SOLVED BY VU MALIK

CS205 - Information Security

Question No.1

What is the purpose of security hardening in information security?
A) To make systems more secure and less vulnerable to attacks
B) To make systems more vulnerable to attacks
C) To make systems less secure and more vulnerable to attacks
D) To have no effect on system security

Question No.2

Which of the following is NOT a reason for using version control for IT assets?

A) To track changes to code over time
B) To collaborate with team members on projects
C) To store backups of files
D) To control access to files for unauthorized users

Question No.3

Which of the following is NOT a common security hardening technique?
A) Disabling unnecessary services and protocols
B) Updating software and operating systems to the latest versions
C) Enabling all services and protocols
D) Configuring firewalls to block all incoming traffic

Question No.4

Why is it important to keep software and operating systems up to date?
A) Newer versions may contain security fixes and patches
B) Newer versions may contain new vulnerabilities
C) Newer versions may have a negative impact on system performance
D) Newer versions may have no impact on system security

Question No.5

How can password security be improved?
A) By using short, simple passwords
B) By using the same password for all accounts
C) By using long, complex passwords and regularly changing them
D) By writing passwords down on a post-it note

SOLVED BY VU MALIK

Question No.6

What is the purpose of vulnerability management in information security?
A) To identify and prioritize vulnerabilities in systems and networks
B) To create new vulnerabilities in systems and networks
C) To ignore vulnerabilities in systems and networks
D) To have no effect on vulnerabilities in systems and networks

Question No.7

How can vulnerabilities be identified in systems and networks?
A) By regularly conducting security scans and assessments
B) By ignoring security alerts and warnings
C) By only relying on manual checks
D) By never updating software and operating systems

Question No.8

What is the purpose of regularly conducting vulnerability assessments?
A) To identify new vulnerabilities in systems and networks
B) To ignore new vulnerabilities in systems and networks
C) To create new vulnerabilities in systems and networks
D) To have no effect on vulnerabilities in systems and networks

Question No.9

What is the purpose of security engineering in information security?
A) To design, develop, and implement secure systems and networks
B) To ignore the security of systems and networks
C) To intentionally create vulnerabilities in systems and networks
D) To have no effect on the security of systems and networks

Question No.10

What is the importance of threat modeling in security engineering?
A) To ignore potential security threats
B) To design systems and networks that are resistant to known security threats
C) To create new security threats
D) To have no effect on the security of systems and networks

Question No.11

What are some common critical security controls?

A) Implementing repeaters
B) Disabling security features
C) Implementing firewalls, anti-virus software, and access controls
D) Creating new security threats

Question No.12

What is the goal of a comprehensive critical security control program?
A) To provide efficient routing
B) To protect systems and networks from known security threats
C) To intentionally create new security threats
D) To increase network capacity

Question No.13

What is the main component of data protection in information security?
a) Encryption
b) Firewall
c) Antivirus software
d) Backup and recovery plan

Question No.14

What is the term used for unauthorized access to sensitive information?
a) Data protection
b) Data confidentiality
c) Data security
d) Data breach

Question No.15

What is the term used for an open network port that can be exploited by malicious actors?
a) Secure port
b) Vulnerable port
c) Blocked port
d) Firewalled port

Question No.16

What is the main control mechanism for limiting network ports, protocols, and services?
a) Firewall
b) Router
c) Switch

d) Hub

Question No.17

What is the role of a Network Security Administrator (NSA)?
a) To monitor and enforce network security policies
b) To provide technical support for network communication
c) To handle public relations for network security
d) To manage budget for network security

Question No.18

What is the main purpose of penetration testing in information security?
a) To evaluate the security of a computer system or network
b) To provide network performance optimization
c) To provide network connectivity
d) To increase network capacity

Question No.19

What is the term used for a simulated attack on a computer system or network to identify vulnerabilities?
a) Security audit
b) Penetration test
c) Vulnerability scan
d) Risk assessment

Question No.20

What is the term used for the set of policies, procedures, and standards for information security management?
a) Information security governance framework
b) Information security management system (ISMS)
c) Information security policy manual
d) Information security standard

Question No.21

What is the main purpose of risk management in information security?
a) To identify and prioritize potential risks to information security and develop strategies to mitigate them
b) To improve network performance
c) To provide network connectivity
d) To ignore risks

SOLVED BY VU MALIK

Question No.22

What is the term used for measures taken to minimize the impact of potential risks to information security?

a) Risk mitigation
b) Risk seeding
c) Risk transfer
d) Risk acceptance

Question No.23

What is the main purpose of the Cyber Security Maturity Matrix (CSMM)?

a) To provide a common framework for assessing and improving the maturity of an organization's cybersecurity practices
b) To provide a measure of an organization's cybersecurity risk
c) To provide a measure of an organization's compliance with cybersecurity regulations
d) To Provide efficient routing when network has congestion

Question No.24

What is the term used for a model that provides a structured approach to assessing and improving an organization's cybersecurity practices?

a) Cybersecurity risk assessment framework
b) Cybersecurity maturity model
c) Cybersecurity best practices framework
d) Cybersecurity audit framework

Question No.25

Who is responsible for conducting internal audits in information security?

a) System administrators
b) Security analysts
c) Internal auditors
d) Database administrators

Question No.26

What is change management in information security?

a) The process of managing and controlling changes to a system to ensure its security
b) The process of implementing security measures in a system
c) The process of verifying the identity of a user
d) The process of testing the security measures in a system

SOLVED BY VU MALIK

Question No.27

Which of the following is considered a key aspect of Human Resource (HR) security in information security?

A. Network security
B. Data encryption
C. Employee screening and background checks
D. Firewall configuration

Question No.28

What is the primary goal of capacity management in information security?
A. To ensure the availability of resources
B. To prevent data breaches
C. To monitor network traffic
D. To manage network performance

Question No.29

What is the purpose of capacity planning in capacity management?
A. To determine the current utilization of resources
B. To predict future resource needs
C. To implement security controls
D. To identify performance bottlenecks

Question No.30

What is the primary objective of conducting an internal security assessment in information security?
A) To identify and evaluate the effectiveness of existing security controls
B) To identify potential vulnerabilities in external networks
C) To ensure regulatory compliance
D) To remove the overall security posture of an organization

Question No.31

Which of the following is **NOT** a common methodologies used to conduct an internal security assessment?
A) Penetration testing
B) Vulnerability scanning
C) Social engineering
D) Image Scanning

SOLVED BY VU MALIK

Question No.32

What is the main purpose of security accreditation in information security?
A) To assess the security of a system or network
B) To determine the security risk of using a system or network
C) To authorize the operation of a system or network in a secure manner
D) To disable the overall security posture of a system or network

Question No.33

What is the primary objective of software security testing and validation?
A) To identify and eliminate security vulnerabilities in software applications
B) To improve the overall performance of software applications
C) To ensure software applications meet user requirements
D) To optimize software applications for maximum profitability

Question No.34

_____is the sum-total of managing, organizing, and prioritizing all resources, and tasks in order to achieve a successful outcome within the stipulated timeframe.
Project referral
Project management
Resource verification
Task scheduling

Question No.35

The_____is an open framework to help organizations formulate and implement a strategy for software security that is tailored to the specific risks facing the organization.

RPM
SAMM
SDLC
IEEE

Question No.36

In context of software security, SAMM stands for_____.

Software Authenticated Maturity Model
Software Authorized Maturity Method

SOLVED BY VU MALIK

Software Assurance Maturity Model
Software Augmented Maturity Model

Question No.37

_____is focused on inspection of software in the runtime environment in order to find security problems.

Security Vibration
Security Testing
Security Hijacking
Security Spamming

Question No.38

In context of Software Security Testing & Validation,_____is focused on building assurance for the runtime environment that hosts the organization's software.

Environment Softening
Environment Hardening
Green House Project
Green House Hardening

Question No.39

In context of Software Security Testing & Validation,_____is focused on gathering security critical information from the project teams building software and communicating it to the users and operators of the software.

Environment Hardening
Operational Enablement
Green House Project
Green House Hardening

Question No.40

Which of the following is one of the stages of 3rd party penetration test?

Operational encryption
Green House Hardening
System Port Scanning
Environment Softening

SOLVED BY VU MALIK

3 marks

Question No. 41.

Can you differentiate between predictable and unpredictable risks?

Solution:

Predictable risks: These are risks that are foreseeable and can be planned for in advance. They are risks that can be anticipated through experience, historical data, and analysis of trends. Predictable risks can be identified and addressed through risk management processes, such as risk assessment, risk mitigation, risk transfer, and risk avoidance. Examples of predictable risks include financial risks, operational risks, legal risks, and regulatory risks.

Unpredictable risks: These are risks that are not foreseeable and cannot be planned for in advance. They are risks that arise unexpectedly and without warning, and are typically outside the control of the organization. Unpredictable risks are often caused by natural disasters, cyber attacks, pandemics, and other events that are difficult to predict or control. Unpredictable risks are typically addressed through contingency planning and disaster recovery processes, such as emergency response plans, crisis management plans, and business continuity plans.

Question No. 42

What is Benchmarking?

Solution:

In information security, benchmarking refers to the process of measuring an organization's security performance against industry standards or best practices. This can include comparing an organization's security controls, processes, policies, and procedures against established frameworks such as ISO 27001, NIST Cybersecurity Framework, and CIS Controls.

Question No. 43

As authentication is the process of validating a user's identity. Which factors should come in consideration for implementing strong authentication policy? List any two factors.

Solution:

There are several factors that should come into consideration when implementing a strong authentication policy. Two important factors are:

Multi-factor authentication: Multi-factor authentication (MFA) is a security measure that requires users to provide more than one form of authentication in order to verify their identity. This can include something the user knows (like a password or PIN), something the user has (like a smart card or token), or something the user is (like a fingerprint or facial recognition).

Password complexity requirements: Passwords are a common form of authentication, but they can be vulnerable to attacks if they are too simple. Strong password complexity requirements can help prevent unauthorized access to user accounts. This can include requiring passwords to be a certain length, contain a mix of upper and lowercase letters, numbers, and special characters, and prohibiting the use of easily guessable words or phrases.

Question No. 44

How can we differentiate between Circuit gateway firewall and MAC layer firewall?

Solution:

Both circuit gateway firewalls and MAC layer firewalls provide network security, they operate at different layers of the network stack and have different strengths and weaknesses. Organizations may choose to implement one or both types of firewalls depending on their specific security needs.

Question No. 45

List down any five best practices for implementing firewalls.

Solution:

Here are five best practices for implementing firewalls:

1. Define and enforce a strong security policy: Before implementing a firewall, it's important to define a security policy that outlines the rules and regulations governing network access. This policy should be communicated to all employees and enforced through the firewall's configuration.
2. Use a defense-in-depth strategy: A firewall should be part of a larger defense-in-depth strategy that includes other security measures, such as intrusion detection and prevention systems, antivirus software, and employee training.
3. Limit access to the firewall: Access to the firewall should be restricted to authorized personnel only. This can be achieved through the use of strong passwords, two-factor authentication, and access control lists.
4. Regularly update the firewall's software and rules: Firewall software and rules should be regularly updated to ensure that the firewall is able to protect against

the latest threats. This includes updating the firewall's firmware, operating system, and signature files.

5. Test the firewall's effectiveness: Regular testing should be performed to ensure that the firewall is operating effectively and providing the intended level of protection. This can include vulnerability scanning, penetration testing, and simulated attacks. Any issues identified during testing should be promptly addressed.

Question No. 46

In case of IP Security, how transport mode is different from tunnel mode?

Solution:

Transport mode is used to secure communication between two hosts or endpoints, while tunnel mode is used to provide secure communication between two networks or between a remote user and a network.

5 marks

Question No. 47

What are the basic reasons of growth of Pretty Good Privacy (PGP)?

Solution:

Pretty Good Privacy (PGP) is a popular encryption software that provides cryptographic privacy and authentication for data communication. The growth of PGP can be attributed to several reasons, including:

1. Security: PGP provides strong security features, such as encryption and digital signatures, which protect the confidentiality, integrity, and authenticity of data.
2. Privacy: PGP enables users to communicate securely without the fear of eavesdropping or interception by third parties.
3. Accessibility: PGP is widely available and can be used on various platforms, including Windows, Mac, Linux, and mobile devices.
4. Ease of use: PGP has a user-friendly interface that makes it easy for non-technical users to encrypt and decrypt messages.
5. Open-source: PGP is an open-source software that allows developers to review and modify the source code, which promotes transparency and accountability.
6. Trust: PGP has gained the trust of users, including journalists, activists, and government officials, who rely on it to communicate securely.
7. Standards-based: PGP uses well-established encryption and signature standards, such as OpenPGP and S/MIME, which ensures compatibility and interoperability with other systems.

Overall, the growth of PGP can be attributed to its strong security and privacy features, accessibility, ease of use, open-source nature, and widespread adoption by users who value privacy and security.

SOLVED BY VU MALIK

Question No. 48

Why does PGP generate a signature before applying compression?

Solution:

PGP (Pretty Good Privacy) generates a signature before applying compression because applying compression before generating a signature can potentially introduce security vulnerabilities. Generating a signature before applying compression helps to ensure the integrity and authenticity of the message, which are important security properties in cryptography.

Question No. 49

Write down in sequence the activities performed in controls validation process?

Solution:

The controls validation process typically involves the following activities performed in sequence:

1. Establishing control objectives: The first step in controls validation is to define the control objectives that need to be achieved. This involves identifying the risks and vulnerabilities associated with the process, as well as the desired outcomes.
2. Designing controls: Once the control objectives have been established, the next step is to design controls that will help achieve those objectives. This involves selecting the appropriate control mechanisms, such as policies, procedures, and technologies, and implementing them.
3. Testing controls: The next step is to test the controls to determine their effectiveness. This involves assessing the controls' ability to detect and prevent risks, as well as their reliability and accuracy.
4. Evaluating control deficiencies: If deficiencies are identified during testing, the next step is to evaluate the extent of those deficiencies and their potential impact on the control objectives.
5. Developing remediation plans: Based on the evaluation of control deficiencies, remediation plans are developed to address the deficiencies and strengthen the controls.

Question No. 50

In case of Employment Policies and Practices, what does background check state and what are the consideration factors involved for hiring some personnel?

SOLVED BY VU MALIK

Solution:

Background checks are an important part of employment policies and practices, as they help employers verify the accuracy of a candidate's job application and ensure that the individual is qualified and suitable for the position they are applying for. A background check typically involves a review of an individual's criminal record, employment history, education, and other relevant personal information.
The factors considered during the hiring process may vary depending on the organization's policies, the nature of the position, and local laws and regulations. However, some of the common considerations include:

1. Criminal history: Employers may conduct criminal background checks to ensure that the individual does not have a criminal record that would make them unsuitable for the position.
2. Employment history: Employers may verify the candidate's previous employment history to ensure that the individual has the necessary experience and skills for the job.
3. Education and credentials: Employers may verify the candidate's educational qualifications and professional credentials to ensure that the individual has the necessary knowledge and training for the job.
4. Reference checks: Employers may contact the candidate's previous employers or references to gather additional information about the individual's work ethic, attitude, and job performance.
5. Drug testing: Employers may conduct drug tests to ensure that the individual is drug-free and can perform the job duties safely and effectively.
6. Credit history: Employers may review a candidate's credit history, particularly if the position involves financial responsibilities, to assess the individual's financial responsibility.

It is important to note that background checks must comply with federal and state laws, such as the Fair Credit Reporting Act (FCRA) and state-specific laws that regulate the use of background checks in employment. Employers should also ensure that they do not discriminate against candidates based on their race, gender, age, or other protected characteristics.

Question #1 Types of software attacks = (3marks)

Question #2: Firewall Processing Modes (5 Marks)

Question #3 PGP operation-Authentication (3marks)

Question #4: One cipher text was given and i had to encrypt that code using key. transportation method. key was also given. it was pretty easy (5 Marks)

Question #5: Write down General IP security Machanism (5 Marks or 3 marks) dont remember exactly

Question # 6: Had to explain the function of Intrusion detection system (3marks)

Mcqs i dont remember but just go through the handouts and you will solve all the mcqs