized access to the target system or network. This can involve using exploits, malware, or other techniques to bypass security controls and gain privileged access.

Privilege escalation: After gaining initial access, the attacker may attempt to escalate their privileges to gain higher levels of access within the system or network. This can involve gaining administrative privileges, root access, or other elevated privileges to gain more control over the target system.

Maintaining access: Once access is obtained, the attacker may use tools and techniques to maintain their access and establish persistence within the system or network. This can involve installing backdoors, creating hidden user accounts, or setting up remote access points for future exploitation.

Covering tracks: After compromising a system or network, the attacker may attempt to cover their tracks to avoid detection. This can involve deleting logs, modifying system files, or using other techniques to hide their presence and activities.

Phishing, on the other hand, is a type of social engineering attack where an attacker tricks individuals into revealing sensitive information, such as usernames, passwords, or credit card details, by posing as a legitimate entity. Phishing attacks typically involve sending deceptive emails, messages, or other communications that appear genuine to trick individuals into divulging their information.

Now, regarding the vulnerabilities that can be present in a website, there are several types, including:

Injection vulnerabilities: These occur when an attacker can inject malicious code, such as SQL or JavaScript, into a website's input fields or parameters, potentially allowing them to manipulate or extract data from the website's database.

Cross-Site Scripting (XSS) vulnerabilities: These vulnerabilities allow attackers to inject malicious scripts into a website, which can then be executed by other users' browsers, potentially allowing the attacker to steal sensitive information or perform other malicious actions.

Cross-Site Request Forgery (CSRF) vulnerabilities: These vulnerabilities allow an attacker to trick authenticated users into unknowingly executing malicious actions on a website by exploiting their authenticated session.

Broken authentication and session management: These vulnerabilities can occur when a website does not properly manage user authentication and session management, allowing attackers to gain unauthorized access to user accounts.

Security misconfigurations: These vulnerabilities occur when a website is not properly configured, leading to weak access controls, default or weak passwords, or other security weaknesses that can be exploited by attackers.

To make a website more secure and fix these vulnerabilities, some steps that can be taken include:

Regularly updating and patching the website's software and plugins to ensure they are up to date and free of known vulnerabilities.

Implementing proper input validation and sanitization techniques to prevent injection attacks and other forms of code injection.

Implementing secure coding practices, such as using secure coding frameworks and libraries, avoiding the use of default or weak passwords, and following the principle of least privilege, which restricts users' access to only what is necessary for their job duties.

Implementing proper authentication and session management mechanisms, such as using strong encryption, multi-factor authentication, and expiring sessions after a certain period of inactivity.

Implementing proper access controls to restrict user privileges and permissions, ensuring that users only have access to the resources and functionality they need to perform their tasks.

Regularly monitoring and auditing the website for any signs of suspicious activity, such as unusual login attempts, unauthorized access, or changes to critical files or configurations.

Conducting regular security assessments, such as penetration testing or vulnerability scanning, to identify and address potential vulnerabilities proactively.

Educating users about safe browsing practices, including not clicking on suspicious links or downloading unknown files, and being cautious about sharing personal information online.

Having a robust incident response plan in place to respond quickly and effectively to any security incidents that may occur, including isolating affected systems, preserving evidence, and notifying appropriate parties.

It is important to note that cybersecurity is an ongoing process, and it requires constant vigilance and proactive measures to protect a website and its users from potential threats. Regular monitoring, updates, and audits should be performed to ensure the website remains secure and vulnerabilities are promptly addressed.

In conclusion, securing a website requires a multi-layered approach, including addressing vulnerabilities, implementing secure coding practices, proper authentication and access controls, regular monitoring, and user education. By taking these steps, the website can be better protected against potential attacks and ensure the privacy and security of its users' information.

Q3. Differentiate between false positive and false negative biometric authentication? Why biometrics are more secure than password? What are the frauds which are possible in biometric authentication? Describe in your own words.

Ans3. False positive and false negative are two terms used in biometric authentication to describe errors that can occur in the identification or verification process.

False positive refers to a situation where the biometric system incorrectly identifies an unauthorized person as an authorized user. In other words, the system wrongly accepts an impostor as a genuine user.

False negative, on the other hand, occurs when the biometric system fails to recognize a legitimate user, and thus denies access to an authorized person.

Biometrics are generally considered more secure than passwords due to their inherent characteristics. Here are some reasons why biometrics are considered more secure:

Unique and Inherent: Biometric traits, such as fingerprints, iris patterns, or facial features, are unique to each individual and are inherently possessed by them. Unlike passwords, which can be forgotten, lost, or stolen, biometric traits are part of a person's physical or behavioral characteristics, making them difficult to duplicate or forge.

Difficult to Replicate: Biometric traits are difficult to replicate or spoof, as they are complex and require specialized equipment and knowledge. For example, creating a fake fingerprint or iris pattern that can bypass a biometric system is extremely challenging and unlikely to succeed.

Non-transferable: Unlike passwords, which can be shared or transferred, biometric traits cannot be easily shared or transferred from one person to another. This makes biometric authentication more reliable in ensuring that the person authenticating is the legitimate user.

However, like any technology, biometric authentication also has its limitations and potential frauds, which include:

False Acceptance: False acceptance occurs when the biometric system incorrectly identifies an unauthorized person as an authorized user, leading to unauthorized access. This can happen due to variations in biometric traits caused by factors such as changes in physical appearance, environmental conditions, or sensor inaccuracies.

False Rejection: False rejection occurs when the biometric system fails to recognize a legitimate user, denying them access. Factors such as changes in biometric traits due to injuries, aging, or variations in the capture conditions can lead to false rejections.

Biometric Data Breach: Biometric data, being unique and sensitive, can be targeted by hackers or malicious actors. If biometric data is compromised, it can lead to identity theft or unauthorized access to systems or accounts.

Replay Attacks: Replay attacks involve capturing and replaying previously captured biometric data to gain unauthorized access. This can be done through techniques such as spoofing or mimicking the biometric trait.

In conclusion, biometric authentication is generally considered more secure than passwords due to their unique and inherent nature. However, it is not foolproof and has its limitations and potential frauds, such as false acceptance, false rejection, biometric data breaches, and replay attacks. Appropriate safeguards, such as using robust biometric systems, implementing multi-factor authentication, and regular monitoring, should be in place to mitigate these risks and ensure the security of biometric authentication systems.

Q4. Differentiate between the following techniques with suitable examples of each.

(a) Symmetric and Asymmetric encryption

(b) Substitution and Transposition cipher

Ans4. (a) Symmetric and Asymmetric encryption:

Symmetric encryption and asymmetric encryption are two different techniques used in cryptography to secure data. Here are the key differences between them:

Symmetric Encryption: In symmetric encryption, the same key is used for both encryption and decryption. The sender and the receiver use the same secret key to encrypt and decrypt the data. It is also known as secret-key cryptography or private-key cryptography. Examples of symmetric encryption algorithms include AES (Advanced Encryption Standard), DES (Data Encryption Standard), and 3DES (Triple DES).

Example: Alice wants to send an encrypted message to Bob. She uses a secret key that she shares with Bob to encrypt the message. Bob then uses the same secret key to decrypt the message and read its contents.

Asymmetric Encryption: In asymmetric encryption, also known as public-key cryptography, a pair of keys is used: a public key and a private key. The public key is used for encryption, while the private key is used for decryption. The public key can be freely shared with anyone, while the private key must be kept secret. Examples of asymmetric encryption algorithms include RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography), and DSA (Digital Signature Algorithm).

Example: Alice wants to send an encrypted message to Bob. She uses Bob's public key to encrypt the message. Only Bob, who possesses the corresponding private key, can decrypt the message and read its contents.

(b) Substitution and Transposition cipher:

Substitution cipher and transposition cipher are two different types of cryptographic techniques used to encrypt messages. Here are the key differences between them:

Substitution Cipher: In a substitution cipher, each letter or character in the plaintext is replaced with another letter or character according to a predetermined substitution rule. The most common example of a substitution cipher is the Caesar cipher, where each letter in the plaintext is shifted by a fixed number of positions in the alphabet.

Example: If the substitution rule is to replace each letter with the letter that comes three positions later in the alphabet, then the letter 'A' would be replaced with 'D', 'B' with 'E', 'C' with 'F', and so on.

Transposition Cipher: In a transposition cipher, the letters or characters in the plaintext are rearranged without changing their actual values. The order of the letters or characters is changed according to a specific rule or key, but their values remain the same. An example of a transposition cipher is the Rail Fence cipher, where the plaintext is written in a zigzag pattern across multiple lines and then read off row by row to get the ciphertext.

Example: If the transposition rule is to write the plaintext "HELLO WORLD" in a zigzag pattern across three lines as follows:

mathematical

Copy code

H . . O . . L . . R . .

. E . L . O . W . L . D

. . L . . . . O . . . .

Then the ciphertext would be "HOLELWRLLDO". Note that the values of the letters remain the same, but their order has changed.

In summary, symmetric encryption uses the same key for encryption and decryption, while asymmetric encryption uses a pair of public and private keys. Substitution cipher replaces letters or characters with others according to a predetermined rule, while transposition cipher rearranges the order of the letters or characters without changing their values.

Encrypt the following plain text using

(a) Caesar cipher

(b) Rail fence cipher(key=exam) Plain text: Online mode of Examination

Ans4. (a) Encrypt using Caesar cipher:

Plain text: Online mode of Examination

Key: 3 (as an example)

Encrypted text: Rspqoh prgh ri Haejylqwhqj

(b) Encrypt using Rail Fence cipher:

Plain text: Online mode of Examination

Key: exam (as an example)

Step 1: Write the plaintext in a zigzag pattern across the number of lines equal to the length of the key "exam":

css

Copy code

O . . . . e . . . . . .

. n . . . l . . . . . .

. . l . . . . i . . . . . .

. . . i . . . . n . . . . . .

. . . . n . . . . e . . . . . .

. . . . . .

Step 2: Read off the characters row by row to get the ciphertext:

Ciphertext: "OeliniinlenneidcOiaxmtiiog"

Note that the spaces between words are removed in the ciphertext as per the Rail Fence cipher encryption rule.

Please note that these encryption techniques (Caesar cipher and Rail Fence cipher) are relatively simple and not considered secure for modern cryptographic purposes. They are used here for illustrative purposes only. In real-world scenarios, stronger encryption algorithms and proper key management practices should be used to ensure the confidentiality and integrity of sensitive information.

Q5. Describe various types of cyber crimes. Differentiate between Section 67 and 67 A of IT Act 2008. Suppose a person fraudulently or dishonestly make use of electronic signature and/or password of other person. Which section of IT Act 2008 will be applicable in this case and what are the penalties and punishments under this section?

Ans5. Cybercrime refers to illegal activities that are committed using computer systems, networks, or digital devices. There are various types of cyber crimes, including:

Cyber fraud: This involves deceiving individuals or organizations online for financial gain, such as online scams, phishing, identity theft, and credit card fraud.

Cyber hacking: This involves unauthorized access to computer systems or networks, such as hacking into email accounts, social media accounts, or corporate networks to steal data or cause disruption.

Cyber harassment: This involves harassing or bullying individuals online, such as cyber stalking, cyberbullying, or sending threatening or offensive messages online.

Cyber espionage: This involves stealing sensitive information, trade secrets, or intellectual property from individuals or organizations for economic or political gain.

Cyber terrorism: This involves using computer systems or networks to create fear, panic, or disruption for political, ideological, or terrorist purposes.

Cyber grooming: This involves using online platforms to lure and exploit minors for sexual exploitation or abuse.

Section 67 and 67A of the Information Technology (IT) Act, 2000, as amended in 2008, are specific provisions that deal with different types of cyber crimes related to publishing or transmitting obscene or sexually explicit content.

Section 67 of the IT Act 2008 deals with the publication or transmission of obscene material in electronic form. It states that whoever publishes or transmits any material that is lascivious or appeals to prurient interests, or is obscene or sexually explicit in nature, in electronic form shall be punished with imprisonment of up to three years and a fine of up to five lakh rupees for the first offense, and imprisonment of up to five years and a fine of up to ten lakh rupees for subsequent offenses.

Section 67A of the IT Act 2008 deals with the publication or transmission of material containing sexually explicit acts in electronic form. It states that whoever publishes or transmits any material that contains sexually explicit acts or conduct, in electronic form, which is lascivious or appeals to prurient interests, or is likely to deprave or corrupt persons who are likely to view, read or hear the material, shall be punished with imprisonment of up to five years and a fine of up to ten lakh rupees for the first offense, and imprisonment of up to seven years and a fine of up to ten lakh rupees for subsequent offenses.

If a person fraudulently or dishonestly makes use of electronic signature and/or password of another person, it may fall under Section 66C of the IT Act, 2008, which deals with identity theft. As per Section 66C, whoever, fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of up to three years and a fine of up to one lakh rupees.

It's important to note that cyber laws and penalties may vary by jurisdiction and it's essential to consult the relevant laws and legal authorities in your specific region for accurate and up-to-date information.

Q6. What is the difference between electronic signature and digital signature? Explain How do you authenticate an electronic document using digital signature. Assume that Alex is able to observe all messages exchanged between Bob and Cina. Alex knows only public key.

Explain how Cina will detect the following attack using digital signature . Bob sends a message x = "Transfer $1000 to Mike" to Cina. Alex intercepts the message and replaces "Mike" with "Alex".

Ans6. Electronic signature and digital signature are two different concepts used for authenticating documents or messages electronically. Here's how they differ:

Electronic signature: An electronic signature is a digital representation of a person's handwritten signature or other identifying mark that is used to sign an electronic document. It can be a scanned image of a physical signature, a typed name, or a unique symbol. Electronic signatures are generally used to indicate intent to sign a document and do not necessarily involve encryption or cryptographic techniques.

Digital signature: A digital signature, on the other hand, is a specific type of electronic signature that uses encryption and cryptographic techniques to provide additional security and integrity to a document or message. It involves the use of a digital certificate, which is issued by a trusted third-party called a Certificate Authority (CA), to verify the identity of the signer and ensure that the document or message has not been tampered with after signing.

To authenticate an electronic document using a digital signature, the following steps are typically involved:

Creation of the digital signature: The signer creates a digital signature using a private key that is securely stored on their computer or cryptographic hardware. The private key is used to generate a unique digital fingerprint of the document or message, which is then encrypted using the signer's private key.

Attachment of the digital signature: The encrypted digital signature is attached to the document or message as a separate data block. This signature serves as a proof of authenticity and integrity of the document or message.

Verification of the digital signature: To verify the digital signature, the recipient uses the signer's public key, which is available from the signer's digital certificate, to decrypt the digital signature. The decrypted digital fingerprint is then compared with a recalculated fingerprint of the received document or message. If the two fingerprints match, it indicates that the document or message has not been tampered with and the signer's identity has been verified.

In the given scenario where Alex intercepts Bob's message and replaces "Mike" with "Alex", Cina can detect the attack using the digital signature. Since the digital signature is calculated based on the entire content of the document or message, any modification or tampering with the document or message, even a minor change, will result in a different digital fingerprint. When Cina receives the tampered message with the modified name "Alex", the recalculated digital fingerprint will not match the decrypted digital signature, indicating that the document has been tampered with. Cina can then reject the message as it has failed the digital signature verification process, alerting Cina to the potential attack.