Computer Networking: Security (CSE 3752)

Assignment – 2

Q.1. Name and explain the possible vulnerabilities associated with user applications running in their computing systems when connected to internet.

Q.2. State, how the SQLI (Structured Query Language Injection) a common possible cyber-attack works to cause harm during web browsing. Also narrate the mitigation process to prevent such type of attack.

Q.3. List and define the flaws in cryptography process which may lead to a possible cryptographic vulnerability.

Q.4. Briefly explain the unwanted files/programs that are downloaded to a user system through internet access which later creates a malware attack.

Q.5. What is meant by DNS cache poisoning associated with DNS attack? Discuss briefly, how DNS sinkhole can be used to prevent DNS attack.

Q.6. Explain the following processes adopted by adversaries to launch an on-path attack in computer network.

(i) Session replay (ii) Message replay (iii) Credential replay (iv) Credential stuffing

Q.7. List and discuss briefly different types of segmentation techniques used in computer networking to reduce the impact of potential breach.

Q.8. Name the two key factors required to be executed to satisfy the goal of access control mechanism associated with security issue in computer networking. Also differentiate between a file System Acces Control List (ACL) and a network ACL being a part of access control mechanism.

Q.9. List and highlight the use of key elements for a multilayer strategy required to be implemented towards achieving effective network security.

Q.10. Discuss the major benefits of Infrastructure as Code (IaC).

Q.11. Explain briefly the micro-services as a secured architecture listing out the key benefits of it.

Q.12. Briefly explain the major security concerns associated with IoT devices.

Q.13. With the help of suitable diagram, explain the function of each of the four Supervisory Control and Data Acquisition (SCADA) system levels.

Q.14. What is meant by attack surface in a network scenario? Explore briefly the key aspects of attack surfaces need to be focused by a cyber-security professional.

Q.15. With the help of suitable examples highlight the attributes associated with different categories of devices in the context of infrastructure security.

Q.16. List and define the various data types considered as a regulated data required to be protected from security beach in organizations.

Q.17. Justify that data classification seems to be important in organizations for giving safeguards to various data types from security beach. Also mention the key classification types of data sets available in organizations.

Q.18. Explain the following methods that are meant for securing data from possible breaches during communication over a network.

(i) Geographic restriction (ii) Hashing (iii) Tokenization (iv) Obfuscation

Q.19. State the use of network load balancer that guarantees the availability of network to the host devices in a company even though the network carries high volume of traffic. Also differentiate the basic two load balancer configurations active/active and active/passive.

Q.20. Name and illustrate briefly the scheduling techniques used by the load balancer to distribute the workload.