Unit 1 – Introduction to computer and information security

2 Marks

1. Define following terms: i) Confidentiality ii) Accountability S22
2. List any four basic for security. Sample
3. Differentiate between viruses & worms (any two). S22
4. Compare virus and logic bomb. (any two points). S23
5. Define computer security and state it's need. W22
6. Describe sniffing attack. W22
7. Give example of Active and Passive attack. Sample W23
8. List any two types of active and passive attacks. S23
9. List any four virus categories. W23

4 Marks

1. Define following terms: i) Operating System Security ii) Hot fix iii) Patch iv) Service pack. S22
2. Define Risk. Describe qualitative and quantitative risk analysis. W22
3. Explain criteria's for information classification. Sample
4. Explain basic principles of information security. W23
5. Describe CIA model with suitable diagram. S23

6 Marks

1. Explain DOS with neat diagram. S22
2. Define Information. Explain the basic principle of information security. S22
3. State the criteria for information classification. Explain information classification. W22, 23
4. List Need and Importance of Information? State the Information Classification. Sample
5. Define virus and describe the phases of virus. W22 S23
6. Explain the terms: i) Vulnerability ii) Threats iii) Risks (iv) Assels. S23
7. Explain the following attacks using an example : (i) Sniffing (ii) Spoofing (iii) Phishing. W23

Unit 2 – User Authentication and Access Control

2 Marks

1. Explain the terms: i) Shoulder surfing S22 W22
2. ii) Piggybacking. S22
3. List any four features of DAC. Sample
4. List any four biometric mechanisms. W23
5. Identify any four individual user responsibilities in computer security. S23

4 Marks

1. Define access control and explain authentication mechanism for access control. S22
2. Describe the features of DAC access control policy. S22
3. Write short note on DAC and MAC. W22
4. State the features of (i) DAC (ii) MAC. W23 S23
5. Explain working of biometric access control with any type of example. Explain the mechanism of fingerprint & voice pattern in Biometrics. S22 W22 Sample
6. Explain the term Authorization and Authentication with respect to security. W22 Sample
7. Describe the dumpster diving with its prevention mechanism. Sample
8. Explain any two password attacks. W23
9. Describe any four password selection criteria. S23
10. Describe : (i) Piggybacking (ii) Dumpster diving (iii) shoulder surfing. S23 W23

Unit 3 – Crytography

2 Marks

1. Define term cryptography. S22, 23 W22, W23 Sample
2. Define term Cryptology. Sample S23
3. Define term Cryptanalysis. W23

4 Marks

1. Explain digital signature in Cryptography. Describe digital signature technique using message digest. S22 W23
2. Enlist substitution techniques & explain anyone. S22
3. Consider plain text “COMPUTER ENGINEERING” and convert given plain text into cipher text using „Caesar Cipher‟ with shift of position three- write down steps in encryption. S22
4. Consider plain text “INFORMATION” and convert given plain text into cipher text using ‘Caesar Cipher’ with shift of position three-write down steps in encryption. Sample
5. Consider plain text “CERTIFICATE” and convert it into cipher text using Caesar Cipher with a shift of position 4. Write steps for encryption. W23
6. Convert the given plain text, encrypt it with the help of Caesor’s cipher technique. “Network and Information Security”. S23
7. Explain Caesar’s cipher substitute technique with suitable example. W22
8. Write & explain DES algorithm with suitable example. S22 W22
9. Differentiate between symmetric and asymmetric key cryptography. S22, 23 Sample
10. Write an algorithm for simple columnar transposition technique and explain with example. W22
11. Write a short note on steganography with an example. Explain stenography technique with suitable diagram. W22, 23 Sample S23
12. Explain creation and verification of digital signature. W22
13. Convert the given plain test into cipher text using single columnar technique using following data • Plain Text: INFORMATION SECURITY • Number of Columns: 06 • Encryption Key: 326154. Sample W23
14. Find the output of the initial permutation box when the input is given in hexadecimal as: 0x0002 0000 0000 0001. Sample
15. Considering DES, find the output of the initial permutation box when the input is given in hexadecimal as, 0×0000 0080 0000 0002. W23
16. Find the output of the initial permutation box when the input is given in hexadecimal as 0 × 0003 0000 0000 0001. S23

Unit 4 – Firewall and Intrusion Detection System

2 Marks

1. Define firewall. Enlist types of firewalls. S22 W23
2. Explain need for firewall. W22 Sample
3. State any two policies of the firewall. S23

4 Marks

1. Differentiate between firewall & IDS. S22, 23 Sample
2. Differentiate between host-based & network-based IDS. S22
3. Explain Host based IDS. W22 Sample
4. Describe DMZ with suitable example. S22, 23 W22, 23
5. Demonstrate the advantages of setting up a DMZ with two firewalls. Sample
6. Explain honey pots. W22
7. State the use of packet filters. Explain its operation. W23
8. State the working principle of application gateways. Describe circuit gateway operation. W23
9. Demonstrate configuration of Firewall setting windows operating system. S23

6 Marks

1. Explain Policies, configuration & limitations of firewall. S22
2. Write a brief note on firewall configuration. State and explain 3 types of firewall configurations with a neat diagram. W22, 23
3. Define & explain. i) Circuit Gateway ii) Honey Pots iii) Application Gateway. S22
4. List types of firewalls and explain any one of them. W22
5. Describe the following i) Network based IDS ii) Packet Filter Firewall. Sample
6. Describe the DMZ with suitable example. Sample
7. State the features of the following IDS : (i) Network based IDS(ii) Host based IDS (iii) Honey pots. W23
8. Describe following terms : (i) Packet filter Firewall (ii) Application gateway (iii) Circuit gateway. S23
9. Describe network based IDS with suitable diagram. S23

Unit 5 – Network Security, Cyber Laws and Compliance Standards

2 Marks

1. Define AH & ESP with respect to IP security. S22
2. Classify following cyber crimes: i) Cyber terrorism against a government organization ii) Cyber-stalking iii) Copyright Infringement iv) Email harassment. S22, 23 Sample W23
3. State the meaning of hacking. W22
4. Explain use of PCI DSS. W22
5. Define AS, TGS with respect to Kerberos. Sample
6. List two protocols in IP Sec. State its function. W23

4 Marks

1. Explain Email security in SMTP. Describe working principle of SMTP. S22 W22 Sample
2. State the use of Digital Certificates. Describe the steps for digital certificate creation. W23
3. Describe PGP with suitable diagram. S23

6 Marks

1. Explain Public Key Infrastructure with example. S22
2. Explain the working of Kerberos. Explain Kerberos with help of suitable diagram. S22, 23 W22, 23
3. Explain IP sec security with help of diagram. W22
4. Describe COBIT framework with neat sketch. Sample S23
5. Describe following terms of intellectual property : i) Copyright ii) Patent iii) Trademark Sample.
6. Describe ITIL framework with different stages of life cycle. W23