CYBER SECURITY AND PRIVACY (NPTEL)

ASSIGNMENT

WEEK – 5

1. The primary function of a cybersecurity policy within an organization is to:
   a. Define a rigid set of penalties for security violations.
   b. Eliminate the need for ongoing security awareness training programs.
   c. Dictate specific technical security controls for implementation.
   d. Establish a comprehensive reference point for organizational cybersecurity practices.

2. Which type of policy is related to an organization's strategic purpose, mission, and vision?
   a. Issue-specific information security policies (ISSP)
   b. Systems-specific information security policies (SysSP)
   c. Enterprise information security policy (EISP)
   d. Technical implementation policy

3. True or False: Standards are broad, abstract documents that provide detailed procedures for employees to comply with policies.
   a. True
   b. False

4. Which of the following reflects the hierarchical top-down order of information security policies?
   a. Enterprise > Issue-Specific > Systems-Specific
   b. Systems-Specific > Issue-Specific > Enterprise
   c. Issue-Specific > Enterprise > Systems-Specific
   d. All three policy types are independent and unconnect

5. Which of the following components is typically included in the Enterprise Information Security Policy (EISP)?
   a. Incident response procedures
   b. Statement of purpose
   c. Software development guidelines
   d. Employee performance evaluations

6. True or False: Systems-specific security policies (SysSPs) can be separated into two general groups, managerial guidance SysSPs and technical specifications SysSPs
   a. True
   b. False

7. ___________ consists of details about user access and use permissions and privileges for an organizational asset or resource.
   a. Access Control Lists
   b. Configuration rules
   c. Authorized access and usage of equipment

    d. Authorization rules

8. True or False: Consequence-driven Cyber-informed Engineering (CCE) is a cyber defense concept that focuses on the lowest consequence events from an engineering perspective so that resource-constrained organizations receive the greatest return on their security investments.
    a. True
    b. False

9. ________ are nonmandatory recommendations the employee may use as a reference in complying with a policy.
    a. Practices
    b. Procedures
    c. Standards
    d. Guidelines

10. Creating "air gaps" to isolate critical systems is a cyber hygiene practice that focuses on:
    a. Installing the latest security patches.
    b. Strengthening user authentication.
    c. Segmenting networks for improved security
    d. Keeping complex passwords up-to-date.

WEEK – 6

1. A determination of the extent to which an organization's information assets are exposed to risk is known as:
    a. Risk identification
    b. Risk control
    c. Risk assessment
    d. Risk Management

2. _______is the risk to information assets that remains even after current controls have been applied.
    a. Risk appetite
    b. Residual risk
    c. Inherent risk
    d. Contingency risk

3. Which of these is not a component of risk identification?
    a. Plan & organize the process
    b. Classify, value, & prioritize assets
    c. Specify asset vulnerabilities
    d. Determine loss frequency

4. The likelihood of an attack together with the attack frequency to determine the expected number of losses within a specified time range is known as:
    a. Loss frequency

b. Attack success probability

c. Loss magnitude

d. Risk

5. _______is an information attack that involves searching through a target organization’s trash for sensitive information.

a. Shoulder surfing

b. Network sniffing

c. Dumpster diving

d. Watering hole attacks

6. Risk management in cyber security involves three key steps. These steps are:

a. Monitoring, auditing, and reporting.

b. Identifying risks, assessing risk, and controlling risks.

c. Training employees, patching vulnerabilities, and using firewalls.

d. Investigating incidents, recovering data, and learning lessons.

7. The "attack surface" in cyber security is a visualization tool that helps to understand:

a. The effectiveness of different security tools.

b. The relationship between various types of threats and the organization's assets.

c. The complexity of the organization's network infrastructure.

d. The cost of implementing different security controls.

8. During the Risk Identification phase, assets are classified into which of the following categories?

a. Financial assets, Intellectual property, and Human resources

b. Assets, Liabilities, and Equity

c. Tangible assets, Intangible assets, and Fixed assets

d. People, Procedures, Data and information, Software, Hardware, and Networking elements

9. Which formula accurately represents the calculation of risk in cyber security risk assessment?

a. Risk = Loss frequency + Loss magnitude

b. Risk = Loss frequency x Loss magnitude + Measurement Uncertainty

c. Risk = (% Risk Mitigated by Controls) / (Loss Frequency x Loss Magnitude)

d. Risk = Loss frequency - Loss magnitude + Measurement Uncertainty

10. You are a security analyst for a company that manages an online store with a customer database. Industry reports indicate a 10 percent chance of an attack this year, based on an estimate of one attack every 10 years. A successful attack could result in the theft of customer data. There is a 20% chance of the threat being able to materialize and achieve its objectives even in place of robust secure protection mechanisms. The customer database is most valued being an e-commerce company at 90 in a 1-100 scale. The IT department informed that 60% of the assets will be exposed after a successful attack. The estimation of measurements is 80% accurate. Calculate the risk associated to the asset with a potential SQL injection attack.

a. 3.756

b. 4.196
c. 3.276
d. 1.296

WEEK - 7

1. ________ is a comprehensive system comprising software, encryption techniques, protocols, legal arrangements, and third-party services that facilitate secure communication among users by utilizing digital certificates.
   a. Registration authority
   b. Public key infrastructure
   c. Digital signature
   d. Certificate authority

2. Which ring does the kernel, the core of the operating system, typically operate?
   a. Ring 2
   b. Ring 1
   c. Ring 0
   d. Ring 3

3. Which of the following statements is not true?
   a. Hash functions are one-way.
   b. It is possible to attach a message authentication code (MAC) to allow only specific recipients to access the message digest.
   c. Hashing functions require the use of keys.
   d. Hash functions are used in password verification systems to confirm the identity of the user.

4. Which of the following is not related to defense against rainbow cracking?
   a. Password hash salting
   b. key stretching
   c. Key strengthening
   d. Private key encryption

5. Which of the following statements is/are correct?
   a. TCP is a connection-oriented protocol, while UDP is connectionless.
   b. TCP is comparatively faster than UDP.
   c. TCP provides reliable data delivery, while UDP does not.
   d. Both a and c.

6. Which Which of the following statements about Virtual Private Networks (VPN) are true? of the following statements is/are correct?
   a. A VPN is an encrypted connection over the Internet from a device to a network.
   b. A VPN keeps the contents of the network messages hidden from observers who may have access to public traffic.
   c. A VPN protects its users by masking their IP address.

d. All the above.

7. Endpoint Detection and Response (EDR) solutions are primarily focused on:
   a. Securing network perimeters and firewalls.
   b. Protecting individual user devices from threats.
   c. Monitoring and analyzing network traffic for malicious activity.
   d. Providing vulnerability assessments for servers and applications.

8. Cryptojacking is a cyberattack that leverages a victim's computer resources for the attacker's financial gain. Which of the following best describes the attacker's activity in a cryptojacking attack?
   a. Encrypting the victim's data and demanding a ransom payment.
   b. Gaining unauthorized access to the victim's personal information for resale.
   c. Silently using the victim's processing power to solve complex mathematical problems for financial reward.
   d. Disrupting the normal operation of the victim's system to cause inconvenience.

9. What kind of infrastructure Advanced Persistent Threat (APT) groups are typically known for targeting?
   a. Personal computers of home users.
   b. Critical infrastructure essential for national security (e.g., power grids, communication networks).
   c. Public Wi-Fi networks at cafes or airports.
   d. Outdated operating systems on personal devices of insignificant value

10. Which of the following is NOT one of the stages in the Intrusion Kill Chain framework?
    a. Reconnaissance
    b. Exploitation
    c. Cleanup
    d. Command and Control

WEEK - 8

1. The Cost-Benefit Analysis (CBA) formula for risk management decisions is given by:

a. CBA = ALE(prior) - ALE(post) – ACS
b. CBA = ALE(prior) - ALE(post) + ACS
c. CBA = ALE(prior) + ALE(post) – ACS
d. CBA = ALE(prior) + ALE(post) + ACS

2. In a cost-benefit analysis, _________ is the expected percentage of loss that would occur from a particular attack

a. Single Loss Expectancy

b. Exposure Factor

c. Annualized Loss Expectancy

d. None of the above

3. A ______ is a network security device that monitors traffic to or from a network and decides whether to allow or block specific traffic based on a defined set of security rules.

a. Intrusion Detection and Prevention System

b. Router

c. Intrusion Detection System

d. Firewall

4. What risk management approach aims to minimize the impact of losses resulting from an actual incident, disaster, or attack by implementing thorough contingency plans and preparations?

a. Mitigation risk control strategy

b. Transference risk control strategy

c. Defense risk control strategy

d. Termination risk control strategy

5. The product of the asset's value and the exposure factor is known as:

a. Single Loss Expectancy

b. Annualized Loss Expectancy (Prior)

c. Annualized Rate of Occurrence

d. Annualized Loss Expectancy (Post)

6. Which of the following is not true?

a. Bit Stream ciphers encrypt data one bit at a time, while block ciphers encrypt data in fixed-size blocks.

b. Bit Stream Cipher is used for Data in Transit Encryption, whereas Block Cipher is used for Data at Rest Encryption

c. Bit Stream Cipher can operate as a Block Cipher but Block Cipher cannot operate as a Bit Stream Cipher

d. Bit Stream ciphers are generally considered faster than block ciphers.

7. The False Acceptance Rate (FAR) in biometrics refers to:

a. The system mistakenly accepting an unauthorized user.

b. The system correctly rejecting an unauthorized user.

c. The time it takes for a system to identify a user.
d. The user's frustration with the authentication process.

8. The IAAA framework in the context of access control stands for?

a. Isolation, Authentication, Authorization, Availability

b. Identification, Authentication, Authorization, Accountability

c. Inspection, Authentication, Access, Authorization
d. Intrusion Detection, Analysis, Authorization, Administration

9. What is a significant challenge associated with symmetric key encryption?

a. Slower encryption and decryption compared to asymmetric methods.

b. Limited compatibility with modern encryption algorithms.

c. Higher computational cost for key generation.

e. Key management: securely distributing and safeguarding the shared key.

10. In risk management, which equation is used to calculate the expected loss per risk?

a. Single Loss Expectancy (SLE) = Asset Value × Exposure Factor (EF)

b. Annualized Loss Expectancy (ALE) = Single Loss Expectancy (SLE) × Annualized Rate of Occurrence (ARO)

c. Asset Value = Single Loss Expectancy (SLE) × Exposure Factor (EF)

d. Annualized Rate of Occurrence (ARO) = Asset Value × Single Loss Expectancy (SLE)

BY : SAURAV KUMAR