An toan thong tin_ Nhom 11

Bắt đầu vào lúc	Sunday, 26 November 2023, 8:37 PM
Trạng thái	Đã xong
Kết thúc lúc	Sunday, 26 November 2023, 8:37 PM
Thời gian thực hiện	28 giây
Điểm	3,00/62,00
Điểm	**0,48** trên 10,00 (**5**%)

Câu hỏi 1

Sai

Đạt điểm 0,00 trên 1,00

Joe, the Chief Technical Officer (CTO), is concerned about new malware being introduced into the corporate network. He has tasked the security engineers to implement a technology that is capable of alerting the team when unusual traffic is on the network. Which of the following types of technologies will BEST address this scenario?

Select one:

- a. Anomaly Based IDS
- b. Proxy Firewall
- c. Application Firewall ✖
- d. Signature IDS

Your answer is incorrect.

The correct answer is: Anomaly Based IDS

Câu hỏi 2

Đúng

Đạt điểm 1,00 trên 1,00

An employee reports work was being completed on a company-owned laptop using a public wireless hot-spot. A pop-up screen appeared, and the user closed the pop-up. Seconds later, the desktop background was changed to the image of a padlock with a message demanding immediate payment to recover the data. Which of the following types of malware MOST likely caused this issue?

Select one:

- a. Scareware
- b. Spyware
- c. Ransomware ✔
- d. Rootkit

Your answer is correct.

The correct answer is: Ransomware

Câu hỏi 3

Đúng

Đạt điểm 1,00 trên 1,00

A rouge wireless access point is created with the same SSID as the corporate SSID.
The attacker has employees connect to the SSID and watches the information as it's relayed to the original SSID. What type of attack is described here?

Select one:

- a. Compromised key attack
- b. Sniffer attack
- c. Man in the middle attack ✔
- d. Smurf attack

Your answer is correct.

The correct answer is: Man in the middle attack

Câu hỏi 4

Sai

Đạt điểm 0,00 trên 1,00

Which of the following should the security administrator implement to limit web traffic based on country of origin? (Select THREE).

Select one or more:

- a. NIDS
- b. Proxies
- c. Antivirus
- d. Spam filter
- e. Load balancer ✖
- f. Firewall
- g. URL filtering

Your answer is incorrect.

The correct answers are: Proxies, Firewall, URL filtering

Câu hỏi 5

Đúng

Đạt điểm 1,00 trên 1,00

Which method would prevent tampering of data in transit?

Select one:

- a. Encryption of the data
- b. Spoofing mitigation
- c. Secure Sockets Layer ✔ Secure Sockets Layer (SSL) communications offer both encryption and authentication of the data via certificate signing. This would prevent tampering of the data end to end
- d. Access control lists

Your answer is correct.

The correct answer is: Secure Sockets Layer

Câu hỏi 6

Không trả lời

Đạt điểm 1,00

Which of the following security architecture elements also has sniffer functionality? (Select TWO).

Select one or more:

- a. HSM
- b. IDS
- c. IPS
- d. WAP
- e. SSL accelerator

Your answer is incorrect.

The correct answers are: IPS, IDS

Câu hỏi 7

Không trả lời

Đạt điểm 1,00

Several employees clicked on a link in a malicious message that bypassed the spam filter and their PCs were infected with malware as a result. Which of the following BEST prevents this situation from occurring in the future?

Select one:

- a. Data loss prevention
- b. Enforcing complex passwords
- c. Digital signatures
- d. Security awareness training

Your answer is incorrect.

The correct answer is: Security awareness training

Câu hỏi 8

Không trả lời

Đạt điểm 1,00

A distributed denial of service attack can BEST be described as:

Select one:

- a. Users attempting to input random or invalid data into fields within a web browser application.
- b. Multiple computers attacking a single target in an organized attempt to deplete its resources.
- c. Invalid characters being entered into a field in a database application.
- d. Multiple attackers attempting to gain elevated privileges on a target system.

Your answer is incorrect.

The correct answer is: Multiple computers attacking a single target in an organized attempt to deplete its resources.

Câu hỏi 9

Không trả lời

Đạt điểm 1,00

By default, which of the following uses TCP port 22? (Select THREE).

Select one or more:

- a. HTTPS
- b. SCP
- c. TLS
- d. STELNET
- e. SSH
- f. FTPS
- g. SSL
- h. SFTP

Your answer is incorrect.

The correct answers are: SCP, SSH, SFTP

Câu hỏi 10

Không trả lời

Đạt điểm 1,00

What is the most commonly used technique to protect against virus attacks?

Select one:

a. Automated reconstruction

b. Signature detection

c. Data integrity assurance

d. Heuristic detection

Your answer is incorrect.

The correct answer is: Signature detection

Câu hỏi 11

Không trả lời

Đạt điểm 1,00

Joe has hired several new security administrators and have been explaining the design of the company's network. He has described the position and descriptions of the company's firewalls, IDS sensors, antivirus server, DMZs, and HIPS. Which of the following best describes the incorporation of these elements?

Select one:

a. UTM security appliance

b. Load balancers

c. Defense in depth

d. Network segmentation

Your answer is incorrect.

The correct answer is: Defense in depth

Câu hỏi 12

Không trả lời

Đạt điểm 1,00

Ann, a security technician, is reviewing the IDS log files. She notices a large number of alerts for multicast packets from the switches on the network. After investigation, she discovers that this is normal activity for her network. Which of the following BEST describes these results?

Select one:

- a. False negatives
- b. True negatives
- c. False positives
- d. True positives

Your answer is incorrect.

The correct answer is: False positives

Câu hỏi 13

Không trả lời

Đạt điểm 1,00

The finance department just procured a software application that needs to communicate back to the vendor server via SSL. Which of the following default ports on the firewall must the security engineer open to accomplish this task?

Select one:

- a. 3389
- b. 443
- c. 80
- d. 130

Your answer is incorrect.

The correct answer is: 443

Câu hỏi 14

Không trả lời

Đạt điểm 1,00

Timestamps and sequence numbers act as countermeasures against which of the following types of attacks?

Select one:

- a. DoS
- b. Replay
- c. Vishing
- d. Smurf

Your answer is incorrect.

The correct answer is: Replay

Câu hỏi 15

Không trả lời

Đạt điểm 1,00

Which type of device can prevent an intrusion on your network?

Select one:

- a. IDS
- b. HIDS
- c. IPS
- d. Honey pots

Your answer is incorrect.

The correct answer is: IPS

Câu hỏi 16

Không trả lời

Đạt điểm 1,00

Sara, a user, downloads a keygen to install pirated software. After running the keygen, system performance is extremely slow and numerous antivirus alerts are displayed. Which of the following BEST describes this type of malware?

Select one:

- a. Trojan
- b. Worm
- c. Logic bomb
- d. Adware

Your answer is incorrect.

The correct answer is: Trojan

Câu hỏi 17

Không trả lời

Đạt điểm 1,00

Although a vulnerability scan report shows no vulnerabilities have been discovered, a subsequent penetration test reveals vulnerabilities on the network. Which of the following has been reported by the vulnerability scan?

Select one:

- a. Passive scan
- b. False negative
- c. Active scan
- d. False positive

Your answer is incorrect.

The correct answer is: False negative

Câu hỏi 18

Không trả lời

Đạt điểm 1,00

A Windows- based computer is infected with malware and is running too slowly to boot and run a malware scanner. Which of the following is the BEST way to run the malware scanner?

Select one:

- a. Disable the network connection
- b. Kill all system processes
- c. Enable the firewall
- d. Boot from CD/USB

Your answer is incorrect.

The correct answer is: Boot from CD/USB

Câu hỏi 19

Không trả lời

Đạt điểm 1,00

A company replaces a number of devices with a mobile appliance, combining several functions. Which of the following descriptions fits this new implementation? (Select TWO).

Select one or more:

- a. Cloud computing
- b. All-in-one device
- c. Load balancing
- d. Single point of failure
- e. Virtualization

Your answer is incorrect.

The correct answers are: All-in-one device, Single point of failure

Câu hỏi 20

Không trả lời

Đạt điểm 1,00

When dealing with firewalls, the term trusted network is used to describe what?

Select one:

a. The DMZ

b. Internal network

c. A network with SSL

d. The Internet

Your answer is incorrect.

The correct answer is: Internal network

Câu hỏi 21

Không trả lời

Đạt điểm 1,00

Which of the following would a security administrator implement in order to discover comprehensive security threats on a network?

Select one:

a. Vulnerability scan

b. Design reviews

c. Code review

d. Baseline reporting

Your answer is incorrect.

The correct answer is: Vulnerability scan

Câu hỏi 22

Không trả lời

Đạt điểm 1,00

Which of the following types of application attacks would be used to identify malware causing security breaches that have NOT yet been identified by any trusted sources?

Select one:

- a. Zero-day
- b. LDAP injection
- c. XML injection
- d. Directory traversal

Your answer is incorrect.

The correct answer is: Zero-day

Câu hỏi 23

Không trả lời

Đạt điểm 1,00

It is MOST important to make sure that the firewall is configured to do which of the following?

Select one:

- a. Deny all traffic and only permit by exception.
- b. Deny all traffic based on known signatures.
- c. Alert the administrator of a possible intrusion.
- d. Alert management of a possible intrusion.

Your answer is incorrect.

The correct answer is: Deny all traffic and only permit by exception.

Câu hỏi 24

Không trả lời

Đạt điểm 1,00

A security administrator wants to block unauthorized access to a web server using a locally installed software program. Which of the following should the administrator deploy?

Select one:

- a. HIPS
- b. NIDS
- c. NIPS
- d. HIDS

Your answer is incorrect.

The correct answer is: HIPS

Câu hỏi 25

Không trả lời

Đạt điểm 1,00

Which of the following software allows a network administrator to inspect the protocol header in order to troubleshoot network issues?

Select one:

- a. Packet sniffer
- b. Switch
- c. Spam filter
- d. URL filter

Your answer is incorrect.

The correct answer is: Packet sniffer

Câu hỏi 26

Không trả lời

Đạt điểm 1,00

Which of the following design components is used to isolate network devices such as web servers?

Select one:

- a. NAT
- b. VPN
- c. VLAN
- d. DMZ

Your answer is incorrect.

The correct answer is: DMZ

Câu hỏi 27

Không trả lời

Đạt điểm 1,00

During a server audit, a security administrator does not notice abnormal activity. However, a network security analyst notices connections to unauthorized ports from outside the corporate network. Using specialized tools, the network security analyst also notices hidden processes running. Which of the following has MOST likely been installed on the server?

Select one:

- a. Backdoor
- b. Rootkit
- c. Logic bomb
- d. SPIM

Your answer is incorrect.

The correct answer is: Rootkit

Câu hỏi 28

Không trả lời

Đạt điểm 1,00

Which is a common attack method used to overwhelm services from traffic from multiple Internet sources?

Select one:

a. Distributed denial of service

b. Denial of service

c. IP address spoofing

d. Session hijacking

Your answer is incorrect.

The correct answer is: Distributed denial of service

Câu hỏi 29

Không trả lời

Đạt điểm 1,00

Which of the following should be deployed to prevent the transmission of malicious traffic between virtual machines hosted on a singular physical device on a network?

Select one:

a. NIPS on the network

b. HIDS on each virtual machine

c. HIPS on each virtual machine

d. NIDS on the network

Your answer is incorrect.

The correct answer is: HIPS on each virtual machine

Câu hỏi 30

Không trả lời

Đạt điểm 1,00

Pete, the system administrator, has blocked users from accessing social media web sites. In addition to protecting company information from being accidentally leaked, which additional security benefit does this provide?

Select one:

- a. Protection against malware introduced by banner ads
- b. No competition with the company's official social presence
- c. Increased user productivity based upon fewer distractions
- d. Elimination of risks caused by unauthorized P2P file sharing

Your answer is incorrect.

The correct answer is: Protection against malware introduced by banner ads

Câu hỏi 31

Không trả lời

Đạt điểm 1,00

Which statement is TRUE about the operation of a packet sniffer?

Select one:

- a. It can only have one interface on a management network.
- b. The Ethernet card must be placed in promiscuous mode
- c. They are required for firewall operation and stateful inspection.
- d. It must be placed on a single virtual LAN interface.

Your answer is incorrect.

The correct answer is: The Ethernet card must be placed in promiscuous mode

Câu hỏi 32

Không trả lời

Đạt điểm 1,00

A firewall technician has been instructed to disable all non-secure ports on a corporate firewall. The technician has blocked traffic on port 21, 69, 80, and 137-139. The technician has allowed traffic on ports 22 and 443. Which of the following correctly lists the protocols blocked and allowed?

Select one:

- a. Blocked: SFTP, TFTP, HTTP, NetBIOS; Allowed: SSH, SCP, HTTPS
- b. Blocked: FTP, HTTP, HTTPS; Allowed: SFTP, SSH, SCP, NetBIOS
- c. Blocked: TFTP, HTTP, NetBIOS; Allowed: HTTPS, FTP
- d. Blocked: FTP, TFTP, HTTP, NetBIOS; Allowed: SFTP, SSH, SCP, HTTPS

Your answer is incorrect.

The correct answer is: Blocked: FTP, TFTP, HTTP, NetBIOS; Allowed: SFTP, SSH, SCP, HTTPS

Câu hỏi 33

Không trả lời

Đạt điểm 1,00

A trojan was recently discovered on a server. There are now concerns that there has been a security breach that allows unauthorized people to access data. The administrator should be looking for the presence of a/an:

Select one:

- a. Backdoor
- b. Adware application
- c. Logic bomb
- d. Rootkit

Your answer is incorrect.

The correct answer is: Backdoor

Câu hỏi 34

Không trả lời

Đạt điểm 1,00

Users have reported receiving unsolicited emails in their inboxes, often times with malicious links embedded. Which of the following should be implemented in order to redirect these messages?

Select one:

- a. Spam filter
- b. Application firewall
- c. Proxy server
- d. Network firewall

Your answer is incorrect.

The correct answer is: Spam filter

Câu hỏi 35

Không trả lời

Đạt điểm 1,00

Which of the following attacks is generally initiated from a botnet?

Select one:

- a. Distributed denial of service
- b. A war driving attack
- c. HTTP header injection
- d. Cross site scripting attack

Your answer is incorrect.

The correct answer is: Distributed denial of service

Câu hỏi 36

Không trả lời

Đạt điểm 1,00

A chief Financial Officer (CFO) has asked the Chief Information Officer (CISO) to provide responses to a recent audit report detailing deficiencies in the organization security controls. The CFO would like to know ways in which the organization can improve its authorization controls. Given the request by the CFO, which of the following controls should the CISO focus on in the report? (Select Three)

Select one or more:

- a. Single sign-on
- b. Biometric systems
- c. Password complexity policies
- d. Multifactor authentication
- e. Hardware tokens
- f. Lease privilege
- g. Role-based permissions
- h. One time passwords
- i. Separation of duties

Your answer is incorrect.

The correct answers are: Role-based permissions, Separation of duties, Lease privilege

Câu hỏi 37

Không trả lời

Đạt điểm 1,00

Which of the following devices would MOST likely have a DMZ interface?

Select one:

- a. Load balancer
- b. Proxy
- c. Firewall
- d. Switch

Your answer is incorrect.

The correct answer is: Firewall

Câu hỏi 38

Không trả lời

Đạt điểm 1,00

A program has been discovered that infects a critical Windows system executable and stays dormant in memory. When a Windows mobile phone is connected to the host, the program infects the phone's boot loader and continues to target additional Windows PCs or phones. Which of the following malware categories BEST describes this program?

Select one:

- a. Trojan
- b. Virus
- c. Rootkit
- d. Zero-day

Your answer is incorrect.

The correct answer is: Virus

Câu hỏi 39

Không trả lời

Đạt điểm 1,00

Which attack can be used on a native VLAN?

Select one:

- a. Trunk popping
- b. Denial of service
- c. VLAN traversal
- d. Double tagging

Your answer is incorrect.

The correct answer is: Double tagging

Câu hỏi 40

Không trả lời

Đạt điểm 1,00

The security administrator is observing unusual network behavior from a workstation. The workstation is communicating with a known malicious destination over an encrypted tunnel. A full antivirus scan, with an updated antivirus definition file, does not show any signs of infection. Which of the following has happened on the workstation?

Select one:

- a. Zero-day attack
- b. Known malware infection
- c. Session hijacking
- d. Cookie stealing

Your answer is incorrect.

The correct answer is: Zero-day attack

Câu hỏi 41

Không trả lời

Đạt điểm 1,00

Which of the following types of malware, attempts to circumvent malware detection by trying to hide its true location on the infected system?

Select one:

- a. Ransomware
- b. Armored virus
- c. Trojan
- d. Keylogger

Your answer is incorrect.

The correct answer is: Trojan

Câu hỏi 42

Không trả lời

Đạt điểm 1,00

Which of the following firewall rules only denies DNS zone transfers?

Select one:

- a. deny all dns packets
- b. deny ip any any
- c. deny tcp any any port 53
- d. deny udp any any port 53

Your answer is incorrect.

The correct answer is: deny tcp any any port 53

Câu hỏi 43

Không trả lời

Đạt điểm 1,00

The network security engineer just deployed an IDS on the network, but the Chief Technical Officer (CTO) has concerns that the device is only able to detect known anomalies. Which of the following types of IDS has been deployed?

Select one:

- a. Anomaly Based IDS
- b. Behavior Based IDS
- c. Heuristic IDS
- d. Signature Based IDS

Your answer is incorrect.

The correct answer is: Signature Based IDS

Câu hỏi 44

Không trả lời

Đạt điểm 1,00

An organization recently switched from a cloud-based email solution to an in-house email server. The firewall needs to be modified to allow for sending and receiving email. Which of the following ports should be open on the firewall to allow for email traffic? (Select THREE).

Select one or more:

- a. TCP 22
- b. TCP 143
- c. TCP 23
- d. TCP 110
- e. TCP 53
- f. TCP 25
- g. TCP 445

Your answer is incorrect.

The correct answers are: TCP 25, TCP 110, TCP 143

Câu hỏi 45

Không trả lời

Đạt điểm 1,00

A security administrator needs to implement a system that detects possible intrusions based upon a vendor provided list. Which of the following BEST describes this type of IDS?

Select one:

- a. Signature based
- b. Anomaly-based
- c. Behavior-based
- d. Heuristic

Your answer is incorrect.

The correct answer is: Signature based

Câu hỏi 46

Không trả lời

Đạt điểm 1,00

After surfing the Internet, Joe, a user, woke up to find all his files were corrupted. His wallpaper was replaced by a message stating the files were encrypted and he needed to transfer money to a foreign country to recover them. Joe is a victim of:

Select one:

- a. a keylogger
- b. spyware
- c. ransomware
- d. a logic bomb

Your answer is incorrect.

The correct answer is: ransomware

Câu hỏi 47

Không trả lời

Đạt điểm 1,00

Which of the following can Joe, a security administrator, implement on his network to capture attack details that are occurring while also protecting his production network?

Select one:

- a. Security logs
- b. Protocol analyzer
- c. Honeypot
- d. Audit logs

Your answer is incorrect.

The correct answer is: Honeypot

Câu hỏi 48

Không trả lời

Đạt điểm 1,00

A system administrator has noticed network performance issues and wants to gather performance data from the gateway router. Which of the following can be used to perform this action?

Select one:

- a. SMTP
- b. IPSec
- c. iSCSI
- d. SNMP

Your answer is incorrect.

The correct answer is: SNMP

Câu hỏi 49

Không trả lời

Đạt điểm 1,00

Which of the following would the security engineer set as the subnet mask for the servers below to utilize host addresses on separate broadcast domains?
Server 1: 192.168.100.6
Server 2: 192.168.100.9
Server 3: 192.169.100.20

Select one:

- a. /24
- b. /27
- c. /29
- d. /28
- e. /30

Your answer is incorrect.

The correct answer is: /29

Câu hỏi 50

Không trả lời

Đạt điểm 1,00

Which the following flags are used to establish a TCP connection? (Select TWO).

Select one or more:

- a. ACK
- b. FIN
- c. PSH
- d. SYN
- e. URG

Your answer is incorrect.

The correct answers are: ACK, SYN

Câu hỏi 51

Không trả lời

Đạt điểm 1,00

Which of the following BEST describes a demilitarized zone?

Select one:

- a. A network where all servers exist and are monitored.
- b. A sterile, isolated network segment with access lists.
- c. A private network that is protected by a firewall and a VLAN.
- d. A buffer zone between protected and unprotected networks.

Your answer is incorrect.

The correct answer is: A buffer zone between protected and unprotected networks.

Câu hỏi 52

Không trả lời

Đạt điểm 1,00

Which of the following will help prevent smurf attacks?

Select one:

- a. Allowing necessary UDP packets in and out of the network
- b. Flash the BIOS with the latest firmware
- c. Disabling unused services on the gateway firewall
- d. Disabling directed broadcast on border routers

Your answer is incorrect.

The correct answer is: Disabling directed broadcast on border routers

Câu hỏi 53

Không trả lời

Đạt điểm 1,00

A network administrator has purchased two devices that will act as failovers for each other. Which of the following concepts does this BEST illustrate?

Select one:

- a. Availability
- b. Integrity
- c. Authentication
- d. Confidentiality

Your answer is incorrect.

The correct answer is: Availability

Câu hỏi 54

Không trả lời

Đạt điểm 1,00

A user casually browsing the Internet is redirected to a warez site where a number of pop-ups appear. After clicking on a pop-up to complete a survey, a drive-by download occurs. Which of the following is MOST likely to be contained in the download?

Select one:

- a. Spyware
- b. Backdoor
- c. DDoS
- d. Smurf
- e. Logic bomb

Your answer is incorrect.

The correct answer is: Spyware

Câu hỏi 55

Không trả lời

Đạt điểm 1,00

A company wants to prevent end users from plugging unapproved smartphones into PCs and transferring data. Which of the following would be the BEST control to implement?

Select one:

- a. IDS
- b. DLP
- c. MDM
- d. HIPS

Your answer is incorrect.

The correct answer is: DLP

Câu hỏi 56

Không trả lời

Đạt điểm 1,00

The Chief Information Officer (CIO) receives an anonymous threatening message that says “beware of the 1st of the year”. The CIO suspects the message may be from a former disgruntled employee planning an attack. Which of the following should the CIO be concerned with?

Select one:

- a. Smurf Attack
- b. Logic bomb
- c. Trojan
- d. Virus

Your answer is incorrect.

The correct answer is: Logic bomb

Câu hỏi 57

Không trả lời

Đạt điểm 1,00

Which of the following malware types may require user interaction, does not hide itself, and is commonly identified by marketing pop-ups based on browsing habits?

Select one:

- a. Rootkit
- b. Adware
- c. Virus
- d. Botnet

Your answer is incorrect.

The correct answer is: Adware

Câu hỏi 58

Không trả lời

Đạt điểm 1,00

Pete, a security administrator, has observed repeated attempts to break into the network. Which of the following is designed to stop an intrusion on the network?

Select one:

- a. HIDS
- b. NIPS
- c. NIDS
- d. HIPS

Your answer is incorrect.

The correct answer is: NIPS

Câu hỏi 59

Không trả lời

Đạt điểm 1,00

A news and weather toolbar was accidently installed into a web browser. The toolbar tracks users online activities and sends them to a central logging server. Which of the following attacks took place?

Select one:

- a. Flash cookies
- b. Session hijacking
- c. Remote code execution
- d. Man-in-the-browser
- e. Malicious add-on

Your answer is incorrect.

The correct answer is: Malicious add-on

Câu hỏi 60

Không trả lời

Đạt điểm 1,00

A user has several random browser windows opening on their computer. Which of the following programs can be installed on his machine to help prevent this from happening?

Select one:

- a. Pop-up blocker
- b. Antivirus
- c. Anti-spam
- d. Spyware blocker

Your answer is incorrect.

The correct answer is: Pop-up blocker

Câu hỏi 61

Không trả lời

Đạt điểm 1,00

A user, Ann, is reporting to the company IT support group that her workstation screen is blank other than a window with a message requesting payment or else her hard drive will be formatted. Which of the following types of malware is on Ann's workstation?

Select one:

- a. Spyware
- b. Ransomware
- c. Trojan
- d. Adware

Your answer is incorrect.

The correct answer is: Ransomware

Câu hỏi 62

Không trả lời

Đạt điểm 1,00

Pete, a security analyst, has been tasked with explaining the different types of malware to his colleagues. The two malware types that the group seems to be most interested in are botnets and viruses. Which of the following explains the difference between these two types of malware?

Select one:

a. Viruses are a class of malware which create hidden openings within an OS

b. Viruses are a subset of botnets which are used as part of SYN attacks.

c. Botnets are a subset of malware which are used as part of DDoS attacks

d. Botnets are used within DR to ensure network uptime and viruses are not

Your answer is incorrect.

The correct answer is: Botnets are a subset of malware which are used as part of DDoS attacks

◄ Chapter 8 - LAB Database Security

Chuyển tới...

Video: Database security ►

An toan thong tin_ Nhom 11

Bắt đầu vào lúc	Sunday, 26 November 2023, 8:43 PM
Trạng thái	Đã xong
Kết thúc lúc	Sunday, 26 November 2023, 8:43 PM
Thời gian thực hiện	6 giây
Điểm	**0,00** trên 10,00 (**0**%)

Câu hỏi 1

Không trả lời

Đạt điểm 1,00

Which of the following controls can be used to prevent the disclosure of sensitive information stored on a mobile device's removable media in the event that the device is lost or stolen?

Select one:

- a. Hashing
- b. Encryption
- c. Device password
- d. Screen locks

Your answer is incorrect.

The correct answer is: Encryption

Câu hỏi 2

Không trả lời

Đạt điểm 1,00

Ann would like to forward some Personal Identifiable Information to her HR department by email, but she is worried about the confidentiality of the information. Which of the following will accomplish this task securely?

Select one:

- a. Hashing
- b. Encryption
- c. Digital Signatures
- d. Secret Key

Your answer is incorrect.

The correct answer is: Encryption

Câu hỏi 3

Không trả lời

Đạt điểm 1,00

Which of the following explains the difference between a public key and a private key?

Select one:

- a. The public key is only used by the client while the private key is available to all.
  Both keys are mathematically related.
- b. The private key is only used by the client and kept secret while the public key is available to all.
- c. The private key only decrypts the data while the public key only encrypts the data.
  Both keys are mathematically related.
- d. The private key is commonly used in symmetric key decryption while the public key is used in asymmetric key decryption.

Your answer is incorrect.

The correct answer is: The private key is only used by the client and kept secret while the public key is available to all.

Câu hỏi 4

Không trả lời

Đạt điểm 1,00

Which of the following is a way to implement a technical control to mitigate data loss in case of a mobile device theft?

Select one:

- a. Disk encryption
- b. Solid state drive
- c. Mobile device policy
- d. Encryption policy

Your answer is incorrect.

The correct answer is: Disk encryption

Câu hỏi 5

Không trả lời

Đạt điểm 1,00

After copying a sensitive document from his desktop to a flash drive, Joe, a user, realizes that the document is no longer encrypted. Which of the following can a security technician implement to ensure that documents stored on Joe's desktop remain encrypted when moved to external media or other network based storage?

Select one:

- a. Removable disk encryption
- b. File level encryption
- c. Database record level encryption
- d. Whole disk encryption

Your answer is incorrect.

The correct answer is: File level encryption

Câu hỏi 6

Không trả lời

Đạt điểm 1,00

An organization must implement controls to protect the confidentiality of its most sensitive data. The company is currently using a central storage system and group based access control for its sensitive information. Which of the following controls can further secure the data in the central storage system?

Select one:

- a. Data encryption
- b. File hashing
- c. Digital signatures
- d. Patching the system

Your answer is incorrect.

The correct answer is: Data encryption

Câu hỏi 7

Không trả lời

Đạt điểm 1,00

Which of the following concepts describes the use of a one way transformation in order to validate the integrity of a program?

Select one:

- a. Steganography
- b. Key escrow
- c. Hashing
- d. Non-repudiation

Your answer is incorrect.

The correct answer is: Hashing

Câu hỏi 8

Không trả lời

Đạt điểm 1,00

John recently received an email message from Bill. What cryptographic goal would need to be met to convince John that Bill was actually the sender of the message?

Select one:

a. Availability

b. Confidentiality

c. Integrity

d. Nonrepudiation

Your answer is incorrect.

The correct answer is: Nonrepudiation

Câu hỏi 9

Không trả lời

Đạt điểm 1,00

Which of the following functions provides an output which cannot be reversed and converts data into a string of characters?

Select one:

a. Stream ciphers

b. Steganography

c. Block ciphers

d. Hashing

Your answer is incorrect.

The correct answer is: Hashing

Câu hỏi 10

Không trả lời

Đạt điểm 1,00

When confidentiality is the primary concern, and a secure channel for key exchange is not available, which of the following should be used for transmitting company documents?

Select one:

- a. Hashing
- b. Asymmetric
- c. Digital Signature
- d. Symmetric

Your answer is incorrect.

The correct answer is: Asymmetric

◄ Video: IDS

Chuyển tới...

Chapter 10 - Synmentric Encyption ►

An toan thong tin_ Nhom 11

Bắt đầu vào lúc	Sunday, 26 November 2023, 8:44 PM
Trạng thái	Đã xong
Kết thúc lúc	Sunday, 26 November 2023, 8:44 PM
Thời gian thực hiện	7 giây
Điểm	0,00/30,00
Điểm	**0,00** trên 10,00 (**0**%)

Câu hỏi 1

Không trả lời

Đạt điểm 1,00

Protecting the confidentiality of a message is accomplished by encrypting the message with which of the following?

Select one:

a. Sender's public key

b. Recipient's public key

c. Recipient's private key

d. Sender's private key

Your answer is incorrect.

The correct answer is: Recipient's public key

Câu hỏi 2

Không trả lời

Đạt điểm 1,00

Which of the following provides additional encryption strength by repeating the encryption process with additional keys?

Select one:

- a. 3DES
- b. Blowfish
- c. TwoFish
- d. AES

Your answer is incorrect.

The correct answer is: 3DES

Câu hỏi 3

Không trả lời

Đạt điểm 1,00

Company A submitted a bid on a contract to do work for Company B via email. Company B was insistent that the bid did not come from Company A. Which of the following would have assured that the bid was submitted by Company A?

Select one:

- a. Digital Signatures
- b. Encryption
- c. Steganography
- d. Hashing

Your answer is incorrect.

The correct answer is: Digital Signatures

Câu hỏi 4

Không trả lời

Đạt điểm 1,00

An SSL session is taking place. After the handshake phase has been established and the cipher has been selected, which of the following are being used to secure data in transport? (Select TWO)

Select one or more:

- a. Symmetrical encryption
- b. Asymmetrical encryption
- c. Diffie-Hellman
- d. AES
- e. Ephemeral Key generation
- f. RSA

Your answer is incorrect.

The correct answers are: Diffie-Hellman, RSA

Câu hỏi 5

Không trả lời

Đạt điểm 1,00

Which of the following concepts is used by digital signatures to ensure integrity of the data?

Select one:

- a. Non-repudiation
- b. Key escrow
- c. Transport encryption
- d. Hashing

Your answer is incorrect.

The correct answer is: Hashing

Câu hỏi 6

Không trả lời

Đạt điểm 1,00

Digital certificates can be used to ensure which of the following? (Select TWO).

Select one or more:

- a. Non-repudiation
- b. Authorization
- c. Confidentiality
- d. Verification
- e. Availability

Your answer is incorrect.

The correct answers are: Confidentiality, Non-repudiation

Câu hỏi 7

Không trả lời

Đạt điểm 1,00

Joe must send Ann a message and provide Ann with assurance that he was the actual sender. Which of the following will Joe need to use to BEST accomplish the objective?

Select one:

- a. Ann's public key
- b. His public key
- c. A pre-shared private key
- d. His private key

Your answer is incorrect.

The correct answer is: His private key

Câu hỏi 8

Không trả lời

Đạt điểm 1,00

An email client says a digital signature is invalid and the sender cannot be verified. The recipient is concerned with which of the following concepts?

Select one:

- a. Integrity
- b. Remediation
- c. Availability
- d. Confidentiality

Your answer is incorrect.

The correct answer is: Integrity

Câu hỏi 9

Không trả lời

Đạt điểm 1,00

Which of the following are restricted to 64-bit block sizes? (Select TWO).

Select one or more:

- a. AES256
- b. DES
- c. PGP
- d. 3DES
- e. AES
- f. RSA

Your answer is incorrect.

The correct answers are: DES, 3DES

Câu hỏi 10

Không trả lời

Đạt điểm 1,00

Joe, a user, wants to send an encrypted email to Ann. Which of the following will Ann need to use to verify that the email came from Joe and decrypt it? (Select TWO).

Select one or more:

- a. Joe's private key
- b. The CA's public key
- c. Ann's private key
- d. The CA's private key
- e. Joe's public key
- f. Ann's public key

Your answer is incorrect.

The correct answers are: Ann's private key, Joe's public key

Câu hỏi 11

Không trả lời

Đạt điểm 1,00

Which of the following is used to verify data integrity?

Select one:

- a. 3DES
- b. RSA
- c. SHA
- d. AES

Your answer is incorrect.

The correct answer is: SHA

Câu hỏi 12

Không trả lời

Đạt điểm 1,00

Which of the following is true about asymmetric encryption?

Select one:

- a. A message encrypted with the public key can be decrypted with a shared key.
- b. A message encrypted with a shared key, can be decrypted by the same key.
- c. A message encrypted with the private key can be decrypted by the same key
- d. A message encrypted with the public key can be decrypted with the private key

Your answer is incorrect.

The correct answer is: A message encrypted with the public key can be decrypted with the private key

Câu hỏi 13

Không trả lời

Đạt điểm 1,00

Symmetric encryption utilizes _____, while asymmetric encryption utilizes _____.

Select one:

- a. Public keys, one time
- b. Shared keys, private keys
- c. Private keys, session keys
- d. Private keys, public keys

Your answer is incorrect.

The correct answer is: Private keys, public keys

Câu hỏi 14

Không trả lời

Đạt điểm 1,00

Digital signatures are used for ensuring which of the following items? (Select TWO).

Select one or more:

- a. Algorithm strength
- b. Integrity
- c. Confidentiality
- d. Non-Repudiation
- e. Availability

Your answer is incorrect.

The correct answers are: Integrity, Non-Repudiation

Câu hỏi 15

Không trả lời

Đạt điểm 1,00

Users need to exchange a shared secret to begin communicating securely. Which of the following is another name for this symmetric key?

Select one:

- a. Private Key
- b. Public Key
- c. Session Key
- d. Digital Signature

Your answer is incorrect.

The correct answer is: Private Key

Câu hỏi 16

Không trả lời

Đạt điểm 1,00

A system administrator is notified by a staff member that their laptop has been lost. The laptop contains the user's digital certificate. Which of the following will help resolve the issue? (Select TWO).

Select one or more:

- a. Restore the certificate using a CRL
- b. Restore the certificate using a recovery agent
- c. Mark the key as private and import it
- d. Issue a new digital certificate
- e. Revoke the digital certificate

Your answer is incorrect.

The correct answers are: Revoke the digital certificate, Issue a new digital certificate

Câu hỏi 17

Không trả lời

Đạt điểm 1,00

A software firm posts patches and updates to a publicly accessible FTP site. The software firm also posts digitally signed checksums of all patches and updates. The firm does this to address:

Select one:

- a. Confidentiality of downloaded software.
- b. Integrity of downloaded software.
- c. Availability of the FTP site.
- d. Integrity of the server logs.

Your answer is incorrect.

The correct answer is: Integrity of downloaded software.

Câu hỏi 18

Không trả lời

Đạt điểm 1,00

Which of the following is used by the recipient of a digitally signed email to verify the identity of the sender?

Select one:

a. Recipient's private key

b. Recipient's public key

c. Sender's private key

d. Sender's public key

Your answer is incorrect.

The correct answer is: Sender's public key

Câu hỏi 19

Không trả lời

Đạt điểm 1,00

Pete, an employee, needs a certificate to encrypt data. Which of the following would issue Pete a certificate?

Select one:

a. Certification authority

b. Registration authority

c. Key escrow

d. Certificate revocation list

Your answer is incorrect.

The correct answer is: Certification authority

Câu hỏi 20

Không trả lời

Đạt điểm 1,00

Which of the following uses both a public and private key?

Select one:

- a. AES
- b. RSA
- c. SHA
- d. MD5

Your answer is incorrect.

The correct answer is: RSA

Câu hỏi 21

Không trả lời

Đạt điểm 1,00

A system administrator is setting up a file transfer server. The goal is to encrypt the user authentication and the files the user is sending using only a user ID and a key pair. Which of the following methods would achieve this goal?

Select one:

- a. IPSec
- b. SSH
- c. PGP
- d. AES

Your answer is incorrect.

The correct answer is: SSH

Câu hỏi 22

Không trả lời

Đạt điểm 1,00

Which of the following is BEST used as a secure replacement for TELNET?

Select one:

- a. GPG
- b. SSH
- c. HTTPS
- d. HMAC

Your answer is incorrect.

The correct answer is: SSH

Câu hỏi 23

Không trả lời

Đạt điểm 1,00

What is the length of the cryptographic key used in the Data Encryption Standard (DES) cryptosystem?

Select one:

- a. 256 bits
- b. 192 bits
- c. 128 bits
- d. 56 bits

Your answer is incorrect.

The correct answer is: 56 bits

Câu hỏi 24

Không trả lời

Đạt điểm 1,00

A security administrator must implement a secure key exchange protocol that will allow company clients to autonomously exchange symmetric encryption keys over an unencrypted channel. Which of the following MUST be implemented?

Select one:

- a. Diffie-Hellman
- b. AES
- c. SHA-256
- d. 3DES

Your answer is incorrect.

The correct answer is: Diffie-Hellman

Câu hỏi 25

Không trả lời

Đạt điểm 1,00

Which one of the following cannot be achieved by a secret key cryptosystem?

Select one:

- a. Nonrepudiation
- b. Key distribution
- c. Confidentiality
- d. Availability

Your answer is incorrect.

The correct answer is: Nonrepudiation

Câu hỏi 26

Không trả lời

Đạt điểm 1,00

How many keys are required to fully implement a symmetric algorithm with 10 participants?

Select one:

- a. 20
- b. 10
- c. 45
- d. 100

Your answer is incorrect.

The correct answer is: 45

Câu hỏi 27

Không trả lời

Đạt điểm 1,00

Which of the following symmetric key algorithms are examples of block ciphers? (Select Two).

Select one or more:

- a. MD5
- b. 3DES
- c. PGP
- d. AES
- e. RC4

Your answer is incorrect.

The correct answers are: 3DES, AES

Câu hỏi 28

Không trả lời

Đạt điểm 1,00

Digital certificates can be used to ensure which of the following? (Select TWO)

Select one or more:

- a. Confidentiality
- b. Non-repudiation
- c. Verification
- d. Availability
- e. Authorization

Your answer is incorrect.

The correct answers are: Confidentiality, Non-repudiation

Câu hỏi 29

Không trả lời

Đạt điểm 1,00

How many encryption keys are required to fully implement an asymmetric algorithm with 10 participants?

Select one:

- a. 20
- b. 10
- c. 100
- d. 45

Your answer is incorrect.

The correct answer is: 20

Câu hỏi 30

Không trả lời

Đạt điểm 1,00

An organization wants to conduct secure transactions of large data files. Before encrypting and exchanging the data files, the organization wants to ensure a secure exchange of keys. Which of the following algorithms is appropriate for securing the key exchange?

Select one:

- a. 3DES
- b. DSA
- c. Diffie-Hellman
- d. Blowfish
- e. DES

Your answer is incorrect.

The correct answer is: Diffie-Hellman

◄ Chapter 11 - Asymmetric and Key Management

Chuyển tới...

Chapter 12 - Hash - MAC - HMAC - Digital Signature ►