Computer Networking: Security (CSE 3752)

Assignment – 1

Q.1. Name and explain the control categories (with suitable examples) that are essential to handle security issues in an organization.

Q.2. Briefly explain various control types with respect to security concern that help organizations to carry out the operations smoothly at their end.

Q.3. What is meant by CIA triad? Highlight its significance as a part of information security to work against cyber threat.

Q.4. State the importance of non-repudiation and discuss its key aspects briefly in digital communication environment.

Q.5. State the need of AAA protocol for remote access to the resources in computer network. Compare and contrast various AAA protocols used in a secured network.

Q.6. Differentiate between the role of control plane and data plane to ensure a zero trust cybersecurity.

Q.7. Explain the use of followings associated with deception and disruption technique to strengthen the security in computer networking.

(i) Honeypot (ii)Honeynet (iii)Honeyfile (iv)Honeytoken

Q.8. Briefly highlight the importance of the following to successfully execute the change management process for mitigating the potential disaster effect.

(i)Impact analysis (ii) Test results (iii) Back out plan (iv) Maintenance window

Q.9. Compare symmetric and asymmetric encryption (with the help of neat diagram), providing examples for each.

Q.10. With the help of suitable example elaborate how substitution cipher is different from transposition cipher.

Q.11. Encrypt the plaintext "TOMORROW" using the Playfair cipher with the key "SECRET". Assume the letter I & J shares the same cell in the key matrix.

Q.12. Consider a Playfair cipher with keyword “SECRET”. Decrypt “ENGNOHWSTEMEZY”, which was formed using this cipher.

Q.13. Encrypt the plaintext “EXAMINATION” using the keyword “KEY” with the help of vignere cipher.

Q.14. What will be the plain text corresponding to cipher text “DYRYVGKP” if Vigenere cipher is used with keyword as “KEY”?

Q.15. An 8 bit data $(AC)_{Hex}$ is permuted using the permutation table as Find the permutated output and the corresponding inverse permutation table which can be used to get the original 8 bit data.

7	3	1	5
6	4	8	2

Q.16. Given the output of round 16 in DES as “0x0000 0002 0000 0080”. Find the respective cipher text.

Q.17. How many S boxes are used in DES? Given the elements of the 2nd row (i.e. row no. “01”) in a S box used in DES as 14,4,13,1,2,15,11,8,3,10,6,12,5,9,0 & 7. If the 6 bits input to the S box is “011011”, determine the corresponding 4 bit output?

Q.18. Given the plaintext “SOA UNIVERSITY” to AES 128 bit algorithm. If the 128 bit key used for encryption as (02020202020202020202020202020202)Hex, then

a. Show the original contents of state array, displayed as a 4 X 4 matrix.

b. Show the value of state array after initial Add Round Key transformation.

c. Show the value of state array after SubBytes transformation.

d. Show the value of state array after ShiftRows transformation.

Q.19. What is meant by the term “hashing” in the field of cryptography? Justify, how hashing ensures both data integrity and password security.

Q.20. Discuss the role of blockchain as a modern technique to ensure a secured mode of data communication and recording highlighting the benefits of it.

Q.21. State the significance of Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP) associated with certificate validity process ensuring a secure interaction over internet.

Q.22. How does the level of resources and level of sophistication influence the threat actor?

Q.23. Briefly describe the following concepts considered as motivations to build defence against cyberthreats.

(i) Data Exfiltration (ii) Service Disruption (iii) Blackmail (iv) Revenge

Q.24. Define "supply chain" in the context of cybersecurity with a comparison among different parties involved in this and explain why it's important.

Q.25. Briefly explain the following techniques associated with attacks made using human psychology.

(i) Phishing (ii) Misinformation (iii) Brand impersonation (iv) Typosquatting