CYBER SECURITY QUESTION BANK

SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

AN AUTONOMOUS INSTITUTION

Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

PART A

1. What is wiretapping?
2. What is replay attack?
3. Define the format of a WiFi Frame.
4. Expand and explain SSID
5. Explain Onion Routing
6. Expand and explain VPN
7. Define Firewall
8. Explain SIEM
9. Write some Advantages of Using Databases
10. List different types of Database Disclosure
11. List three characteristics of a Trusted system.
12. What is Digital Signature?
13. What is ROC Curve?
14. Define Reference Monitor.
15. What is CIA Triad?
16. List examples for Protected Objects.
17. Define Integrity and Confidentiality?
18. What Is Computer Security?
19. Define Trusted system with its characteristics.
20. Define Vulnerability and Trust.

PART B

1. Compare link and end-to-end encryption.
2. Explain the Strengths of WPA over WEP.
3. Explain different types of Firewalls.
4. Explain different Threats to Network Communications
5. What is Intrusion Detection System? Explain different types of IDS
6. Explain browser encryption and its types.
7. Explain Authentication based on biometrics is useful or not.
8. How Operating System Design is used to Protect Objects?
9. Explain different E-Mail attacks and methods to protect against E-Mail attacks.
10. Differentiate Symmetric and Asymmetric Cryptosystem
11. Explain different types of Threats?
12. What is Rootkit? Explain different Rootkits.
13. Explain how to choose a good password
14. Differentiate Block Cipher and Stream Cipher.
15. AES and DES

16. Operating system Design for self Protection
17. Explain Privacy Impacts of Emerging Technologies
18. Explain the concept of business continuity planning an Organization
19. Explain Precautions for Web Surfing
20. Explain how disaster affects Cyber Security

PART C

1. If the useful life of DES was about 20 years (1977–1999), how long do you predict the useful life of AES will be? Justify your answer.
2. Respond to the allegation “An operating system requires no protection for its executable code (in memory) because that code is a duplicate of code maintained on disk.”
3. If you forget your password for a website and you click [Forgot my password], sometimes the company sends you a new password by email but sometimes it sends you your old password by email. Compare these two cases in terms of vulnerability of the website owner..
4. Respond to the allegation “Rootkit is an attack package that attains root status.”
5. Respond to the allegation “WPA fixes many shortcomings of WEP by using stronger encryption; longer, changing keys; and secure integrity checks”
6. Can link and end-to-end encryption both be used on the same communication? What would be the advantage of that? Cite a situation in which both forms of encryption might be desirable.
7. One argument in the security community is that lack of diversity is itself a vulnerability. For example, the two dominant browsers, Mozilla Firefox and Microsoft Internet Explorer, are used by approximately 95 percent of Internet users. What security risk does this control of the market introduce? Explain your answer.
8. Do firewall rules have to be symmetric? That is, does a firewall have to block a particular traffic type both inbound (to the protected site) and outbound (from the site)? Why or why not?
9. Describe a situation in which the source of information is more sensitive than the information itself. Explain why the sum of sensitive data might also be sensitive.
10. Identify the three most probable threats to a computing system in an office with fewer than ten employees. That is, identify the three vulnerabilities most likely to be exploited. Estimate the number of times each vulnerability is exploited per year. Justify your estimate.
11. If you were supplying electronic voting machines for an election, what could you do to violate individuals’ privacy rights? That is, suggest some not readily apparent ways you could rig the machines to make it possible to determine after the election who had voted for which candidates.
12. When is an incident over? That is, what factors influence whether to continue the work of the incident handling team or to disband it?