SNS COLLEGE OF TECHNOLOGY

(Autonomous)

COIMBATORE – 35

DEPARTMENT OF COMPUTER SIENCE AND ENGINEERING (UG & PG)

Third Year Computer Science and Engineering, 5th Semester

Two Mark Question and Answer

Subject Code & Name : 19CSE304 - CYBER SECURITY

UNIT I – CYBER SCURITY FUNDAMENTALS

1. What is Security?

- "The quality or state of being secure--to be free from danger"
- To be protected from adversaries

2. Define Physical security

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

3.Define Personal Security

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

4. 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

5. What is the scope of computer security?

The scope of computer security grew from physical security to include:

a. Safety of the data

b. Limiting unauthorized access to that data

c. Involvement of personnel from multiple levels of the organization

6. What are the critical characteristics of information?

- Availability
- Accuracy
- Authenticity
- Confidentiality
- Integrity
- Utility
- Possession

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

- attacker sends a large number of connection or information requests to a target
- so many requests are made that the target system cannot handle them successfully along with other, legitimate requests for service
- may result in a system crash, or merely an inability to perform ordinary functions

8. Explain active and passive attack with example? Passive attack:

Monitoring the message during transmission. Eg: Interception

Active attack:

It involves the modification of data stream or creation of false data stream. E.g.: Fabrication, Modification, and Interruption

9. Define integrity and nonrepudiation? Integrity:

Service that ensures that only authorized person able to modify the message.

Nonrepudiation:

This service helps to prove that the person who denies the transaction is true or false.

10.Differentiate symmetric and asymmetric encryption?

Symmetric Asymmetric

It is a form of cryptosystem in which encryption and decryption performed using the same key.

It is a form of cryptosystem in which encryption and decryption

Performed using two keys.

Eg: DES, AES Eg: RSA, ECC

11. Define steganography

Hiding the message into some cover media. It conceals the existence of a message.

12. Why network need security?

When systems are connected through the network, attacks are possible during transmission time.

13. Define Encryption

The process of converting from plaintext to cipher text.

14. Specify the components of encryption algorithm.

- Plaintext
- Encryption algorithm
- secret key
- ciphertext
- Decryption algorithm

15. Define confidentiality and authentication

Confidentiality
It means how to maintain the secrecy of message. It ensures that the information in a computer system and transmitted information are accessible only for reading by authorised person.
Authentication
It helps to prove that the source entity only has involved the transaction.

16. Define cryptography.

It is a science of writing Secret code using mathematical techniques. The many schemes used for enciphering constitute the area of study known as cryptography.

17. Compare Substitution and Transposition techniques.

SUBSTITUTION TRANSPOSITION

*A substitution techniques is one in which the letters of plaintext are replaced by other letter or by number or symbols.
*Eg: Caeser cipher.
* It means,different kind of mapping is achieved by performing some sort of permutation on the plaintext letters.
*Eg: DES, AES.

18 .What are roles of public and private key?

The two keys used for public-key encryption are referred to as
The public key and the private key. Invariably, the private key is kept secret and the public key is known publicly. Usually the public key is used for encryption purpose and the private key is used in the decryption side.

19. Differentiate MAC and Hash function?

MAC: In Message Authentication Code, the secret key shared by sender and receiver. The MAC is appended to the message at the source at a time which the message is assumed or known to be correct.

Hash Function: The hash value is appended to the message at the source at time when the message is assumed or known to be correct. The hash function itself not considered to be secret.

20 . What are different types of IDSs?

- Network-based IDS
- Host-based IDS
- Application-based IDS
- Signature-based IDS
- Statistical Anomaly-Based ID

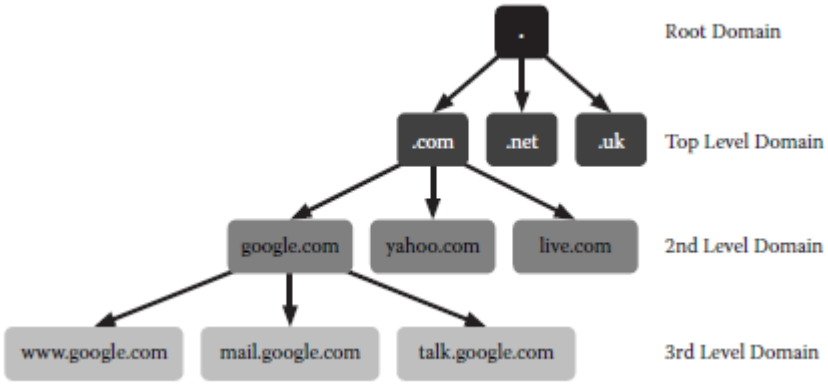
21. Explain RSA algorithm in detail with an example.

- Requirements
- Algorithm
- Example
- Computational Aspects
- Security of RSA

22. Define Domain Name System (DNS).

The DNS uses computers known as name servers to map domain names to the corresponding IP addresses using a database of records.DNS is a fundamental piece of the Internet architecture. Knowledge of how the DNS works is necessary to understand how attacks on the system can affect the Internet as a whole and how criminal infrastructure can take advantage of it.

24. Draw the hierarchical structure of the domain name system (DNS).



25. What's firewall?

Firewalls are network devices or software that separates one trusted network from an untrusted network

26. List the types of Firewall.

There are three basic types of firewall:

- Packet-filtering firewalls,
- stateful firewalls
- Application gateway firewalls.

27. What is Packet-Filtering Firewall?

The most rudimentary of firewalls is the packet-filtering firewall. Packet-filtering firewalls work at the IP level of the network. Most routers integrate this type of firewall to perform basic filtering of packets based on an IP address. The principle behind packet-filtering firewalls is that the firewall bases the decision to allow a packet from one network into another network solely on the IP address of the source and destination of the packet.

28. Define Stateful Firewall.

Simple packet-filtering firewalls suffer from one significant downside: they do not take into consideration the state of a connection, only the endpoints of the connection. Stateful firewalls allow only properly established connections to traverse the firewall's borders. While packet filtering is still a key element of these firewalls, the firewall also pays attention to the state of the connection.

29. Define Application Gateway Firewall

Application gateway firewalls, also known as proxies, are the most recent addition to the firewall family. These firewalls work in a similar manner to the stateful firewalls, but instead of only understanding the state of a TCP connection, these firewalls understand the protocol associated with a particular application or set of applications. A classic example of an application gateway firewall is a Web proxy or e-mail-filtering proxy.

30. Define Virtualization.

Virtualization Technology has advanced to the point that server consolidation through virtualization can help tame the cost of infrastructure deployment and operation by reducing the number of servers required to perform the same level of operational standards, given that

enterprises typically underutilize the full capacity available in physical servers. This section explores the history, concepts, and technologies of virtualization.

31. What is Radio-Frequency Identification (RFID)?

The term RFID does not describe one particular technology, but a group of technologies used for the purposes of identification using radio waves. RFID devices, commonly referred to as tags, are commonplace in everyday life. In RFID communication, there are two actors: the interrogator (reader) and the device (tag).

32. List the types of RFID?

These types include passive, battery-assisted passive, and active.

33. Define Proxy.

Proxies are useful to attackers in many ways. Most attackers use proxies to hide their IP address and, therefore, their true physi-cal location. In this way, attackers can conduct fraudulent financial transactions, launch attacks, or perform other actions with little risk.

34. What are the types of Proxies?

- TCP
- UDP

35. Define Tunneling

Tunneling data through other protocols often bypasses these controls and may allow sensitive data to exit the network and unwanted data to enter. It is even possible to extend all networks through these means without ever triggering an alert or log entry.

36. Find out the Fraud Techniques

Phishing, Smishing, Vishing, and Mobile Malicious Code

37. What are the Botnets ?

Systems connected to the Internet are at risk of infection from exposure to social-engineering attacks or vulnerability exploitation. Regardless of the infection vector, compromised machines can wait for commands from the attacker, which turns the system into a bot. A bot is a single node added to a network of other infected systems called a botnet.

38. Define Botmaster?

A botnet is a network of infected systems controlled by an administrator known as a botmaster. A botmaster controls many bots by issuing commands throughout the botnet infrastructure. The ability to run commands on many systems makes botnets practical for malware authors seeking a management solution and provides multiple capabilities.

39.What is cybersecurity?

Cybersecurity is the body of technologies, processes, and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

40. Why is cybersecurity important?

Listed below are the reasons why cybersecurity is so important in what's become a predominant digital world:

- With each passing year, the sheer volume of threats is increasing rapidly. According to the report by McAfee, cybercrime now stands at over $400 billion, while it was $250 billion two years ago.
- Cyber attacks can be extremely expensive for businesses to endure. In addition to financial damage suffered by the business, a data breach can also inflict untold reputational damage.
- Cyber-attacks these days are becoming progressively destructive. Cybercriminals are using more sophisticated ways to initiate cyber attacks.
- Regulations such as GDPR are forcing organizations into taking better care of the personal data they hold.

41. Who needs cyber security?

It is a mistake to believe that you are of no interest to cyber attackers. Everyone who is connected to the Internet needs cyber security. This is because most cyber attacks are automated and aim to exploit common vulnerabilities rather than specific websites or organisations.

42. List the types of cyber threats.

Common cyber threats include:

- Malware, such as ransomware, botnet software, RATs (remote access Trojans), rootkits and bootkits, spyware, Trojans, viruses, and worms.
- Backdoors, which allow remote access.
- Formjacking, which inserts malicious code into online forms.

- Cryptojacking, which installs illicit cryptocurrency mining software.
- DDoS (distributed denial-of-service) attacks, which flood servers, systems, and networks with traffic to knock them offline.
- DNS (domain name system) poisoning attacks, which compromise the DNS to redirect traffic to malicious sites.

43. Distinguish Cyber security & information security

Cyber security is often confused with information security.

- Cyber security focuses on protecting computer systems from unauthorised access or being otherwise damaged or made inaccessible.
- Information security is a broader category that protects all information assets, whether in hard copy or digital form.