Mục lục

[1. Who was known as the founder of the Internet? What did he develop? 2](#_Toc131146490)

[2. DDoS attack định nghĩa 2](#_Toc131146491)

[3. Dictionary attack định nghĩa 2](#_Toc131146492)

[4. Password attack (cracking attack) định nghĩa 2](#_Toc131146493)

[5. Firewall định nghĩa, phân loại, generations, function of second generation 2](#_Toc131146494)

[6. IDS (2), IDPS detection method (3), security technology (7) 2](#_Toc131146495)

[7. Chức năng NIDS, có bao nhiêu loại (onl & off), so sánh các loại 3](#_Toc131146496)

[8. Hacker skills 3](#_Toc131146497)

[9. components of an information system (6). Tại sao dữ liệu là mục tiêu chính? 3](#_Toc131146498)

[10. How many critical characteristics does information have (7)? What are they? 3](#_Toc131146499)

[11. Attack là gì, có bao nhiêu loại, liệt kê các loại đã học? Why is a trap door hard to detect? 3](#_Toc131146500)

[12. DES, AES, tại sao AES ra đời, sự khác nhau DES&AES 4](#_Toc131146501)

[13. Mật mã hiện đại chủ yếu dựa vào gì, thuật toán mật mã được thiết kế như nào? 4](#_Toc131146502)

[14. What is Encryption & Decryption? Cần làm gì để Encryption & Decryption? 4](#_Toc131146503)

[15. What is security? What is information security? 5](#_Toc131146504)

[16. Khi nào thông tin cần được bảo mật, khi nào được coi là không chính xác, khi nào cần xác thực thông tin? 5](#_Toc131146505)

[17. Spam là gì? Hậu quả? Solution? 5](#_Toc131146506)

[18. Mục tiêu của mật mã? Miêu tả 1 trong số đó 5](#_Toc131146507)

[19. Sự khác nhau giữa sender, receiver, adversary 5](#_Toc131146508)

[20. What is the difference between MULTICS system and UNIX system? 6](#_Toc131146509)

[21. What is LaBrea? How does it work? 6](#_Toc131146510)

[22. Can an encryption scheme be broken? When and how? 6](#_Toc131146511)

[23. What do simple firewall models examine? 6](#_Toc131146512)

[24. What is the primary disadvantage of stateful inspection? 6](#_Toc131146513)

[25. Why do employees’ mistakes represent a serious threat to the confidentiality, integrity, and availability of data? 6](#_Toc131146514)

[26. Can human error or failure be prevented? How can it be protected? 6](#_Toc131146515)

# 1. Who was known as the founder of the Internet? What did he develop?

- Larry Roberts, known as the founder of the Internet, developed the project which was called ARPANET from its inception

# 2. DDoS attack định nghĩa

- Distributed denial-of-service (DDoS) is an attack in which a coordinated stream of requests is launched against a target from many locations at the same time.

# 3. Dictionary attack định nghĩa

- The dictionary attack is a variation of the brute force attack which narrows the field by selecting specific target accounts and using a list of commonly used passwords (the dictionary) instead of random combinations.

# 4. Password attack (cracking attack) định nghĩa

- Attempting to reverse-calculate a password is often called cracking.

- A cracking attack is a component of many dictionary attacks. It is used when a copy of the Security Account Manager (SAM) data file.

# 5. Firewall định nghĩa, phân loại, generations, function of second generation

- In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

- Firewalls can be categorized by processing mode, development era, or structure.

- First generation: Packet filters, second generation: Stateful filters, Third generation: Application layer

- The functions of stateful filters are maintaining knowledge of specific conversations between endpoints by remembering which port number the two IP addresses are using at layer 4 (transport layer) of the OSI model for their conversation, allowing examination of the overall exchange between the nodes.

# 6. IDS (2), IDPS detection method (3), security technology (7)

- An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations ( NIDS and HIDS)

- IDPSs use a variety of detection methods to monitor and evaluate network traffic.

- Three methods dominate: the signature-based approach, the statistical-anomaly approach, and the stateful packet inspection approach.

- IDS, IPS, honeypots, honeynets, padded cell system, trap and trace system, active intrusion prevention system

# 7. Chức năng NIDS, có bao nhiêu loại (onl & off), so sánh các loại

- NIDS performs an analysis of passing traffic on the entire subnet, and matches the traffic that is passed on the subnets to the library of known attacks. Once an attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator.

- On-line NIDS deals with the network in real time. It analyses the Ethernet packets and applies some rules to decide if it is an attack or not.

- Off-line NIDS deals with stored data and passes it through some processes to decide if it is an attack or not.

# 8. Hacker skills

- The first is the expert hacker, or elite hacker, who develops software scripts and program exploits used by those in the second category, the novice or unskilled hacker. The expert hacker is usually a master of several programming languages, networking protocols, and operating systems and also exhibits a mastery of the technical environment of the chosen targeted system.

# 9. components of an information system (6). Tại sao dữ liệu là mục tiêu chính?

- Software, hardware, data, people, procedures, networks.

- Data is often the most valuable asset possessed by an organization so that it is the main target of intentional attacks

# 10. How many critical characteristics does information have (7)? What are they?

- Authenticity, Availability, accuracy, utility, possesion, confidentiality, integrity.

# 11. Attack là gì, có bao nhiêu loại, liệt kê các loại đã học? Why is a trap door hard to detect?

*- Attack*: An intentional or unintentional act that can cause damage to or otherwise compromise information and/or the systems that support it.

- Attacks can be active or passive, intentional or unintentional, and direct or indirect. -> 6 types of attack.

- Malicious Code, Hoaxes, Back Doors, Password crack, Brute Force, Dictionary, Denial –of –Service(DoS) and Distributed, DdoS, Spoofing, Spam, Mail Bombing, Man- in- the –Middle, Sniffers, Social Engineering, Phising, Pharming, Timing Attack

- A trap door is hard to detect, because very often the programmer who puts it in place also makes the access exempt from the usual audit logging features of the system.

# 12. DES, AES, tại sao AES ra đời, sự khác nhau DES&AES

- [DES is a symmetric-key algorithm for the encryption of digital data](https://en.wikipedia.org/wiki/Data_Encryption_Standard), which was developed by IBM and is based on the company’s Lucifer algorithm, which uses a key length of 128 bits. As implemented, DES uses a 64-bit block size and a 56-bit  
key.

- AES is a federal information processing standard (FIPS) that specifies a cryptographic algorithm used within the U.S. government to protect information in federal agencies that are not a part of the national defense infrastructure. – 26/02/2002

- AES has been developed to replace both DES and 3DES

- DES uses a key length of 128 bits, uses a 64-bit block size and a 56-bit key while AES implements a block cipher called the Rijndael Block Cipher with a variable block length and a key length of 128, 192, or 256 bits.

# 13. Mật mã hiện đại chủ yếu dựa vào gì, thuật toán mật mã được thiết kế như nào?

- Modern cryptography is heavily based on mathematical theory and computer science practice;

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

# 14. What is Encryption & Decryption? Cần làm gì để Encryption & Decryption?

- The process of making the information unreadable is called encryption or enciphering.

- Reversing this process and retrieving the original readable information is called decryption or deciphering.

- You can use security tools, or encryption & decryption algorithms

# 15. What is security? What is information security?

- Security is “the quality or state of being secure to be free from danger.”. In other words, protection against adversaries from those who would do harm, intentionally or otherwise is the objective.

- Information security as the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information

# 16. Khi nào thông tin cần được bảo mật, khi nào được coi là không chính xác, khi nào cần xác thực thông tin?

- Information need to be secured when it’s sensitive or confidential.

- The information that is considered inaccurate may have been intentionally or unintentionally modified.

- When it is in the same state in which it was created, placed, stored, or transferred.

# 17. Spam là gì? Hậu quả? Solution?

- Spam is unsolicited commercial e-mail.

- The most significant consequence of spam, however, is the waste of computer and human resources.

-Many organizations attempt to cope with the flood of spam by using e-mail filtering technologies. Other organizations simply tell the users of the mail system to delete unwanted messages.

# 18. Mục tiêu của mật mã? Miêu tả 1 trong số đó

- Cryptography goals: Confidentiality, Data integrity, Authentication, non-reputation.

*- Data integrity* is a service which addresses the unauthorized alteration of data. To assure data integrity, one must have the ability to detect data manipulation by unauthorized parties

# 19. Sự khác nhau giữa sender, receiver, adversary

- A *sender* is an entity in a two-party communication which is the legitimate transmitter of information.

- A r*eceiver* is an entity in a two-party communication which is the intended recipient of information.   
- An *adversary* is an entity in a two-party communication which is neither the sender nor receiver, and which tries to defeat the information security service being provided between the sender and receiver

# 20. What is the difference between MULTICS system and UNIX system?

- While the MULTICS system implemented multiple security levels and passwords , the UNIX system did not.

- Multiplexed Information and Computing Service (MULTICS)

# 21. What is LaBrea? How does it work?

- One tool that provides active intrusion prevention is known as LaBrea.

-LaBrea is a “sticky” honeypot and IDPS and works by taking up the unused IP address space within a network.

# 22. Can an encryption scheme be broken? When and how?

Yes, it can. By trying all possible keys to see which one the communicating parties are using

# 23. What do simple firewall models examine?

Two aspects of the packet header : the destination and source address.

# 24. What is the primary disadvantage of stateful inspection?

Is the additional processing required to manage and verify packets against the state table

# 25. Why do employees’ mistakes represent a serious threat to the confidentiality, integrity, and availability of data?

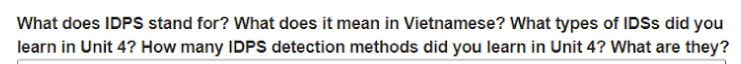
- Because employees use data in everyday activities to conduct the organization’s business .

# 26. Can human error or failure be prevented? How can it be protected?

- Yes. It can be prevented with training and on going awareness activities, but also with controls, ranging from simple procedures, such as requiring the user to type a critical command twice, to more complex procedures, such as the verification of command by a second party .

Câu 1. 7. - IDS, IPS, honeypots, honeynets, padded cell system, trap and trace system, active intrusion prevention system

(Hệ thống phát hiện xâm nhập , Hệ thống ngăn chặn xâm nhập , Hệ thống mồi nhử, hệ thống bẫy mật,Hệ thống bộ đệm,bẫy và hệ thống theo dõi,Hệ thống ngăn chặn xâm nhập chủ động )

Câu 2. Intrution detection and Prevention System (Hệ thống phát hiện và ngăn chặn xâm nhập )

This alarm can be audible and/or visual (producing noise and lights, respectively), or it can be silent (an e-mail message or pager alert).

Three methods dominate: the signature-based approach, the statistical-anomaly approach, and the stateful packet inspection approach. (IDPS)

Câu 3. - Larry Roberts, known as the founder of the Internet, developed the project which was called ARPANET from its inception

Câu 4.



Ronald Rivest, Adi Shamir, and Leonard Adleman developed a practical public-key cipher for both confidentiality and digital signatures; . They invented RSA algorithms which are based on the problem of factorization of large prime.

Câu 5 . 

A cryptographic hash function is an algorithm that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that any (accidental or intentional) change to the data will change

Cryptographic hash functions have many information security applications, notably in digital signatures, message authentication codes (MACs), and other forms of authentication.

Câu 6 . 

Advanced Encryption Standard.

AES is a federal information processing standard (FIPS) that specifies a cryptographic algorithm used within the U.S. government to protect information in federal agencies that are not a part of the national defense infrastructure



- The process of making the information unreadable is called encryption or enciphering.

- Reversing this process and retrieving the original readable information is called decryption or deciphering.

- You can use security tools, or encryption & decryption algorithms



*- Attack*: An intentional or unintentional act that can cause damage to or otherwise compromise information and/or the systems that support it.

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

Chúng là mã độc, Trò lừa bịp, cửa hậu, bẻ khóa mật khẩu,tấn công vũ phu,tấn công từ điển, tấn công từ chối dịch vụ, Giả mạo, tấn công trung gian, thư rác, đánh bom thư, trình thám thính, Kỹ thuật xã hội, Pharming, Tấn công thời gian

1.Why are hash functions used in password verification systems to confirm the identity of the user?

A. Because hash functions are mathematical algorithms.

B. Because hash functions are one-way.

C. Because hash functions are publish functions.

D. Because hash functions don’t require the use of key.

2. Which of the following attacks that can, in theory, be used to attempt to decrypt any encrypted data? A. A brute-force attack B. dictionary attack C. A&B are correct D. Man-in the middle attack

3. By taking ………… of a security weakness a bank consultant can order millions of dollars to be transferred by wire to his own account.

A. advantage C. position B. a flier D. opportunity

4. Unfortunately, most information systems are built on hardware platforms that cannot guarantee any level of information security if unrestricted access to the hardware is possible.

A. designed/make sure C.make sure/design

B. ensure/design D. implemented/certain

5. …………. of the IS comprises applications, operating systems, and assorted command

utilities.

A. The software component C. The network component

B. The hardware component D. A&C are correct

6. ………………….. is the quality or state of ownership or control.

A. The utility of information

B. The availability of information

C. The confidentiality of information

D. The possession of information

7. The ………………. is the quality or state of having value for some purpose or end.

A. integrity C. availability B. utility of information D. A&B are correct

8. In information security, ................ exists when a vulnerability known to an

attacker is present.

A. safeguard C. risk

B. exposure D. security posture

9. Network security was referred to as network insecurity............... the range and frequency of computer security violations and the explosion in the numbers of hosts and users on ARPANET.

A. Because of C. Therefore

B. However D. Although

10. Which of the followings has the highest level of security?

A. DES B. Triple DES

C. AES D. RSA

11. Which of the followings is one of the first block ciphers?

A. Caesar cipher B.Wheel cipher

C.Lucifer cipher D.Vigenère cipher

12. ……………………….. , 1s a multilayered system that protects the sovereignty of a

state, its assets, its resources, and its people.

A. Personnel security C. Network security

B. National security D. Physical security

13. ……………. is a category of objects, persons, or other entities that presents a

danger to an asset.

A. Threat C. Risk

B. Security posture D. Vulnerability

14. …………. is a service which prevents an entity from denying previous

commitments or actions.

A. Non-repudiation B. Authentication

C. Data integrity D. Confidentiality