P.G Department of Computer Applications

K2 level question 18PMC427 –Information security

Unit I

1.What is the primary goal of an information security program?
A. To eliminate losses related to employee actions
B. To eliminate losses related to risk
C. To reduce losses related to residual risk
D**. To reduce losses related to loss of confidentiality, integrity, and availability**

2. Which of the following is not a stage of the traditional SDLC?

a. Planning
b. Analysis
c. Prototyping
d. Implementation

3. When changes are made to the firm's data, information, and software, the type of information security risk is:

a. unauthorized disclosure and theft.
b. unauthorized use.
c. unauthorized destruction and denial of service.
d. unauthorized modification.

4.The backup plan that is in use when hot and cold sites are in place is referred to as:

a. redundancy.
b. diversity.
c. mobility.
d. contingency.

5.What is the methodology for the design and implementation of an information system in an organi'ation.

a.LCSD

b.DSLC

c.CLSD

d.SDLC

6.The most successful kind of top-down approach involves a formal development strategy referred to as a ____.

a. **systems development life cycle**

b. systems schema

c. systems design

d. development life project

7.computer is the ____ of an attack when it is used to conduct the attack.

a. subject

b. facilitator

c. target

d. object

8.Protecting data being transferred from exposure to third party is referred as

(a) denial of service

(b) integrity

(c) **authentication**

(d) unavailability

9.What are the three main goals of computer security?

(a) Control, intelligence, action

(b) Central intelligence agency

(c) **Confidentiality, integrity, availability**

(d) Confidence, integrity, action

Unit II

10._____ is a weakness that can be exploited by attackers.
a) System with Virus
b) System without firewall
c) **System with vulnerabilities**
d) System with strong password

11.ISMS is abbreviated as _____
a) Information Server Management System
b) Information Security Management Software
c) Internet Server Management System
d) **Information Security Management System**

12.When identifying the assets you have in your organization, what would you include?
A. Hardware
B. Software
C. Personnel
D. Only A and B
E. A, B, and C

13.When identifying the assets you have in your organization, what would you include?
A. Hardware
B. Software
C. Personnel
D. Only A and B
E. A, B, and C

14.Who should perform vulnerability assessments?
A. Internal security professionals working as employees
B. External security professionals hired as consultants
C. **Either internal or external security professionals, or both**
D. Only the IT personnel who own the systems

15. You want to identify if any of the discovered vulnerabilities can be exploited. What should you perform?
A. Audit
B. Transaction and applications test
C. Functionality test
D. Exploit assessment

Unit III

16.Which of the following is a goal of risk management?
A. **To identify the correct cost balance between risk and controls**

B. To eliminate risk by implementing controls
C. To eliminate the loss associated with risk
D. To calculate value associated with residual risk

17.Which of the following is not a component of risk management?

a. Implement the controls.
b. Establish an information security policy.
c. Define the risks.
d. Set benchmarks

18.Which of the following is not one of the objectives of a risk management plan?

a. Create a list of threats

b. Create a list of vulnerabilities

c. Identify costs

d. Eliminate risk

19.Which one of the following properly defines total risk?
A. Threat - Mitigation
B. Threat × Vulnerability × Asset Value
C. Vulnerability - Controls
D. Vulnerability × Controls

20.Which one of the following properly defines risk?
A. Threat × Mitigation
B. Vulnerability × Controls
C. Controls - Residual Risk
D. Threat × Vulnerability

21. You have applied controls to minimize risk in the environment. What is the remaining risk called?
A. Remaining risk
B. Mitigated risk
C. Managed risk
D. Residual risk

22.Who is ultimately responsible for losses resulting from residual risk?
A. End users
B. Technical staff
C**. Senior management**
D. Security personnel

23.What are valid contents of a risk management plan?
A. Objectives
B. Scope
C. Recommendations
D. POAM
E. All of the above

24.What are valid contents of a risk management plan?
A. Objectives
B. Scope
C. Recommendations
D. POAM
E. All of the above

25.What will the scope of a risk management plan define?
A. Objectives
B. POAM
C. Recommendations
D. Boundaries

26.Which of the following should you match with a control to mitigate a relevant risk?
A. Threats
B. Vulnerabilities
C. Threat/vulnerability pair
D. Residual risk

Unit IV

Unit V

27.What are two types of intrusion detection systems?
A. Intentional and unintentional
B. Natural and man-made
C. Host-based and network-based
D. Technical and physical

28.What type of control is an intrusion detection system (IDS)?
A. Preventive
B. **Detective**
C. Corrective
D. Recovery

P.G DEPARTMENT OF COMPUTER APPLICATIONS

INFORMATION SECURTIY-18PMC427

K1 LEVEL QUESTION& ANSWER

UNIT I

1.Define information security.

It is a well-informed sense of assurance that the information risks and controls are in balance.

2. List the critical characteristics of information.

•Availability • Accuracy • Authenticity

• Confidentiality • Integrity • Utility • Possession

3. Define security. What are the multiple layers of security?

Security is "the quality or state of being secure-to be free from danger".

• Physical Security • Personal Security

• Operations Security • Communication Security

• Network Security • Information Security

4. When can a computer be a subject and an object of an attack respectively?

When a computer is the subject of attack, it is used as an active tool to conduct theattack. When a computer is the object of an attack, it is the entity being attacked.

5. Why is a methodology important in implementing the information security?

Methodology is a formal approach to solve a problem based on a structured sequenceof procedures.

6.Difference between vulnerability and exposure.

Vulnerability

Weakness or fault in a system or protectionmechanism that expose information toattack or damage.

Exposure

The exposure of an information system is asingle instance when the system is open todamage.

7.List out the security services.

Three security services:Confidentiality, integrity, and availabilityThreats are divided into four broad classes:

Disclosure, or unauthorized access to information

Deception, or acceptance of false data

Disruption, or interruption or prevention of correct operation

Usurpation or unauthorized control of some part of a system.

8. Define the snooping and spoofing.

Snooping:

The unauthorized interception of information is a form of disclosure. It
is passive, suggesting simply that some entity is listening to (or reading) communications or bro wsing through files or system information.

Masquerading or spoofing:

An impersonation of one entity by another is a form of both deception and usurpation.

9. List the components used in security models.

Software,,,Hardware,Data,People,Procedures,Networks

10. What are the functions of Information Security?

Protects the organization's ability to function

Enables the safe operation of applications implemented on the organizations ITsystems

Protects the data the organization collects and uses

11. What are the phases of SDLC Waterfall method?

Investigation,Analysis,Logical Design,,Physical Design,Implementation,Maintenance & change

12.Define information security.

It is a well-informed sense of assurance that the information risks and controls are in balance.

13. What is C.I.A?

The C.I.A. triangle was the standard based on confidentiality, integrity, and availability. The C.I.A. triangle has expanded into a list of critical characteristics of information.

14.Write a note on the history of information security

Computer security began immediately after the first mainframes were developed Groups developing code-breaking computations during World War II created the first modern computers Physical controls were needed to limit access to authorized personnel to sensitive military locations Only rudimentary controls were available to defend against physical theft, espionage, and sabotage

15. What is the scope of computer security?

The scope of computer security grew from physical security to include: Safety of the data Limiting unauthorized access to that data Involvement of personnel from multiple levels of the organization

16. Define Physical security

Physical Security - to protect physical items, objects or areas of organization from unauthorized access and misuse

17. Define Personal Security

Personal Security involves protection of individuals or group of individuals who are authorized to access the organization and its operations

18. Define Operations security

Operations security focuses on the protection of the details of particular operations or series of activities.

19.Define Communications security

Communications security - encompasses the protection of organization's communications media, technology and content

20.Define Network security

Network security - is the protection of networking components,connections,and contents

21.Define Information security

Information security - is the protection of information and its critical elements, including the systems and hardware that use, store, and transmit the information

22. What are the critical characteristics of information?

Availability,Accuracy,Authenticity,Confidentiality,Integrity,Utility,Possession

23.What are the components of an information system?

An Information System (IS) is much more than computer hardware; it is the entire set of software, hardware, data, people, and procedures necessary to use information as a resource in the organization

24. What is meant by balancing Security and Access?

Balancing Security and Access

It is impossible to obtain perfect security - it is not an absolute; it is a process

Security should be considered a balance between protection and availability

To achieve balance, the level of security must allow reasonable acces, yet protect against threats

25.What are the approaches used for implementing information security?

Bottom Up Approach

Top-down Approach

26. What is SDLC?

The Systems Development Life Cycle

Information security must be managed in a manner similar to any other major system implemented in the organization

Using a methodology

ensures a rigorous process

avoids missing steps

27.Explain different phases of SDLC

Investigation, Analysis, Logical Design, Physical Design, Implementation,Maintenance and Change

28.What is Security SDLC?

Security Systems Development Life Cycle

The same phases used in the traditional SDLC adapted to support the specialized implementation of a security project

Basic process is identification of threats and controls to counter them

The SecSDLC is a coherent program rather than a series of random, seemingly unconnected actions

29. How information security is viewed as a social science?

Social science examines the behavior of individuals interacting with systems

Security begins and ends with the people that interact with the system

End users may be the weakest link in the security chain

Security administrators can greatly reduce the levels of risk caused by end users, and create more acceptable and supportable security profiles

30.What are the information security roles to be played by various professionals in a typical organization?

Senior Management - Chief Information Officer, Chief Information Security Officer
Security Project Team
The champion
The team leader
Security policy developers
Risk assessment specialists
Security professionals
Systems administrators
End users

31. What is attack?

An attack is an intentional or unintentional attempt to cause damage or otherwise compromise the information. If some one casually reads sensitive information not intended for his or her use ,this considered as a passive attack. If a hacker attempts to break into an information system,the attack is considered active.

Unit II

32.What are the three types of data ownwership and their responsibilities?

Data Owner - responsible for the security and use of a particular set of information Data Custodian - responsible for the storage, maintenance, and protection of the information Data Users - the end systems users who work with the information to perform their daily jobs supporting the mission of the organization

33.What is the difference between a threat agent and a threat?

A threat is a category of objects,persons,or other entities that pose a potential danger to an asset. Threats are always present. A threat agent is a specific instance or component of a threat. (For example All hackers in the world are a collective threat Kevin Mitnick,who was convicted for hacking into phone systems was a threat agent.)

34.What is the difference between vulnerability and exposure?

The exposure of an information system is a single instance when the system is open to damage. Weakness or faults in a system expose information or protection mechanism that expose information to attack or damage or known as vulnerabilities.

35.What is hacking?

Hacking can be defined positively and negatively. To writes computer programs for enjoyment to gain access to a computer illegally

36.What is security blue print?

The security blue print is the plan for the implementation of new security measures in the organization. Some times called a framework,the blue print presents an organized approach to the security planning process.

37.Define Threat.

Threats is anything that can exploit a vulnerability accidentally or intentionally and destroy or damage an asset

38.Define Deliberate software attacks

Deliberate software attacks can be referred as malware, Malicious code or malicious software. Deliberate software attacks occur when an individual or group designs or deploys a software to attack a system. These software components or programs are designed to damage, destroy, or deny service to the target systems.

39.Define Vu**lnerability**

It means gap or weakness in our protection efforts.

40.What is Intellectual Property?

Intellectual property, or IP as it is commonly referred to, consists of all the pieces of your business that you or your employees have thought of. It's the things that differentiate you from the competition that you came up with using your intellect

41.Define DELIBERATE ACTS of theft

These acts are done by people of organizations to harm the information. The attackers have a malicious intent and wish to steal or destroy the data. Acts of espionage, Hacking, Cracking, come under deliberate acts.

42.How are deliberate software attacks referred as?

Deliberate software attacks can be referred as malware, Malicious code or malicious software. Deliberate software attacks occur when an individual or group designs or deploys a software to attack a system. These softwarecomponents or programs are designed to damage, destroy, or deny service to the target systems.

43.What is NSTISSC Security model?

This refers to "The National Security Telecommunications and Information Systems Security Committee" document. This document presents a comprehensive model for information security. The model consists of three dimensions

44.What are the four important functions, the information security performs in an organization?

Information security performs four important functions for an organization: Protects the organization's ability to function. Enables the safe operation of applications implemented on the organization's IT systems.

45.What are threats?

A threat, in the context of computer security, refers to anything that has the potential to cause serious harm to a computer system.

46.What are the different categories of threat? Give Examples.

Spoofing of user identity.

Tampering.

Repudiation.

Information disclosure (privacy breach or Data leak)

Denial of Service (D.o.S.)

Elevation of privilege.

47.What are different acts of Human error or failure?

Human error is an unintentional action or decision. Violations are intentional failures – deliberately doing the wrong thing. There are three types of human error: slips and lapses (skill-based errors), and mistakes. These types of human error can happen to even the most experienced and well-trained person.

48.How human error can be prevented?

Standard Operating Procedures, Fatigue Management, workplace ergonomics and Safety Management are examples of systems and methods to prevent human error.

49.What is Intellectual property?

Intellectual property (IP) is the lifeblood of every organization. ... IP protection is a complex duty with aspects that fall under the purview of legal, IT, human resources and other departments. Ultimately a chief security officer (CSO) or risk committee often serves to unify intellectual property protection efforts.

50.**How Intellectual property can be protected?**

Intellectual property law deals with the rules for securing and enforcing legal rights to inventions, designs, and artistic works. Just as the law protects ownership of personal property and real estate, so too does it protect the exclusive control of intangible assets.

51. What is deliberate acts of espionage or trespass?

Deliberate Acts of Espionage or Trespass (unauthorized access and/or data collection) Deliberate Acts of Information Extortion (blackmail or information disclosure) Deliberate Acts of Sabotage or Vandalism (destruction of systems or information)

52. **Who are Hackers? What are the two hacker levels?**

The classic perpetrator of deliberate acts of espionage or trespass is the hacker. Hackers are "people who use and create computer software [to] gain access to information illegally". Generally two skill levels among hackers: Expert hacker , unskilled hacker

53. What is information extortion?

Extortion (also called shakedown, outwrestling and exaction) is a criminal offense of obtaining money, property, or services from an individual or institution, through coercion. ... Extortion is commonly practiced by organized crime groups

54.What is Cyber terrorism?

cyber terrorism means to damage information, computer systems and data that result in harm against non-combatant targets

55. What are the deliberate acts of theft?

Deliberate Acts of Information Extortion, the intentional illegal acquisition of information from an organization, with the intent to blackmail the organization with the threat of publication, dissemination, or use.

56. What are the forces of Nature affecting information security?

Fire, Flood , Earthquake, lightning, etc

57. What are technical hardware failures or errors?

Physical threats cause damage to computer systems hardware and infrastructure. Examples include theft, vandalism through to natural disasters.

58. What are technical software failures or errors?

"An error is a deviation from accuracy or correctness" and "A software bug is an error, flaw, failure, or fault in a computer program or system that causes it to produce an incorrect or unexpected result, or to behave in unintended ways "

59. What is technological obsolescence?

When a technical product or service is no longer needed or wanted even though it could still be in working order. Technological obsolescence generally occurs when a new product has been created to replace an older version.

60.What is an attack?

Attack is any attempt to expose, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of an asset.

61. What is a malicious code?

Malicious code is the term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system. Malicious code is an application security threat that cannot be efficiently controlled by conventional antivirus software alone.

62.Define Virus

A computer virus is a type of malicious software that, when executed, replicates itself by modifying other computer programs and inserting its own code.

Define Hoaxes

63. What is Distributed Denial-of-service (DDoS)?

A distributed denial-of-service (DDoS) attack is an attack in which multiple compromised computer systems attack a target, such as a server, website or other network resource, and cause a denial of service for users of the targeted resource.

64. What is Back Door?

A backdoor is a means to access a computer system or encrypted data that bypasses the system's customary security mechanisms. ... However, attackers often use backdoors that they detect or install themselves as part of an exploit.

65. Define Dictionary attack

A dictionary attack is a method of breaking into a password-protected computer or server by systematically entering every word in a dictionary as a password. A dictionary attack can also be used in an attempt to find the key necessary to decrypt an encrypted message or document.

66.What are the various forms of attacks.

In computers and computer networks an attack is any attempt to expose, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of an asset.

67. What are the attack vectors?

An attack vector is a path or means by which a hacker (or cracker) can gain access to a computer or network server in order to deliver a payload or malicious outcome. Attack vectors enable hackers to exploit system vulnerabilities, including the human element.

68. What is Denial-of-service (DoS) ?

A denial-of-service (DoS) is any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service.

69. Define Spoofing

A spoofing attack is when a malicious party impersonates another device or user on a network in order to launch attacks against network hosts, steal data, spread malware or bypass access controls.

70. Define Man-in-the-Middle

In cryptography and computer security, a man-in-the-middle attack (MITM) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

Unit III

71.What are the five steps in risk management process?

Step 1: Identify the Risk. ...

Step 2: Analyze the risk. ...

Step 3: Evaluate or Rank the Risk. ...

Step 4: Treat the Risk. ...

Step 5: Monitor and Review the risk.

72.Define Risk identification

It is the process of determining **risks** that could potentially prevent the program, enterprise, or investment from achieving its objectives.

73.Define disaster recovery plan

It is a documented process or set of procedures torecover and protect a business IT infrastructure in the event of a disaster. Such aplan, ordinarily documented in written form, specifies procedures an organization is to follow in the event of a disaster

74.What are the four risk control strategies?

Apply safeguards (**avoidance**) **Transfer** the risk (transference) Reduce the impact (mitigation) Inform themselves of all of the consequences and **accept** the risk without control or mitigation (acceptance)

75.Define residual risk

It is a threat that remains after an organization has implemented security controls to comply with legal requirements

76.Define Risk Assessment

It can determine the relative risk for each of the vulnerabilities through a process called risk assessment

77.Listout the types of Access Controls

- Discretionary Access Controls (DAC) are implemented at the discretion or option of the data user
- Mandatory Access Controls (MACs) are structured and coordinated with a data classification scheme, and are required
- Nondiscretionary Controls are those determined by a central authority in the organization and can be based on that individual‘s role (Role-Based Controls) or a specified set of duties or tasks the individual is assigned (Task-Based Controls) or can be based on specified lists maintained on subjects or objects

78. Define Lattice-based Control

Another type of nondiscretionary access is lattice-based control, where a lattice structure (or matrix) is created containing subjects and objects, and the boundaries associated with each pair is contained

This specifies the level of access each subject has to each object

In a lattice-based control the column of attributes associated with a particular object are referred to as an access control list or ACL

The row of attributes associated with a particular subject (such as a user) is referred to as a capabilities table

UNIT IV

79.What is a policy?

Information security policy is a set of policies issued by an organization to ensure that all information technology users within the domain of the organization or its networks comply with rules and guidelines related to the security of theinformation stored digitally at any point in the network

80.What is a security blueprint?

A blueprint is a detailed plan or program of action

81.What does NIST stand for?

NIST is the National Institute of Standards and Technology, a unit of the U.S. Commerce Department. Formerly known as the National Bureau of Standards, NIST promotes and maintains measurement standards. It also has active programs for encouraging and assisting industry and science to develop and use these standards.

82.What is NIST compliance?

NIST guidance provides the set of standards for recommended security controls for information systems at federal agencies

83.Why is the NIST important?

A NIST certification is important because it supports and develops measurement standards for a particular service or product. It is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems.

84. What are the three types of security policies?

The security policy is a high-level document that defines the organization's vision concerning security, goals, needs, scope, and responsibilities.

85. Define Issue-Specific Security Policy (ISSP)

Issue-Specific Security Policy,ISSP, addresses specific technology, requires updates frequently, and contains a statement on the organization's position on specific issues.

86. What are ACL Policies?

An access control list (ACL), with respect to a computer file system, is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects.

87. Mention the Drawbacks of ISO 17799/BS 7799

BS 7799 was created in 1995 by the British Standards Institute (BSI). It focused on protecting the availability, confidentiality and integrity of an organization's information. ... However, it is possible for an organization to develop its security posture based off of the ISO 17799:2005 Code of Practice only.

88. What are the objectives of ISO 17799?

The ISO/IEC 17799 details 127 security measures, organized into 10 sections; these specify best practices for: business continuity planning; system access control; system development and maintenance; physical and environmental security; compliance; personnel security; security organization; computer and operations

89.What is Security perimeter?

Network perimeter security is an essential element for any modern business whose network has access to the Internet and the World Wide Web.

90.What are the key technological components used for security implementation?

For years information security professionals have been focusing on keyconcepts such as Confidentiality, Availability, Integrity, Privacy, Authentication, Authorization and Availability. These concepts depend on the design, development, implementation and management of technological solutions and processes.

91.What is Systems-Specific Policy (SysSP)?

System-Specific Security Policy, SysSP, is a policy that functions as instructions or procedures that are to be used when configuring systems.

92. What is the goal of blueprint?

The goal of an information security blueprint is to gather an organization's requirements, provide a visualization of those requirements and initiate the process of interweaving information security as part of the organization's culture.

93.What are the approaches of ISSP?

Three approaches when creating and managing ISSPs:

- Create a number of independent ISSP documents
- Create a single comprehensive ISSP document
- Create a modular ISSP document

Unit V

94.What are firewalls?

A firewall is a network security system designed to prevent unauthorized access to or from a private network.

95. Explain different generations of firewalls.

Packet-filtering firewalls are divided into two categories: stateful and stateless. ... Next-generation firewalls (NGFW) combine traditional firewall technology with additional functionality, such as encrypted traffic inspection, intrusion prevention systems, anti-virus, and more.

96.What is the drawback of packet-filtering router?

Despite their advantages, packet-filtering firewalls have these disadvantages: They can be complex to configure. They cannot prevent application-layer attacks. They are susceptible to certain types of TCP/IP protocol attacks.

What are Screened-Host Firewall Systems

97.A screened subnet firewall is a model that includes three important components for security. This type of setup is often used by enterprise systems that need additional protection from outside attacks.

98.What is the use of an Application proxy?

A proxy firewall is a network security system that protects network resources by filtering messages at the application layer.

99. What are dual homed host firewalls?

Dual-homed is a general term for proxies, gateways, firewalls, or any server that provides secured applications or services directly to an untrusted network.

100.What is the use of NAT?

A NAT (Network Address Translation or Network Address Translator) is the virtualization of Internet Protocol (IP) addresses. NAT helps improve security and decrease the number of IP addresses an organization needs.

101.What are intrusion detection systems(IDS)?

An intrusion detection system (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. ... Although intrusion detection systems monitor networks for potentially malicious activity, they are also prone to false alarms

P.G Department of Computer Applications

K3k4 level question

18PMC427 –Information security

Unit I

1. List the types of attack? Compare.
2. What is meant by top-down approach to security implementation? Give its advantages.
3. What is meant by bottom-up approach to security implementation? Give its disadvantages.
4. List the three components of C.I.A. triangle? What are they used for?
5. Compare threat agent and a threat
6. Who is involved in the security development life cycle?
7. Give the measures that can be taken to protect confidentiality of information.
8. Classify the critical characteristics of information
9. Discuss in detail NSTISSC security model.

Unit II

10. Differentiate between threats and attacks.
11. What is a threat? Explain in detail the various groups of threats facing an organization.
12. List the four important functions of information security in an organization?
13. Compare law and ethics
14. Discuss about civil law, and what does it accomplish?
15. Classify the primary examples of public law
16. What is a policy? Compare it from a law?
17. List the three general categories of unethical and illegal behavior?
18. Classify the best method for preventing an illegal or unethical activity?
19. Discuss about vulnerability

Unit III

20. List the four risk strategies for controlling risk?
21. Which community of interest usually takes the lead in Information security risk management? Why?

22. Discuss the formula for calculating risk
23. List the three types of plans that are involved in mitigation of risk?
24. List the three common methods of risk avoidance?
25. Describe in detail the process of risk identification.
26. Discuss about risk assessment and the documentation of its results.
27. Classify the risk control strategies that guide an organization? Elaborate.
28. Classify the components of asset valuation?
29. Classify the various feasibility studies considered for a project of information security
30. Controls and safeguards?

Unit IV

31. List the styles of architecture security models .Discuss them in detail.
32. List out the people affected in security policy.

    State the pros of Visa international security model.
33. Briefly explain the NIST SECURITY MODEL

UNIT V

34. List the basic functions of access control devices?.
35. Discuss about intrusion detection system. Explain its types in detail.

P.G Department of Computer Applications

K4k5 level question & Answers

18PMC427 –Information security

Unit I

1. Analyze the security of SDLC.
2. Describe the critical characteristics of information. How are they used in the study of computer security?
3. Briefly explain the components of an information system and their security. How will you balance security and access?
4. Describe the system development life cycle?
5. Explain the security system development life cycle?

Unit II

6. Discuss in detail the Legal ,Ethical and Professionalism issues during security investigation.
7. Explain Ethical Concepts in Information Security.
8. Explain the ethical concepts in Information Security and the deterrence to illegal and unethical behaviour.
9. Define an attack. Describe attack replication vectors & major types of attacks.
10. Analyze Espionage laws

Unit III

11. Discuss in detail the process of assessing and controlling risk management issues.
12. Classify the four basic steps in risk management? Describe.
13. What are access controls and explain their types?
14. Discuss about Asset Identification & Valuation
15. Discuss about Data Classification & Management

Unit IV

17. Explain the design of Security Architecture in detail.
18. Discuss about NIST Security Models in detail.
19. Explain VISA International Security Model in detail.

UNIT V

20. List any two IDS. Mention its category of classification
21. Write notes on the control devices used in security design
22. Discuss about Firewalls in detail.
23. Discuss about cryptography in detail