1.What are hash algorithms?

hash algorithms are public functions that create a hash value, by converting variable-length messages into a single fixed-length value

2. What is the protocol for handling TCP traffic via a proxy server?

SOCKS

3. What does SHS stand for? What is it?

Secure Hash Standard (SHS) is a standard issued by the National Institute of Standards and Technology (NIST).

4. What are the disadvantages of the statistical anomaly-based approach?

these systems require much more overhead and processing capacity than signature-based IDPSs

5. What is cryptanalysis?

Cryptanalysis is the study and analysis of existing ciphers or encryption algorithms

6. What is public-key encryption based?

on a hash value

7. How many major processing-mode categories are firewalls categorized? What are they?

5. packet-filtering firewalls, application gateways, circuit gateways, MAC layer firewalls, and hybrid

8. How many NICs does the bastion host contain? What are they?

2. NICs (network interface cards)

9. How can firewalls be categorized?

by processing mode, development era, or structure

10. What does SPA stand for?

Stateful protocol analysis

11. Which attack does an attacker monitor packets from the network, modify them, and insert them back into the network?

Man in the middle attack

12.What do hackers use to engage in IP spoofing?

hackers use a variety of techniques to obtain trusted IP addresses, and then modify the packet headers to insert these forged addresses

13. What is an intrusion detection system?

is a device or software application that monitors a network or systems for malicious activity or policy violations

14.What are the weaknesses of the signature-based approach?

new attack strategies must be added into the IDPS’s database of signatures; otherwise, attacks use new strategies will not be recognized and might succeed

15.Which attack includes the execution of viruses, worms, Trojan horses, and active Web scripts with the intent to destroy or steal information.

malicious code attack

16.What common architectural implementations are mentioned in the text?

Packet-filtering routers, screened host firewalls, dual-homed firewalls, and screened subnet firewalls

17.What is phishing? What is its variant?

is an attempt to gain personal or financial information from an individual, usually by posing as a legitimate entity. A variant is spear phishing

18,What does DES, AES stand for?

DES (Data Encryption Standard), AES (Advanced Encryption Standard)

19.How many subsets of packet-filtering firewalls are mentioned in the text? What are they?

3. static filtering, dynamic filtering, and stateful inspection

20.What is a vulnerability?

is an identified weakness in a controlled system, where controls are not present or are no longer effective

21.Which attack can the cookie allow the designer to collect information on how to access password-protected sites?

timing attack

22.Which areas does information security include?

The broad areas of information security management, computer and data security, and network security

24.What can you use to protect the confidentiality of information?

Information classification, Secure document storage, Application of general security policies, Education of information custodians and end user

25.How many fundamental characteristics does information have? What are they? Translate into Vietnamese.

3. confidentiality, integrity, and availability

26.What is an information system?

It is the entire set of software, hardware, data, people, procedures, and networks that make possible the use of information resources in the organization

27.Give some information about DES

DES was developed in the early 1970s at IBM - was published as FIPS for the United States in 1977 - uses 16 round Feistel structure. The block size is 64-bit

28.What is security?

Security is “the quality or state of being secure to be free from danger

29.What is an attack?

An attack is an act that takes advantage of a vulnerability to compromise a controlled system.

30.How many critical characteristics of information did you learn? What are they?

7. vailability, accuracy, authenticity, confidentiality, integrity, utility, and possession

31.Give some information about AES?

AES is established by NIST in 2001 - is a variant of the Irondale block cipher - is much more secure than DES

32.What is modern cryptography heavily based on?

On mathematical theory and computer science practice

33,How are cryptographic algorithms designed?

around computational hardness assumptions, making such algorithms hard to break in practice by any adversary

34.What do you have to use if you want to encrypt information and decrypt information?

KEYS

35.How many components does an information system consist of? What are they?

6. They are network security, policy, computer & data, management of information security

36.How many types of attacks did you learn?

15. They are malicious code, Hoaxes, backdoors, password crack, brute force, dictionary, DoS – DDoS, Spoofing, man-in-the middle, spam, mail bombing, sniffers

37.What is decryption?

decryption is the process reversing unreadable information to readable