ĐỀ KT SÁNG T5

phần mềm phân tích lưu lượng mạng

Một quản trị mạng mới thay thế hub bằng switch. Khi sử dụng phần mềm Sniffer bắt các gói tin trên mạng, người quản trị thấy được dữ liệu trao đổi giữa máy tính của anh ta và máy chủ, nhưng không thấy được các trao đổi giữa những máy khác trong mạng với máy chủ. Coi như switch hoạt động tốt, điều gì đã tạo ra hiện tượng trên?

a. Switch được cấu hình VLAN

hub dùng khuếch đại tín hiệu
switch: ghi nhớ địa chỉ MAC của các thiết bị nối với từng cổng của nó, chỉ chuyển tiếp gói tin đến cổng có địa chỉ MAC đích của gói tin, thay vì phát tán đến tất cả các cổng
sswitch sẽ gửi 1 broadcast ai có mac này sau áo máy có mac sẽ phát 1 tín hiện trả cề và truyền

b. Trừ thông tin broadcast và unknown unicast, switch không gửi thông tin ra tất cả các cổng

c. Phần mềm Sniffer không bắt được thông tin qua cổng Ethernet

d. Phần mềm Sniffer cấu hình sai

=>B

Đảm bảo dữ liệu không bị sửa đổi trong quá trình lưu trữ hay trong quá trình truyền qua mạng bởi những người dùng không hợp pháp gọi là?

a. Nonrepudiation

làm cho 1 người không thể chối bỏ những hành động mình đã làm

b. Integrity

đảm bảo thông tin y hệt ban đầu không bị sửa bởi người không có quyền

c. Confidentiality

thông tin bảo đảm dc giữ kín, chĩ người có quyền mới biết

d. Availability

luôn có khi những ng có quyền truy cập

=> B

Mặc dù báo cáo quét lỗ hổng cho thấy không có lỗ hổng nào được phát hiện, nhưng một cuộc kiểm tra thâm nhập tiếp theo cho thấy có các lỗ hổng trên mạng. Thuật ngữ nào sau đây mô tả cho trường hợp này?

a. Passive scan

quết mạng nhưng không gửi bất kì gói tin nào, thu thập thông tin trên lưu lượng mạng

là khi một hệ thống hoặc công cụ không phát hiện ra lỗ hổng hoặc vấn đề tồn tại trong thực t

b. False negative

Là một phương pháp quét mạng mà công cụ quét sẽ gửi các gói tin đến các hệ thống mục tiêu để tìm kiếm lỗ hổng

c. Active scan

Là khi một hệ thống hoặc công cụ báo cáo có lỗ hổng hoặc vấn đề nhưng thực tế không tồn tại.

d. False positive

=> B

Email Server nên được đặt ở vùng mạng nào?

a. DZM

b. INSIDE

c. DMZ

DMZ (Demilitarized Zone): chứa các dịch vụ công cộng (server hay tb kết nối cã INSIDE OUTSIDE

d. OUTSIDE

=> C

kẻ tấn công lừa gạt hoặc thao túng con người để tiết lộ thông tin nhạy cảm, thực hiện hành động có lợi cho kẻ tấn công hoặc phá vỡ các biện pháp bảo mật

Đâu là mục tiêu chủ yếu của kiểu tấn công Social Engineering?

a. Peer to Peer Network

b. Email

c. Con người

d. Local Area Network

=> C

Quản trị viên bảo mật thiết lập một AP mới nhưng nhận ra quá nhiều người bên ngoài có thể kết nối với AP đó và truy cập trái phép. Các cách nào sau đây sẽ là cách TỐT NHẤT để giảm thiểu vấn đề này?

a. Tất cổng kết nối có dây

b. Disable SSID broadcast

Vô hiệu hóa việc phát SSID (Service Set Identifier) sẽ giúp mạng không xuất hiện trong danh sách các mạng Wi-Fi có sẵn

c. MAC filtering là chĩ có những MAC dc cho mới được phép truy cập

d. Sử dụng kênh 1, 4, 7 trong cấu hình AP

e. Sử dụng 802.11ax

=> b, c

Access control liên quan đến 2 chức năng chính là?

a. Role Based Access Control phân quyền dựa trên vai trò người dùng

b. Authentication

c. Least privilege principle chính sách phân quyền: cấp ÍT quyền NHẤT nhưng đảm bảo hoàn thành cviec

d. Authorization

e. Rule Based Access Control

=> b, d

Khái niệm bảo mật nào khuyến khích quản trị viên cài đặt tường lửa, chương trình quét phần mềm độc hại (malware scanner) và IDS trên các host?

a. Endpoint security

b. Network access control (NAC)

C. SAFE

d. VLAN

e. RADIUS

=> a

Mục tiêu chính của an toàn thông tin là đảm bảo các tính chất theo mô hình C-I-A là?

a. Tính chống chối bỏ

b. Tính sẵn sàng

c. Tính toàn vẹn

d. Tính dễ mở rộng

e. Tính xác thực

f. Tính bí mật

=> b, c, f

Hệ thống IDS/IPS phát hiện xâm nhập dựa vào các kỹ thuật nào sau đây?

a. Role-based detection

b. Anomaly-based detection phát hiện hành vi bất thường

c. Classify-based detection

d. Attribute-based detection

e. Signature-based detection sử dụng các tập tin hoặc mẫu của các cuộc tấn công đã biết để so sánh với lưu lượng mạng nếu trùng sẽ ngăn chặn

=> b, e

Giải pháp StackGuard giúp phòng chống tấn công tràn bộ đệm trên stack thực hiện như sau:

a. Sử dụng một vùng nhớ đệm an toàn giữa Return Address và Buffer. Sử dụng vùng nhớ đệm an toàn này để kiểm tra xem Return Address có bị sửa đổi hay không.

b. Kiểm tra chiều dài dữ liệu nhập trước khi thực hiện việc gán dữ liệu

c. Kiểm tra giá trị Return Address có bị sửa đổi hay không

d. Lưu trữ giá trị Return Address ở một nơi khác và sử dụng nó để kiểm tra xem giá trị ở Return Address có bị sửa đổi hay không.

=> a

Kiểu tấn công nào sau đây không phải khai thác các lỗ hổng của ứng dụng Web ?

a. Cross Site Request Forgery Tấn công CSRF là khi kẻ tấn công lừa người dùng thực hiện các hành động không mong muốn trên một trang web mà họ đã đăng nhập

b. SQL Injection Tấn công SQL Injection là khi kẻ tấn công chèn các câu lệnh SQL độc hại vào các trường đầu vào của ứng dụng web

c. Cross-site scripting Tấn công XSS là khi kẻ tấn công chèn mã JavaScript độc hại vào các trang web

d. Social Engineering tấn công con người

=> d

Theo bạn giải pháp nào cần được áp dụng với các tài khoản người dùng trong hệ thống của một nhân viên nghỉ việc?

a. Vô hiệu hóa các tài khoản của nhân viên đó và xóa ngay lập tức các dữ liệu được lưu trữ

b. Duy trì các tài khoản người dùng và giữ lại các dữ liệu được lưu trữ trong một thời gian

C. Vô hiệu hóa các tài khoản của nhân viên đó và giữ lại các dữ liệu được lưu trữ trong một thời gian

d. Không sử dụng các lựa chọn nào ở đây

=> C

/*/Bạn là người tư vấn giải pháp an toàn thông tin, một khách hàng của bạn quan tâm đến việc chống lại giả mạo và nhiễm độc ARP trong mạng của họ. Giải pháp nào dưới đây KHÔNG áp dụng cho mục đích này?

ARP (Address Resolution Protocol) là một giao thức mạng được sử dụng để ánh xạ địa chỉ IP (Internet Protocol) của một thiết bị mạng sang địa chỉ MAC (Media Access Control)

a. Sử dụng firewall giữa các phân vùng trong LAN

b. Sử dụng công cụ giám sát ARP trong mạng

port nào chỉ có mac nào truy cập dc

C. Sử dụng port security trên các switch

d. Nếu trong một mạng nhỏ thì sử dụng ARP tỉnh

ARP tĩnh cho phép bạn cấu hình một ánh xạ cố định giữa địa chỉ IP và địa chỉ MAC của một thiết bị, thay vì để cho ARP tự động học.

=> d

Mô hình AAA liên quan đến các chứng năng nào sau đây?

a. Authentication

b. Automation

c. Authenticity

d. Authorization

e. Accounting

f. Accessing

=> a, d, e

Kiểu tấn công nào sau đây không phải kiểu tấn công từ chối dịch vụ?

một kiểu tấn công từ chối dịch vụ (DDoS) khi nhiều máy tính bị nhiễm mã độc (botnet) cùng tấn công vào mục tiêu máy attack server sẽ tạo ra các con bots tấn công khiến máy chu

a. Sử dụng Botnet

b. Ping of Death kẻ tấn công gửi các gói tin Ping có kích thước lớn vượt quá khả năng xử lý của hệ thống mục tiêu

c. Main-In-The-Middle (MITM) kẻ tấn công can thiệp vào quá trình giao tiếp giữa hai bên, để nghe lén, thay đổi hoặc giả mạo thông tin

d. ICMP Flood gửi một lượng lớn gói tin ICMP để làm quá tải hệ thống

e. Teardrop kẻ tấn công gửi các gói tin IP bị phanh mảnh để gây lỗi cho hệ thống mục tiêu

=>C

Cho mô tả sau: User Nam có quyền đọc và ghi trên file bt1. Nam cũng có quyền đọc trên file bt2 và có quyền thực thi trên file bt3, User Ha có quyền đọc trên file bt1. Hà có quyền đọc và ghi trên file bt2. Hà không có quyền truy cập trên file bt3.

Xác định ACL (Access control list) đối với file bt2?

a. ACL(bt2) = Nam: {read), Ha: {read}

b. ACL(bt2) Nam: (read, write), Ha: {read, write}

c. ACL(bt2) = Nam: {read}, Ha: {read, write}

d. ACL(bt2)= Nam: (read, write), Ha: (read)

e. ACL(bt2) = Nam: (read, execute), Ha: (read, write}

=> C

	bt1	bt2	bt3
Nam	đọc ghi	đọc	đọc ghi thực thi
Hà	đọc	đọc ghi	không quền

Capability table (bound to a subject) - users
Access control List (bound to an object - các files

/*/Phát biểu nào sau đây không đúng về vùng DMZ?

a. Để nâng cao sự bảo mật cho hệ thống

b. Thường chứa email server hoặc web server

c. Chứa các server chỉ phục vụ cho người dùng bên trong

d. Là nơi đặt các public server

=> C

Từ ma trận điều khiển truy cập, ta có thể suy ra các thông tin nào sau đây?

a. Subjects orientation lists

b. Access control lists

c. Objects orientation list

d. Group policy objects

access control matrix → object

subject ↓

	bt1	bt2	bt3
Nam	đọc ghi	đọc	đọc ghi thực thi
Hà	đọc	đọc ghi	không quền

e. Capability lists

=> b, e

Việc tắt các port không sử dụng trên switch hay gỡ bỏ các dịch vụ, giao thức, phần mềm không cần thiết gọi là gì?

a. Hashing

b. Hardening

vá lỗ hỏng
khóa port ko xài
set pass policy
xóa dịch vụ ko xài
xóa default account
quản lí quyền user

c. Unused-removing

d. Auditing

e. Non-repudiation

=> b

Ma trận điều khiển truy cập (Access control matrix) thể hiện mối quan hệ giữa các thành phần nào sau đây?

a. Subjects

b. Objects

c. Rights/Permissions

d. Data

e. Security policies

=> a, b, c

Muốn thay thế telnet với một giao thức an toàn hơn để quản lý các thiết bị mạng, ta cần sử dụng giao thức nào sau đây?

a. SMTP simple mail transfer -> chuyễn mail

b. SSH secure shell

d. SFTP (ssh file transfer protocol -> dùng để truyền file không phải quản lí tb mạng)

e. SNMP

C. HTTP

=> B

Điều nào sau đây xảy ra khi một chuỗi dữ liệu được gửi đến bộ đệm lớn hơn bộ đệm được thiết kế để xử lý?

a. Man in the middle attack

b. SYN flood tấn công từ chối dịch vụ (DoS) trong đó kẻ tấn công gửi một loạt các yêu cầu kết nối TCP SYN đến máy chủ để làm cạn kiệt tài nguyên và ngăn chặn máy chủ phản hồi các yêu cầu hợp lệ

c. Brute Force attack

d. Buffer overflow

e. Spoofing attack giả mạo danh tính của một thực thể khác để đánh lừa hệ thống

=> d

Tại sao các nhà phát triển phần mềm đính kèm theo các giá trị băm bằng hàm MD5 của các gói cập nhật cho phần mềm cùng với các gói đó để các khách hàng của họ có thể download từ Internet?

a. Khách hàng có thể yêu cầu các bản cập nhật mới cho phần mềm trong tương lai bằng cách sử dụng giá trị hàm băm đính kèm theo

b. Khách hàng có thể xác thực tính toàn vẹn của gói cập nhật cho phần mềm sau khi download về

c. Khách hàng có thể khẳng định tính xác thực của Site mà họ download gói cập nhật về

d. Khách hàng cần giá trị của hàm băm để có thể kích hoạt được phần mềm mới

=> b

Điều nào sau đây mô đúng nhất cơ chế kiểm soát truy cập cho phép chủ sở hữu dữ liệu tạo và quản lý kiểm soát truy cập?

a. MACS (Mandatory Access Control) chỉ có hệ thống ms có quyền kiểm soát access control

b. Rule Based Access Control tự động gắn quyền cho user thông qua các criteria defined by systems

c. RBACS (Role Based Access Control) cung cấp truy cập dựa trên chức vụ của user trong hệ thống

d. LBACS (List Based Access Control)

tùy ý

e. DACs (Discretionary Access Control) cho phép owner control what they own,

=> e

Một kiểu tấn công DoS sử dụng cơ chế bắt tay ba bước (three-way handshake) của TCP là?

three way handshake

a. SYN Flood

b. Buffer Overflow

c. Ping of Death

d. SQL Injection

e. Brute force

=>A

Điều nào sau đây không check với file đáp án của test cuối kỳ rùi khi nói về lỗ hổng 0-day?

a. Là lỗ hổng phá hoại hệ thống trong vòng một ngày

b. Là lỗ hồng nguy hiểm khi tấn công vào hệ thống chưa có giải pháp bảo vệ

c. Là lỗ hồng hacker chưa công bố rộng rãi

d. Là lỗ hồng nhà sản xuất chưa kịp và

=> a

Trong tổ chức bộ nhớ của chương trình C, phần Data-Segment lưu các thông tin gì của chương trình?

data segment: các biến đã khai báo
code segment: các đoạn lệnh cũa chương trình
bss segment: các biến chưa dc khỏi tạo

a. Lưu các đối số của một hàm

b. Lưu các biến static/global chưa được khởi tạo trong chương trình

C. Lưu các biến cục bộ trong chương trình

d. Lưu mã nguồn thực thi

e. Lưu các biến static/giobal đã được khởi tạo trong chương trình

=> e

Chuẩn nào sau đây liên quan đến an toàn thông tin?

a. ISO 2600

b. ISO 9001

c. ISO 2015

d. ISO 27001

e. ISO 21997

=>D

Tấn công Buffer Overflow có hai loại là?

a. SQL injection và XSS

O b. Stack và memory

heap: các hàm maloc()
stack: strcp(), strcat(),...

c. Heap và stack

O d. Heap và network overflow

O e. Stack và SQL injection

=>C

Câu hỏi 48: Công cụ nào dùng sau đây để quét cổng của máy tính?

a. ping kiễm traa kết nối giửa 2 máy

b. nslookup tra cứu thông tin về tên miền, ip add,..

c. telnet cấu hình từ xa, quàn lí thiết bị mạng

d. nmap phần mềm quét mạng

e. tracert xác định đường đi của các gói tin

=>d

Mã độc Rootkit thường trú ẩn ở đâu?

a. Text file

b. RAM

c. Boot Sector

d. Operation system

=> d

Chế độ hoạt động nào sau đây mã hóa các khối một cách riêng biệt?

a. Cipher feedback mode - CFB khối mã hóa được sử dụng để tạo ra một chuỗi đồng bộ, và sau đó, chuỗi đồng bộ được sử dụng để mã hóa các khối tiếp theo. Không mã hóa các khối đơn lẻ một cách riêng biệt

b. Output feedback mode - OFB

mỗi khối mã hóa được kết hợp với khối trước đó trước khi được mã hóa

c. Cipher block chaining mode - CBC

d. Electronic codebook mode – ECB

mỗi khối dữ liệu được mã hóa bằng cùng một khóa và giống nhau một cách không thay đổi. Điều này có nghĩa là một khối dữ liệu cụ thể sẽ mã hóa thành một khối mã hóa cố định và không thay đổi mỗi khi nó được mã hóa

=> d

Giả sử thuật toán RSA đã tạo ra cặp khóa pubic (7,187) và private (23,187). Message M= 12 sẽ được mã hóa thành gì?

a. 133

khóa public (e,n) --> e = 7, n = 187
khóa private (d,n) --> d = 23, n = 187

1> 2 số p, q
2> n = p.q , N = (q-1)(p-1)
3> e.d mod N = 1
4> công bố khóa

b. 17

crypted = m^e mod n

c. 121

decrytped = c^d mod n

d. 177

=>D

Trong mật mã khóa công khai, nếu A muốn gửi thông điệp đến B

a. Thông điệp được mã hóa bằng khóa riêng của A

b. Thông điệp được mã hóa bằng khóa công khai của A

c. Thông điệp được mã hóa bằng khóa riêng của B

d. Thông điệp được mã hóa bằng khóa công khai của B

=> d

Thuật toán mật mã nào sau đây dựa trên độ khó của bài toán phân tích các số lớn thành tích của hai thừa số nguyên tố ban đầu?

a. Diffie-Hellman

b. DES

c. ECC

d. ZUC

e. RSA

=> e

mạng ảo

Tại sao hacker hay sử dụng máy chủ proxy?

a. Để có được kết nối truy cập từ xa

b. Để tạo một máy chủ ma trên mạng

c. Để tạo kết nối mạnh mẽ hơn với mục tiêu

d. Để ẩn hoạt động của chúng trên mạng

=> d

Thuật toán nào dưới đây không phải là thuật toán mã hóa khối?

a. AES

b. 3DES

C. DES

d. RC4 stream cipher: tạo ra các dòng byte để mã hóa dữ liệu

=> d

Câu nào sau đây không phải là một mô hình điều khiển truy cập?

a. Role Based Access Control

b. Attribute Based Access Control

c. Discretionary Access Control (DAC)

d. Subjective Access Control

e. Mandatory Access Control (MAC)

=> d

Loại malware nào sau đây có thể ẩn các tiến trình và các tập tin trên hệ thống?

a. Worm

b. Rootkit

c. Trojan tưỡng là phần mêm tốt nhưng tiềm tàng mã độc

d. Adware hiển thị quảng cáo ko mong muốn

=>b

Frank rất quan tâm đến các cuộc tấn công vào máy chủ thương mại điện tử của công ty. Ông đặc biệt lo lắng về tấn công SQL Injection. Điều nào sau đây sẽ bảo vệ tốt nhất trước cuộc tấn công cụ thể này?

sql injectuon: là tấn công dựa trên dữ liệu nhập vào nhằm lấy các thông tin user

a. Lưu lượng truy cập web được mã hóa

b. Lọc dữ liệu người dùng nhập vào

c. Firewall

d. IDS

=>b

Trong mật mã khóa công khai (PKI), để xác nhận mình là người gửi thông tin, người gửi sẽ sử dụng khóa nào?

a. Session key

người gửi muốn xác nhận mình là người gửi thông tin trong PKI, họ sẽ sử dụng khóa riêng tư (private key) của mình để tạo chữ ký số cho thông tin, và bên nhận sẽ sử dụng khóa công khai (public key) tương ứng để xác minh chữ ký số đó

b. Secret key

c. Public key

d. Private key

=> d

Nếu bạn chia sẻ quá nhiều thông tin trên phương tiện truyền thông xã hội, bạn có thể gặp rủi ro gì?

a. Tấn công giả mạo (Phishing)

b. Mã độc (malware)

c. Ransomware

d. Đánh cắp danh tính (Identity theft)

=>a

Giao thức nào sau đây thuộc mã khóa công khai ?

a. AES

b. 3DES

c. DES

d. RSA

=> d

Điều nào sau đây là rủi ro tiềm ẩn khi chương trình chạy ở chế độ đặc quyền?

a. Nó có thể cho phép mã độc được chèn vào

b. Nó có thể tạo ra việc loại bỏ các ứng dụng không cần thiết

c. Nó có thể không thực hiện việc phân chia xử lý các tác vụ

d. Nó có thể phục vụ cho việc tạo ra các đoạn mã phức tạp không cần thiết

=>a

Công cụ nào dưới đây có thể dùng để xác định các kết nối mạng đang có trên máy tính?

a. Netstat

b. Tracert

c. Ipconfig

d. Ping

=>a

Rủi ro chính từ việc sử dụng phần mềm lỗi thời (outdated software) là gì?

a. Nó có thể không còn được hỗ trợ bởi các nhà cung cấp

b. Nó có thể không có tất cả các tính năng bạn cần

c. Nó có thể không có các tính năng bảo mật hiện đại nhất

d. Có thể dễ dàng xâm nhập hơn phần mềm mới hơn

=>a

Máy chủ web của một công ty được cấu hình những dịch vụ sau HTTP, SSL, FTP, SMTP Máy chủ này được đặt trong vùng DMZ. Đấu là những cổng cần phải mở trên tường lửa để cho phép các máy trạm có thể sử dụng dịch vụ trên máy này?

a. 434, 21, 80, 25, 20

http: 80
ssl: 443
ftp: 20, 21
smtp: 25

b. 119, 23, 21, 80, 23

110: pop3

c. 80, 20, 21, 25, 443

d. 110, 443, 21, 59,25

=> c

Mục đích chính của chương trình nâng cao nhận thức bảo mật là? (ransomware)

a. Đảm bảo rằng mọi người đều hiểu chính sách và thủ tục của tổ chức

b. Thông báo cho người dùng để tuân thủ các quy định liên quan đến bảo vệ dữ liệu và thông tin

c. Thông báo cho mọi người rằng quyền truy cập vào thông tin sẽ được cấp khi người sử dụng có yêu cầu

d. Cảnh báo tất cả người dùng truy cập vào tất cả các hệ thống sẽ được theo dõi hàng ngày

=>a

ĐỀ CUỐI KỲ

Started on	Thursday, 19 October 2023, 10:42 AM
State	Finished
Completed on	Thursday, 19 October 2023, 10:42 AM
Time taken	7 secs
Marks	0.00/55.00
Grade	**0.00** out of 10.00 (**0**%)

Question 1

Not answered

Marked out of 1.00

Điều nào sau đây KHÔNG đúng khi nói về lỗ hổng Zero-day

a. Là lỗ hổng nhà sản xuất chưa kịp vá

b. Là lỗ hổng nguy hiểm khi tấn công vào hệ thống chưa có giải pháp bảo vệ

c. Là lỗ hổng hacker chưa công bố rộng rãi

d. Là lỗ hổng phá hoại hệ thống trong vòng một ngày

Câu trả lời của bạn sai.

The correct answer is:
Là lỗ hổng phá hoại hệ thống trong vòng một ngày

Question 2

Not answered

Marked out of 1.00

Các giải pháp mã hóa KHÔNG đảm bảo được tính chất nào sau đây

a. Tính xác thực

b. Tính toàn vẹn

c. Tính sẵn sàng

d. Tính bí mật

Câu trả lời của bạn sai.

The correct answer is:
Tính sẵn sàng

Question 3

Not answered

Marked out of 1.00

Đảm bảo dữ liệu không bị sửa đổi trong quá trình lưu trữ hay trong quá trình truyền qua mạng bởi những người dùng không hợp pháp gọi là?

- a. Non-repudiation
- b. Availability
- c. Confidentiality
- d. Integrity

Câu trả lời của bạn sai.

The correct answer is:
Integrity

Question 4

Not answered

Marked out of 1.00

Mục đích chính của chương trình nâng cao nhận thức bảo mật là?

- a. Rootkit
- b. Code Red
- c. Ransomeware
- d. Logic boom

Câu trả lời của bạn sai.

The correct answer is:
Ransomeware

Question 5

Not answered

Marked out of 1.00

Phương pháp nào sau đây là TỐT NHẤT để giảm hiệu quả của các cuộc tấn công lừa đảo trên mạng?

- a. Phần mềm chống lừa đảo
- b. Xác thực 2 yếu tố
- c. Đào tạo nâng cao nhận thức người dùng
- d. Quét lỗ hổng cho hệ thống định kỳ

Câu trả lời của bạn sai.

The correct answer is:
Đào tạo nâng cao nhận thức người dùng

Question 6

Not answered

Marked out of 1.00

Rủi ro chính từ việc sử dụng phần mềm lỗi thời (outdated software) là gì

- a. Nó có thể không còn được hỗ trợ bởi các nhà cung cấp
- b. Nó có thể không có các tính năng bảo mật hiện đại nhất
- c. Nó có thể không có tất cả các tính năng bạn cần
- d. Có thể dễ dàng xâm nhập hơn phần mềm mới hơn

Câu trả lời của bạn sai.

The correct answer is:
Nó có thể không còn được hỗ trợ bởi các nhà cung cấp

Question 7

Not answered

Marked out of 1.00

Nếu bạn chia sẻ quá nhiều thông tin trên phương tiện truyền thông xã hội, bạn có thể gặp rủi ro gì?

- a. Mã độc (malware)
- b. Đánh cắp tiền
- c. Ransomware
- d. Tấn công giả mạo (Phishing)

phising là loại tấn công đánh cắp thông tin ng dùng thông qua những gì họ chưa sẻ, tấn công vào tâm lí để hộ tiết lộ thông tin

Câu trả lời của bạn sai.

The correct answer is:
Tấn công giả mạo (Phishing)

Question 8

Not answered

Marked out of 1.00

Frank rất quan tâm đến các cuộc tấn công vào máy chủ thương mại điện tử của công ty. Ông đặc biệt lo lắng về tấn công SQL Injection. Điều nào sau đây sẽ bảo vệ tốt nhất trước cuộc tấn công cụ thể này?

- a. Firewall
- b. IDS
- c. Lọc dữ liệu người dùng nhập vào
- d. Lưu lượng truy cập web được mã hóa

Câu trả lời của bạn sai.

The correct answer is:
Lọc dữ liệu người dùng nhập vào

Question 9

Not answered

Marked out of 1.00

Điều nào sau đây đúng khi nói về tấn công làm tràn bộ đệm (buffer Overflow)

- a. Ghi đè các giá trị lên các biến của chương trình nhằm thay đổi hành vi của chương trình theo mục đích của kẻ tấn công
- b. Xảy ra do kiểm tra dữ liệu đầu vào không đầy đủ hoặc bị bỏ qua
- c. Xóa dữ liệu người dùng
- d. Kẻ tấn công gửi các chuỗi dữ liệu lớn làm tràn bộ đệm đã được thiết kế cho chương trình

Câu trả lời của bạn sai.

The correct answer is:
Kẻ tấn công gửi các chuỗi dữ liệu lớn làm tràn bộ đệm đã được thiết kế cho chương trình

Question 10

Not answered

Marked out of 1.00

Câu nào sau đây KHÔNG phải là một cơ chế điều khiển truy cập?

- a. Mandatory Access Control (MAC)
- b. Attribute Based Access Control (ABAC)
- c. Discretionary Access Control (DAC)
- d. Subjective Access Control (SAC)
- e. Role Based Access Control (RBAC)

Câu trả lời của bạn sai.

The correct answer is:
Subjective Access Control (SAC)

Question 11

Not answered

Marked out of 1.00

Điều nào sau đây xảy ra khi một chuỗi dữ liệu được gửi đến bộ đệm lớn hơn bộ đệm được thiết kế để xử lý?

- a. Brute Force attack
- b. Buffer overflow
- c. SYN flood
- d. Blue Screen of Death
- e. Spoofing attack
- f. Man in the middle attack

Câu trả lời của bạn sai.

The correct answer is:
Buffer overflow

Question 12

Not answered

Marked out of 1.00

Điều nào sau đây mô tả tốt nhất cơ chế kiểm soát truy cập trong đó các quyết định kiểm soát truy cập dựa trên trách nhiệm của người dùng trong một tổ chức?

- a. Role Based Access Control (RBAC)
- b. Mandatory Access Control (MAC)
- c. Discretionary Access Control (DAC)
- d. Subjective Access Control (SAC)
- e. Attribute Based Access Control (ABAC)

Câu trả lời của bạn sai.

The correct answer is: Role Based Access Control (RBAC)

Question 13

Not answered

Marked out of 1.00

Điều nào sau đây mô tả đúng nhất cơ chế kiểm soát truy cập cho phép chủ sở hữu dữ liệu tạo và quản lý kiểm soát truy cập?

- a. Role Based Access Control (RBAC)
- b. List Based Access Control (LBAC)
- c. Discretionary Access Control (DAC)
- d. Attribute Based Access Control (ABAC)
- e. Mandatory Access Control (MAC)

Câu trả lời của bạn sai.

The correct answer is:
Discretionary Access Control (DAC)

Question 14

Not answered

Marked out of 1.00

Hình sau đây mô tả đúng nhất cơ chế kiểm soát truy cập nào

- a. Discretionary Access Control (DAC)
- b. Role Based Access Control (RBAC)
- c. Attribute Based Access Control (ABAC) mô hình kiểm soát truy cập dựa trên các thuộc tính của người dùng (Subject attributes), các thuộc tính của đối tượng (Object attributes), và các điều kiện môi trường (Environmental conditions)
- d. Mandatory Access Control (MAC)
- e. List Based Access Control (LBAC)

Câu trả lời của bạn sai.

The correct answer is: Attribute Based Access Control (ABAC)

Question 15

Not answered

Marked out of 1.00

Ma trận điều khiển truy cập (Access control matrix) thể hiện mối quan hệ giữa các thành phần nào sau đây? (chọn 3)

- a. Subject
- b. Users
- c. Database
- d. Rights/Permissions
- e. Object
- f. Security policy

Câu trả lời của bạn sai.

The correct answers are:
Subject, Object, Rights/Permissions

Question 16

Not answered

Marked out of 1.00

Từ ma trận điều khiển truy cập, ta có thể suy ra các thông tin nào sau đây?

- a. Access control lists
- b. Capability lists
- c. Group policy objects
- d. Objects orientation list
- e. Subjects orientation lists

Câu trả lời của bạn sai.

The correct answers are: Access control lists, Capability lists

Question 17

Not answered

Marked out of 1.00

Mô hình AAA liên quan đến các chứng năng nào sau đây?

- a. Accessing
- b. Authorization
- c. Automation
- d. Authentication
- e. Availability
- f. Accounting

Câu trả lời của bạn sai.

The correct answers are: Authentication, Authorization, Accounting

Question 18

Not answered

Marked out of 1.00

Access control liên quan đến 2 chức năng chính là?

- a. Discretionary Access Control (DAC)
- b. Role Based Access Control (RBAC)
- c. Authentication
- d. Rule Based Access Control
- e. Authorization

Câu trả lời của bạn sai.

The correct answers are:
Authentication, Authorization

Question 19

Not answered

Marked out of 1.00

Cho mô tả sau: User Nam có quyền đọc và ghi trên file bt1. Nam cũng có quyền đọc trên file bt2 và có quyền thực thi trên file bt3.

User Ha có quyền đọc trên file bt1. Hà có quyền đọc và ghi trên file bt2. Hà không có quyền truy cập trên file bt3.

Xác định **ACL** (Access control list) đối với file **bt2**

	bt2
Nam	đọc
Hà	đọc ghi

- a. ACL(bt2) = Nam: {read}, Ha: {read, write}
- b. ACL(bt2) = Nam: {read, write}, Ha: {read}
- c. ACL(bt2) = Nam: {read, execute}, Ha: {read, write}
- d. ACL(bt2) = Nam: {read}, Ha: {read}
- e. ACL(bt2) = Nam: {read, write}, Ha: {read, write}

Câu trả lời của bạn sai.

The correct answer is:
ACL(bt2) = Nam: {read}, Ha: {read, write}

Question 20

Not answered

Marked out of 1.00

Tấn công Buffer Overflow có hai loại là?

- a. Heap và network overflow
- b. Stack và memory
- c. SQL injection và XSS
- d. Stack và SQL injection
- e. Heap và stack

Câu trả lời của bạn sai.

The correct answer is:
Heap và stack

Question 21

Not answered

Marked out of 1.00

Cho mô tả sau: User Nam có quyền đọc và ghi trên file bt1. Nam cũng có quyền đọc trên file bt2 và có quyền thực thi trên file bt3.

User Ha có quyền đọc trên file bt1. Hà có quyền đọc và ghi trên file bt2. Hà không có quyền truy cập trên file bt3.

Xác định **CList** (Capability list) đối với user **Ha**?

	bt1	bt2	bt3
Hà	đọc	đọc ghi	không quyền

- a. CList(Ha) = bt1: {read}, bt2: {read, write}, bt3: {read, write}
- b. CList(Ha) = bt1: {read}, bt2: {read, write}, bt3: {}
- c. CList(Ha) = bt1: {}, bt2: {write}, bt3: {}
- d. CList(Ha) = bt1: {read, write}, bt2: {write}, bt3: {read}
- e. CList(Ha) = bt1: {read, write}, bt2: {read, write}, bt3: {}

Câu trả lời của bạn sai.

The correct answer is:
CList(Ha) = bt1: {read}, bt2: {read, write}, bt3: {}

Question 22

Not answered

Marked out of 1.00

John muốn thêm luật (rule) vào ACL cho tệp script00.sh để cấp cho student04 quyền đọc và ghi đối với tệp đó. Lệnh nào sau đây được thực hiện?

setfacl = set access control list cho 1 file hay folder
-m; tạo mới hoặc modified
-x: tùy chọn xóa

- a. getfacl -m u:student04:rw- script00.sh
- b. setfacl -m u:student04:rw- script00.sh
- c. setfacl -x u:student04:rw- script00.sh
- d. getfacl -x u:student04:rw- script00.sh

Câu trả lời của bạn sai.

The correct answer is:
setfacl -m u:student04:rw- script00.sh

Question 23

Not answered

Marked out of 1.00

Giải pháp StackGuard giúp phòng chống tấn công tràn bộ đệm trên stack thực hiện như sau

- a. Sử dụng một vùng nhớ đệm an toàn giữa Return Address và Buffer. Sử dụng vùng nhớ đệm an toàn này để kiểm tra xem Return Address có bị sửa đổi hay không
- b. Lưu trữ giá trị Return Address ở một nơi khác và sử dụng nó để kiểm tra xem giá trị ở Return Address có bị sửa đổi hay không
- c. Kiểm tra giá trị Return Address có bị sửa đổi hay không
- d. Kiểm tra chiều dài dữ liệu nhập trước khi thực hiện việc gán dữ liệu

Câu trả lời của bạn sai.

The correct answer is:
Sử dụng một vùng nhớ đệm an toàn giữa Return Address và Buffer. Sử dụng vùng nhớ đệm an toàn này để kiểm tra xem Return Address có bị sửa đổi hay không

Question 24

Not answered

Marked out of 1.00

Mục tiêu chính của an toàn thông tin là đảm bảo các tính chất theo mô hình **C-I-A** là?

- a. Tính sẵn sàng
- b. Tính dễ mở rộng
- c. Tính xác thực
- d. Tính toàn vẹn
- e. Tính bí mật
- f. Tính chống chối bỏ

Câu trả lời của bạn sai.

The correct answers are:
Tính sẵn sàng, Tính toàn vẹn, Tính bí mật

Question 25

Not answered

Marked out of 1.00

Trong tổ chức bộ nhớ của chương trình C, phần Data-Segment lưu các thông tin gì của chương trình?

- a. Lưu mã nguồn thực thi
- b. Lưu các biến static/global đã được khởi tạo trong chương trình
- c. Lưu các biến static/global chưa được khởi tạo trong chương trình
- d. Lưu các đối số của một hàm
- e. Lưu các biến cục bộ trong chương trình

Câu trả lời của bạn sai.

The correct answer is:
Lưu các biến static/global đã được khởi tạo trong chương trình

Question 26

Not answered

Marked out of 1.00

Phần nào trong kiến trúc bộ nhớ lưu trữ biến cục bộ trong chương trình, các dữ liệu liên quan đến lời gọi hàm?

- a. Stack
- b. Heap
- c. BSS segment
- d. Text
- e. Data Segment

Câu trả lời của bạn sai.

The correct answer is:
Stack

Question 27

Not answered

Marked out of 1.00

Mục đích chính của các kỹ thuật điều khiển truy cập là?

- a. Cung cấp tất cả các quyền truy cập cho người dùng
- b. Bảo vệ máy tính khỏi virus
- c. Ngăn chặn người dùng trái phép truy cập vào tài nguyên hệ thống
- d. Giới hạn các quyền truy cập và các hành động cho người dùng hợp pháp được sử dụng

Câu trả lời của bạn sai.

The correct answer is:
Giới hạn các quyền truy cập và các hành động cho người dùng hợp pháp được sử dụng

Question 28

Not answered

Marked out of 1.00

Cho hai số nguyên tố p=13, q=19, giá trị e nào sẽ được chọn trong thuật toán mã hóa RSA từ số các giá trị sau:

- a. 47
- b. 27
- c. 39
- d. 21

n = p.q = 247
N = (p-1)(q-1)=12*18=216
chọn 1 < e < n=247 sao cho gcd(e,N) = 1

cách ấn casio: alpha + x ra GCD()

Câu trả lời của bạn sai.

The correct answer is:
47

Question 29

Not answered

Marked out of 1.00

Giả sử thuật toán RSA đã tạo ra cặp khóa pubic (7,187) và private (23,187). Message M= 12 sẽ được mã hóa thành gì?

- a. 17
- b. 121
- c. 177
- d. 133

e = 7
d = 23
n = 187
c = m^e mod n = 177
m = c^d mod n

Câu trả lời của bạn sai.

The correct answer is:
177

Question 30

Not answered

Marked out of 1.00

e = 7 d = 23

Giả sử thuật toán RSA đã tạo ra cặp khóa pubic (7,187) và private (23,187). Muốn tạo chữ kí cho message M= 3 sẽ được tính là?

- a. 181
- b. 121
- c. 23
- d. 137

chuki = m^d mod n = 3^16 mod 187 * 3^4 mod 187 * 3^3 mod 187
= (69 * 81 * 27) mod 187 = 181

Câu trả lời của bạn sai.

The correct answer is:
181

Question 31

Not answered

Marked out of 1.00

Trong mã hóa bất đối xứng (còn gọi là mã hóa hóa công khai). Bob muốn tạo 1 chữ ký cho văn bản M để gửi cho Alice. Bob cần dùng khóa gì?

- a. Khóa Private của Bob
- b. Khóa Private của Alice
- c. Khóa Public của Alice
- d. Khóa Public của Bob

Câu trả lời của bạn sai.

The correct answer is:
Khóa Private của Bob

Question 32

Not answered

Marked out of 1.00

Trong mã hóa bất đối xứng (còn gọi là mã hóa hóa công khai). Alice cần **giải mã** văn bản mà Bob gửi cho thì Alice cần dùng khóa gì?

trong mã hóa bất đối xứng nếu bob muốn gửi cho alice thì dùng khóa public của alice mã hóa rồi alice sẽ dùng khóa private của mình để giải mã

- a. Khóa Public của Alice
- b. Khóa Private của Bob
- c. Khóa Private của Alice
- d. Khóa Public của Bob

Câu trả lời của bạn sai.

The correct answer is: Khóa Private của Alice

Question 33

Not answered

Marked out of 1.00

Thuật toán DES – Data Encryption Standard có kích thước khối, kích thước khóa gì?

- a. Khối 56bit, khóa 48bit
- b. Khối 64bit, khóa 56bit
- c. Khối 64bit, khóa 48bit
- d. Khối 56bit, khóa 48bit

Câu trả lời của bạn sai.

The correct answer is:
Khối 64bit, khóa 56bit

Question 34

Not answered

Marked out of 1.00

Diffie - Hellman là thuật toán dùng để:

- a. Tạo khoá
- b. Hash
- c. Trao đổi khóa
- d. Mã hóa

Câu trả lời của bạn sai.

The correct answer is:
Trao đổi khóa

Question 35

Not answered

Marked out of 1.00

Để đảm bảo tính toàn vẹn của message, các giải pháp nào được dùng? (chọn 2)

- a. Mã hóa đối xứng
- b. Hash
- c. MAC – Message Authentication code
- d. Mã hóa khối

Câu trả lời của bạn sai.

The correct answers are:
Hash, MAC – Message Authentication code

Question 36

Not answered

Marked out of 1.00

Tấn công nào sau đây là tấn công bị động (passive)

- a. Ransomeware
- b. Crack password
- c. DoS
- d. Scan port

Câu trả lời của bạn sai.

The correct answer is:
Scan port

Question 37

Not answered

Marked out of 1.00

Đắc điểm của tấn công chủ động (active)

- a. Dễ ngăn chặn
- b. Không ảnh hưởng đến hệ thống
- c. Khó phát hiện
- d. Dễ phát hiện

Câu trả lời của bạn sai.

The correct answer is:
Dễ phát hiện

Question 38

Not answered

Marked out of 1.00

Mã độc Rootkit thường trú ẩn ở đâu?

- a. Text file
- b. Boot Sector
- c. Hệ điều hành
- d. RAM

Câu trả lời của bạn sai.

The correct answer is:
Hệ điều hành

Question 39

Not answered

Marked out of 1.00

Tấn công nào vượt qua được cơ chế bảo mật máy tính để truy cập vào máy tính không thông qua hệ thống xác thực?

- a. Front door
- b. Backdoor
- c. Brute Force
- d. DoS

Câu trả lời của bạn sai.

The correct answer is:
Backdoor

Question 40

Not answered

Marked out of 1.00

John muốn thêm luật (rule) vào ACL cho tệp script00.sh để cấp cho nhóm **sysop** quyền đọc và thực thi đối với tệp đó. Lệnh nào sau đây được thực hiện?

- a. setfacl -x o:sysop:r-x script00.sh
- b. setfacl -x g:sysop:r-x script00.sh
- c. setfacl -m u:sysop:r-x script00.sh
- d. setfacl -m g:sysop:r-x script00.sh

Câu trả lời của bạn sai.

The correct answer is:
setfacl -m g:sysop:r-x script00.sh

Question 41

Not answered

Marked out of 1.00

Tấn công nào sau đây là tấn công chủ động (active)

- a. Sniffing lắng nghe và thu thập dữ liệu
- b. DoS
- c. Scan port quét các cổng được mở
- d. ping

Câu trả lời của bạn sai.

The correct answer is:
DoS

Question 42

Not answered

Marked out of 1.00

Thành phần nào KHÔNG phải là của virus?

- a. Cơ chế lây nhiễm
- b. Payload - những gì nó làm, độc hại hay lành tính
- c. Password
- d. Trigger - sự kiện làm cho payload được kích hoạt

Câu trả lời của bạn sai.

The correct answer is:
Password

Question 43

Not answered

Marked out of 1.00

Hai dạng mã độc nào sau đây sống độc lập?

- a. Zombie máy bụ nhiễm virus và bị máy khác điều khiển
- b. Trojan
- c. Rootkit
- d. Logic boom
- e. Worm tự động nhân bản

Câu trả lời của bạn sai.

The correct answers are:
Worm, Zombie

Question 44

Not answered

Marked out of 1.00

Mã độc nào KHÔNG lây nhiễm?

- a. Zombie
- b. Trojan
- c. Worm
- d. Virus

Câu trả lời của bạn sai.

The correct answer is:
Trojan

Question 45

Not answered

Marked out of 1.00

Metamorphic virus có đặc điểm gì?

- a. Lẩn tránh phát hiện nhờ thông minh
- b. Lẩn tránh phát hiện thông qua nén kích thước
- c. Lẩn tránh phát hiện nhờ mã hóa
- d. Lẩn tránh phát hiện thông qua việc ghi đè lên chính nó

Câu trả lời của bạn sai.

The correct answer is:
Lẩn tránh phát hiện thông qua việc ghi đè lên chính nó

Question 46

Not answered

Marked out of 1.00

Firewall lọc gói dữ liệu dựa vào những yếu tố nào?

- a. Hệ điều hành của server
- b. Vị trí đặt server
- c. IP nguồn, IP đích
- d. Đường link

Câu trả lời của bạn sai.

The correct answer is:
IP nguồn, IP đích

Question 47

Not answered

Marked out of 1.00

Một hệ thống xác thực sinh trắc học xác định một người dùng hợp pháp là trái phép khi vào hệ thống là hiện tượng gì sau?

a. True negative
b. True positive
c. False negative
d. False positive

Câu trả lời của bạn sai.

The correct answer is:
False positive

Question 48

Not answered

Marked out of 1.00

Một hệ thống xác thực sinh trắc học cho phép một người giả mạo hình thức nhân viên công ty khi vào hệ thống là hiện tượng gì sau?

a. False positive
b. False negative
c. True positive
d. True negative

Câu trả lời của bạn sai.

The correct answer is: False negative

Question 49

Not answered

Marked out of 1.00

Ví dụ nào sau đây là ví dụ về xác thực hai yếu tố?

- a. Thumbprint và card
- b. Client và server
- c. Username và password
- d. L2TP và IpSec

Cái mà bạn biết (Something you know): Ví dụ như mật khẩu, mã PIN.
Cái mà bạn có (Something you have): Ví dụ như thẻ bảo mật, điện thoại di động.
Cái mà bạn là (Something you are): Ví dụ như dấu vân tay (thumbprint), nhận diện khuôn mặt.
thuộc 2 trong 3
đấu vân tay (sth you are) card (sth u have) 2FA

Câu trả lời của bạn sai.

The correct answer is: Thumbprint và card

Question 50

Not answered

Marked out of 1.00

Hệ thống phát hiện xâm nhập dựa vào dấu hiệu (Signature-based IDS) hoạt động dựa vào yếu tố nào?

- a. Các dấu hiệu tấn công
- b. Các dấu hiệu bất thường
- c. Nội dung website
- d. Các dấu hiệu bình thường

IDS: xác định bất thường nhưng không ngăn chặn
IPS: xác định bất thường và ngăn chặn nó

Câu trả lời của bạn sai.

The correct answer is:
Các dấu hiệu tấn công

Question 51

Not answered

Marked out of 1.00

Hệ thống phát hiện xâm nhập dựa vào bất thường (Anomaly-based IDS) hoạt động dựa vào yếu tố nào?

a. Nội dung website xấu
b. Các hành vi bình thường
c. Các hành vi bất thường
d. Các tấn công

Câu trả lời của bạn sai.

The correct answer is:
Các hành vi bình thường

Question 52

Not answered

Marked out of 1.00

Chế độ hoạt động nào sau đây mã hóa các khối một cách riêng biệt?

a. Cipher block chaining mode - CBC
b. Cipher feedback mode - CFB
c. Electronic codebook mode - ECB
d. Output feedback mode – OFB

Câu trả lời của bạn sai.

The correct answer is: Electronic codebook mode - ECB

Question 53

Not answered

Marked out of 1.00

Chuẩn nào sau đây liên quan đến an toàn thông tin?

a. ISO 2015
b. ISO 27001
c. ISO 2600
d. ISO 9001

Câu trả lời của bạn sai.

The correct answer is: ISO 27001

Question 54

Not answered

Marked out of 1.00

Nam làm hỏng máy tính của Lan, tính chất nào sau đây bị vi phạm? (chọn 2)

- a. Tính sẵn sàng
- b. Tính toàn vẹn
- c. Tính bí mật
- d. Tính xác thực
- e. Tính chống chối bỏ

Câu trả lời của bạn sai.

The correct answers are:
Tính sẵn sàng, Tính toàn vẹn

Question 55

Not answered

Marked out of 1.00

Mô hình Bell La Padula (BLP) qui định cách truy xuất thông tin là gì

- a. No read down, no write down
- b. No read up, no write up
- c. No read down, no write up
- d. No read up, no write down

Câu trả lời của bạn sai.

The correct answer is:
No read up, no write down

Started on	Thursday, 1 June 2023, 11:00 PM
State	Finished
Completed on	Thursday, 1 June 2023, 11:00 PM
Time taken	7 secs
Marks	0.00/50.00
Grade	**0.00** out of 10.00 (**0**%)

Question 1

Not answered

Marked out of 1.00

Cho mô tả sau:

User Nam có quyền đọc và ghi trên file bt1. Nam cũng có quyền đọc trên file bt2 và có quyền thực thi trên file bt3.

User Ha có quyền đọc trên file bt1. Hà có quyền đọc và ghi trên file bt2. Hà không có quyền truy cập trên file bt3.

Xác định CList (Capability list) đối với user Ha?

- a. CList(Ha) = bt1: {read, write}, bt2: {read, write}, bt3: {}
- b. CList(Ha) = bt1: {read}, bt2: {read, write}, bt3: {read, write}
- c. CList(Ha) = bt1: {read}, bt2: {read, write}, bt3: {}
- d. CList(Ha) = bt1: {read, write}, bt2: {write}, bt3: {read}
- e. CList(Ha) = bt1: {}, bt2: {write}, bt3: {}

Your answer is incorrect.

The correct answer is:
CList(Ha) = bt1: {read}, bt2: {read, write}, bt3: {}

Question 2

Not answered

Marked out of 1.00

Để nâng cao việc phát triển các giải pháp an toàn cho một hệ thống CNTT, người ta tập trung đầu tư vào 3 vấn đề chính là?

- a. Tăng chi phí đầu tư cho bảo mật
- b. Đội ngũ chuyên gia bảo mật
- c. Công nghệ
- d. Con người
- e. Quy trình
- f. Đào tạo nâng cao nhận thức

ppt (people - process - technology)

Your answer is incorrect.

The correct answers are:
Con người,

Quy trình,

Công nghệ

Question 3

Not answered

Marked out of 1.00

Hệ thống phát hiện xâm nhập dựa vào dấu hiệu (Signature-based IDS) hoạt động dựa vào yếu tố nào?

- a. Các dấu hiệu bình thường
- b. Các dấu hiệu bất thường
- c. Các dấu hiệu tấn công
- d. Nội dung website

Your answer is incorrect.

The correct answer is:
Các dấu hiệu tấn công

Question 4

Not answered

Marked out of 1.00

Một hệ thống kiểm soát truy cập chỉ cấp cho người dùng những quyền cần thiết để họ thực hiện công việc đang hoạt động theo nguyên tắc bảo mật nào?

- a. Discretionary Access Control
- b. Least Privilege
- c. Separation of Duties
- d. Mandatory Access Control

Your answer is incorrect.

The correct answer is:
Least Privilege

Question 5

Not answered

Marked out of 1.00

address resolution protocol

Điều gì xảy ra khi máy X sử dụng kỹ thuật ARP spoofing để nghe lén thông tin từ máy Y?

a. X giả mạo địa chỉ IP của Y

b. Y giả mạo địa chỉ MAC của X

c. Y giả mạo địa chỉ IP của X

d. X giả mạo địa chỉ MAC của Y

arp là 1 giao thức chuyển từ tầng network sang data link
đặc trưng tầng network là IP, còn datalink là MAC
arp request là gửi 1 gói tin chứa IP add và yêu cầu mac gói tin này
arp reply là phản hồi 1 gói tin và cung cấp mac theo ip yêu cầu

ARP spoofing là 1 kĩ thuật mà người tấn công giả mạoMAC của máy nạn nhân bằng cách gửi gói tin ARP reply có địa chỉ chứa MAC của nó

Your answer is incorrect.

The correct answer is:
X giả mạo địa chỉ MAC của Y

Question 6

Not answered

Marked out of 1.00

Kiểu tấn công nào sau đây **không** phải khai thác các lỗ hổng của ứng dụng Web?

- a. Cross Site Request Forgery
- b. Cross-site scripting
- c. SQL Injection
- d. Social Engineering

Your answer is incorrect.

The correct answer is:
Social Engineering

Question 7

Not answered

Marked out of 1.00

Tấn công DoS/DDoS làm ảnh hưởng đến tiêu chuẩn nào của an toàn thông tin?

- a. Tính sẵn sàng
- b. Tính toàn vẹn
- c. Tính xác thực
- d. Tính bí mật
- e. Tính chống thoái thác

Your answer is incorrect.

The correct answer is:
Tính sẵn sàng

Question 8

Not answered

Marked out of 1.00

Giải pháp Stackshield giúp phòng chống tấn công tràn bộ đệm trên stack thực hiện như sau:

a. Sử dụng một vùng nhớ đệm an toàn giữa Return Address và Buffer. Sử dụng vùng nhớ đệm an toàn này để kiểm tra xem Return Address có bị sửa đổi hay không

b. Kiểm tra giá trị Return Address có bị sửa đổi hay không

c. Lưu trữ giá trị Return Address ở một nơi khác và sử dụng nó để kiểm tra xem giá trị ở Return Address có bị sửa đổi hay không

d. Kiểm tra chiều dài dữ liệu nhập trước khi thực hiện việc gán dữ liệu

Your answer is incorrect.

The correct answer is:
Lưu trữ giá trị Return Address ở một nơi khác và sử dụng nó để kiểm tra xem giá trị ở Return Address có bị sửa đổi hay không

Question 9

Not answered

Marked out of 1.00

Điều nào sau đây là rủi ro tiềm ẩn khi chương trình chạy ở chế độ đặc quyền?

- a. Nó có thể phục vụ cho việc tạo ra các đoạn mã phức tạp không cần thiết
- b. Nó có thể tạo ra việc loại bỏ các ứng dụng không cần thiết
- c. Nó có thể cho phép mã độc được chèn vào
- d. Nó có thể không thực hiện việc phân chia xử lý các tác vụ

Your answer is incorrect.

The correct answer is:
Nó có thể cho phép mã độc được chèn vào

Question 10

Not answered

Marked out of 1.00

Việc gỡ bỏ những dịch vụ và giao thức không cần thiết gọi là?

- a. Hardening
- b. Cleaning
- c. Nonrepudiation
- d. Auditing
- e. Hashing

hardening có 6 việc:
vá phần mềm
khóa port ko xài
remove các dịch vụ ko xài
xóa các defaule accounr
set pass policy
phân quyền đủ dùng

Your answer is incorrect.

The correct answer is:
Hardening

Question 11

Not answered

Marked out of 1.00

Điều nào sau đây sẽ bảo vệ tốt nhất trước cuộc tấn công cụ SQL Injection?

- a. Lọc dữ liệu người dùng nhập vào
- b. Lưu lượng truy cập web được mã hóa
- c. Firewall
- d. IDS

Your answer is incorrect.

The correct answer is:
Lọc dữ liệu người dùng nhập vào

Question 12

Not answered

Marked out of 1.00

Mục đích chính của các kỹ thuật điều khiển truy cập là?

- a. Giới hạn các quyền truy cập và các hành động cho người dùng hợp pháp được sử dụng
- b. Ngăn chặn người dùng trái phép truy cập vào tài nguyên hệ thống
- c. Cung cấp tất cả các quyền truy cập cho người dùng
- d. Bảo vệ máy tính khỏi virus

Your answer is incorrect.

The correct answer is:
Giới hạn các quyền truy cập và các hành động cho người dùng hợp pháp được sử dụng

Question 13

Not answered

Marked out of 1.00

Giải pháp StackGuard giúp phòng chống tấn công tràn bộ đệm trên stack thực hiện như sau:

- a. Sử dụng một vùng nhớ đệm an toàn giữa Return Address và Buffer. Sử dụng vùng nhớ đệm an toàn này để kiểm tra xem Return Address có bị sửa đổi hay không
- b. Kiểm tra giá trị Return Address có bị sửa đổi hay không
- c. Lưu trữ giá trị Return Address ở một nơi khác và sử dụng nó để kiểm tra xem giá trị ở Return Address có bị sửa đổi hay không
- d. Kiểm tra chiều dài dữ liệu nhập trước khi thực hiện việc gán dữ liệu

Your answer is incorrect.

The correct answer is:
Sử dụng một vùng nhớ đệm an toàn giữa Return Address và Buffer. Sử dụng vùng nhớ đệm an toàn này để kiểm tra xem Return Address có bị sửa đổi hay không

Question 14

Not answered

Marked out of 1.00

Chuẩn nào sau đây liên quan đến an toàn thông tin?

- a. ISO 9001
- b. ISO 27001
- c. ISO 21997
- d. ISO 2600
- e. ISO 2015

Your answer is incorrect.

The correct answer is:
ISO 27001

Question 15

Not answered

Marked out of 1.00

Access control liên quan đến 2 chức năng chính là?

- a. Rule Based Access Control
- b. Least privilege principle
- c. Authorization
- d. Authentication
- e. Role Based Access Control

Your answer is incorrect.

The correct answers are:
Authentication,

Authorization

Question 16

Not answered

Marked out of 1.00

Công cụ nào dùng để quét cổng của máy tính

a. tracert

b. nmap

c. ping

d. nslookup

e. telnet

tracert: là show đường đi cụ thể của gói tin
nmap: dùng để quét cổng, quét mạng
ping: dùng kiểm tra kết nối giữa 2 máy trạm
nslookup: tìm IP từ tên miền
telnet: dùng quản trị mạng từ xa

Your answer is incorrect.

The correct answer is:
nmap

Question 17

Not answered

Marked out of 1.00

Trong HĐH Linux, để tắt chức năng phát sinh địa chỉ bộ nhớ ngẫu nhiên, sử dụng lệnh nào sau đây?

a. $sudo sysctl –w kernel.randomize_as_space=0

b. $sudo sysctl –w kernel.randomize_ram_space=0

c. $sudo sysctl –w kernel.randomize_store_space=0

d. $sudo sysctl –w kernel.randomize_va_space=0

e. $sudo sysctl –w kernel.randomize_sa_space=0

Your answer is incorrect.

The correct answer is:
$sudo sysctl –w kernel.randomize_va_space=0

Question 18

Not answered

Marked out of 1.00

Một máy chủ Web của một công ty được cấu hình các dịch vụ sau: HTTP, HTTPS, FTP, SMTP. Máy chủ này được đạt trong vùng DMZ. Những cổng nào cần phải mở trên Firewall để cho phép máy người dùng có thể sử dụng dịch vụ trên máy này?

- a. 434, 21, 80, 25, 20
- b. 80, 20, 21, 25, 443
- c. 110, 443, 21, 59, 25
- d. 119, 23, 21, 80, 23

Your answer is incorrect.

The correct answer is:
80, 20, 21, 25, 443

Question 19

Not answered

Marked out of 1.00

Trong an toàn thông tin, Ping Sweep được sử dụng để làm gì?

- a. Để xác định vị trí của các host đang hoạt động trên mạng
- b. Để xác định các cổng đang mở trên mạng
- c. Để xác định vị trí của các tường lửa trên mạng
- d. Để xác định các host đang hoạt động trên mạng

Your answer is incorrect.

The correct answer is:
Để xác định các host đang hoạt động trên mạng

Question 20

Not answered

Marked out of 1.00

Sắp xếp các thông tin cho đúng về độ dài đầu ra của các thuật toán mã hóa sau

DES	Choose...	64 bits
MD5	Choose...	128 bits
SHA-512	Choose...	512 bits
3DES	Choose...	64 bits
AES	Choose...	128 bits

Your answer is incorrect.

The correct answer is:
DES → 64bits,

MD5 → 128bits,

SHA-512 → 512bits,

3DES → 64bits,

AES → 128bits

Question 21

Not answered

Marked out of 1.00

Cơ chế kiểm soát truy cập nào cho phép chủ sở hữu dữ liệu tạo và quản lý kiểm soát truy cập?

- a. Attribute Based Access Control (ABAC) sử dụng các thuộc tính để xác định quyền truy cập
- b. Discretionary Access Control (DAC) cho phép chủ sở hữu control những gì mình sở hữu
- c. List Based Access Control (LBAC)
- d. Mandatory Access Control (MAC) chỉ hệ thống mới có quyền chỉnh sửa
- e. Role Based Access Control (RBAC) được truy cập theo quyền mà owner hoặc system cấp phát

Your answer is incorrect.

The correct answer is:
Discretionary Access Control (DAC)

Question 22

Not answered

Marked out of 1.00

Mục tiêu chính của an toàn thông tin là đảm bảo các tính chất theo mô hình C-I-A là?

- a. Tính chống chối bỏ
- b. Tính xác thực
- c. Tính dễ mở rộng
- d. Tính sẵn sàng
- e. Tính toàn vẹn
- f. Tính bí mật

Your answer is incorrect.

The correct answers are:
Tính bí mật,

Tính toàn vẹn,

Tính sẵn sàng

code segment (text) lưu code
bss segment: lưu các biến chưa khởi tạo
dss: lưu các biến đã được khởi tạo

Question 23

Not answered

Marked out of 1.00

Trong tổ chức bộ nhớ của chương trình C, phần Data-Segment lưu các thông tin gì của chương trình?

- a. Lưu các biến static/global chưa được khởi tạo trong chương trình
- b. Lưu các biến static/global đã được khởi tạo trong chương trình
- c. Lưu các đối số của một hàm
- d. Lưu các biến cục bộ trong chương trình
- e. Lưu mã nguồn thực thi

Your answer is incorrect.

The correct answer is:
Lưu các biến static/global đã được khởi tạo trong chương trình

Question 24

Not answered

Marked out of 1.00

Tại sao hacker hay sử dụng máy chủ proxy?

- a. Để tạo một máy chủ ma trên mạng
- b. Để ẩn hoạt động của chúng trên mạng
- c. Để tạo kết nối mạnh mẽ hơn với mục tiêu
- d. Để có được kết nối truy cập từ xa

Your answer is incorrect.

The correct answer is:
Để ẩn hoạt động của chúng trên mạng

Question 25

Not answered

Marked out of 1.00

Câu nào sau đây không phải là một cơ chế điều khiển truy cập?

- a. Role Based Access Control
- b. Mandatory Access Control (MAC)
- c. Discretionary Access Control (DAC)
- d. Subjective Access Control
- e. Attribute Based Access Control

Your answer is incorrect.

The correct answer is:
Subjective Access Control

Question 26

Not answered

Marked out of 1.00

Mô hình bảo mật theo chiều sâu (defense in depth) gồm các lớp bảo mật theo thứ tự từ trong ra ngoài là?

Layer 3	Choose...	host
Layer 4	Choose...	internal network
Layer 1	Choose...	data
Layer 2	Choose...	application
Layer 7	Choose...	policy, procedures,...
Layer 5	Choose...	perimeter
Layer 6	Choose...	physical

defense in depth
data > appplication > host > internal network > perimeter > physical > policy

DAHIPPP

Your answer is incorrect.

The correct answer is:
Layer 3 → Host security,

Layer 4 → LAN security,

Layer 1 → Data security,

Layer 2 → Application security,

Layer 7 → Policies, procedures, awareness,

Layer 5 → Perimeter security,

Layer 6 → Physical security

Question 27

Not answered

Marked out of 1.00

Điều nào sau đây KHÔNG đúng khi nói về lỗ hổng 0-day?

- a. Là lỗ hổng nguy hiểm khi tấn công vào hệ thống chưa có giải pháp bảo vệ
- b. Là lỗ hổng hacker chưa công bố rộng rãi
- c. Là lỗ hổng nhà sản xuất chưa kịp vá
- d. Là lỗ hổng phá hoại hệ thống trong vòng một ngày

Your answer is incorrect.

The correct answer is:
Là lỗ hổng phá hoại hệ thống trong vòng một ngày

Question 28

Not answered

Marked out of 1.00

Tấn công Buffer Overflow có hai loại là?

- a. Heap và network overflow
- b. SQL injection và XSS
- c. Stack và SQL injection
- d. Stack và memory
- e. Heap và stack

Your answer is incorrect.

The correct answer is:
Heap và stack

Question 29

Not answered

Marked out of 1.00

Trong mã hóa bất đối xứng (còn gọi là mã hóa hóa công khai). Alice cần **mã hóa** văn bản để gửi cho Bob thì Alice cần dùng khóa gì?

- a. Khóa Public của Bob
- b. Khóa Private của Bob
- c. Khóa Public của Alice
- d. Khóa Private của Alice

Your answer is incorrect.

The correct answer is:
Khóa Public của Bob

Question 30

Not answered

Marked out of 1.00

Phương pháp nào sau đây là TỐT NHẤT để giảm hiệu quả của các cuộc tấn công lừa đảo trên mạng?

- a. Quét lỗ hổng cho hệ thống định kỳ
- b. Phần mềm chống lừa đảo
- c. Đào tạo nâng cao nhận thức người dùng
- d. Xác thực 2 yếu tố

Your answer is incorrect.

The correct answer is:
Đào tạo nâng cao nhận thức người dùng

Question 31

Not answered

Marked out of 1.00

Cách tốt nhất để nhận ra hành vi bất thường và đánh ngờ trên hệ thống của bạn là gì?

- a. Nhận biết các cuộc tấn công mới
- b. Biết các hoạt động bình thường của hệ thống là như thế nào
- c. Cấu hình IDS để phát hiện và báo cáo tất cả các lưu lượng bất thường
- d. Nghiên cứu dấu hiệu hoạt động của các loại tấn công chính

Your answer is incorrect.

The correct answer is:
Biết các hoạt động bình thường của hệ thống là như thế nào

Question 32

Not answered

Marked out of 1.00

Trong các giao thức dưới đây, giao thức nào cho phép xác thực user khi user gắn thiết bị vào port layer 2?

- a. Radius
- b. 802.3D
- c. 802.11X
- d. 802.3

Your answer is incorrect.

The correct answer is:
Radius

Question 33

Not answered

Marked out of 1.00

Mô hình AAA liên quan đến các chứng năng nào sau đây?

- a. Authentication
- b. Authorization
- c. Automation
- d. Accounting
- e. Authenticity
- f. Accessing

Your answer is incorrect.

The correct answers are:
Authentication,

Authorization,

Accounting

Question 34

Not answered

Marked out of 1.00

Một hệ thống xác thực sinh trắc học cho phép một người giả mạo hình thức nhân viên công ty khi vào hệ thống là hiện tượng gì sau?

- a. False positive
- b. False negative
- c. True negative
- d. True positive

Your answer is incorrect.

The correct answer is:
False negative

Question 35

Not answered

Marked out of 1.00

Trong mã hóa bất đối xứng (còn gọi là mã hóa hóa công khai). Bob muốn **tạo chữ ký** cho văn bản M để gửi cho Alice. Bob cần dùng khóa gì?

a. Khóa Public của Bob

b. Khóa Private của Alice

c. Khóa Private của Bob

d. Khóa Public của Alice

Your answer is incorrect.

The correct answer is:
Khóa Private của Bob

Question 36

Not answered

Marked out of 1.00

1Cho mô tả sau:

User Nam có quyền đọc và ghi trên file bt1. Nam cũng có quyền đọc trên file bt2 và có quyền thực thi trên file bt3.

User Ha có quyền đọc trên file bt1. Hà có quyền đọc và ghi trên file bt2. Hà không có quyền truy cập trên file bt3.

Xác định ACL (Access control list) đối với file bt2?

- a. ACL(bt2) = Nam: {read}, Ha: {read, write}
- b. ACL(bt2) = Nam: {read, write}, Ha: {read}
- c. ACL(bt2) = Nam: {read, write}, Ha: {read, write}
- d. ACL(bt2) = Nam: {read, execute}, Ha: {read, write}
- e. ACL(bt2) = Nam: {read}, Ha: {read}

Your answer is incorrect.

The correct answer is:
ACL(bt2) = Nam: {read}, Ha: {read, write}

Question 37

Not answered

Marked out of 1.00

Giao thức nào sau đây được dùng để mã hóa dữ liệu trao đổi giữa Web Browser và Web server?

- a. HTTP
- b. SMTP
- c. SSL/TLS
- d. VPN
- e. IPSec

Your answer is incorrect.

The correct answer is:
SSL/TLS

Question 38

Not answered

Marked out of 1.00

Tấn công nào có thể bỏ qua hệ thống xác thực để truy cập vào máy tính?

- a. Brute Force
- b. Front door
- c. Backdoor
- d. DoS

Your answer is incorrect.

The correct answer is:
Backdoor

Question 39

Not answered

Marked out of 1.00

Hai dạng mã độc nào sau đây sống độc lập?

- a. Worm
- b. Logic boom
- c. Trojan
- d. Zombie
- e. Rootkit

Your answer is incorrect.

The correct answers are:
Zombie,

Worm

Question 40

Not answered

Marked out of 1.00

Các khối xử lý nào được dùng trong mã hóa đối xứng AES? (chọn 3)

- a. ShiftRows
- b. Shif left
- c. SubBytes
- d. Straight P-box
- e. Compression P-box
- f. MixRows

subbytes
shiftrow
mixcolumn

Your answer is incorrect.

The correct answers are:
ShiftRows,

SubBytes,

MixRows

Question 41

Not answered

Marked out of 1.00

Tại sao các nhà phát triển phần mềm đính kèm theo các giá trị băm bằng hàm MD5 của các gói cập nhật cho phần mềm cùng với các gói đó để các khách hàng của họ có thể download từ Internet?

- a. Khách hàng có thể yêu cầu các bản cập nhật mới cho phần mềm trong tương lai bằng cách sử dụng giá trị hàm băm đính kèm theo
- b. Khách hàng cần giá trị của hàm băm để có thể kích hoạt được phần mềm mới
- c. Khách hàng có thể khẳng định tính xác thực của Site mà họ download gói cập nhật về
- d. Khách hàng có thể xác thực tính toàn vẹn và gói cập nhật cho phần mềm sau khi download về

Your answer is incorrect.

The correct answer is:
Khách hàng có thể xác thực tính toàn vẹn và gói cập nhật cho phần mềm sau khi download về

Question 42

Not answered

Marked out of 1.00

Chế độ hoạt động nào sau đây mã hóa các khối một cách riêng biệt?

- a. Output feedback mode – OFB
- b. Cipher block chaining mode - CBC
- c. Electronic codebook mode - ECB
- d. Cipher feedback mode - CFB

Your answer is incorrect.

The correct answer is:
Electronic codebook mode - ECB

Question 43

Not answered

Marked out of 1.00

Từ ma trận điều khiển truy cập, ta có thể suy ra các thông tin nào sau đây?

- a. Capability lists
- b. Group policy objects
- c. Objects orientation list
- d. Subjects orientation lists
- e. Access control lists

Your answer is incorrect.

The correct answers are:
Access control lists,

Capability lists

Question 44

Not answered

Marked out of 1.00

Mục đích chính của chương trình nâng cao nhận thức bảo mật là?

- a. Cảnh báo tất cả người dùng truy cập vào tất cả các hệ thống sẽ được theo dõi hàng ngày
- b. Thông báo cho người dùng để tuân thủ các quy định liên quan đến bảo vệ dữ liệu và thông tin
- c. Đảm bảo rằng mọi người đều hiểu chính sách và thủ tục của tổ chức
- d. Thông báo cho mọi người rằng quyền truy cập vào thông tin sẽ được cấp khi người sử dụng có yêu cầu

Your answer is incorrect.

The correct answer is:
Đảm bảo rằng mọi người đều hiểu chính sách và thủ tục của tổ chức

Question 45

Not answered

Marked out of 1.00

Loại malware nào sau đây có thể ẩn các tiến trình và các tập tin trên hệ thống?

- a. Trojan
- b. Adware
- c. Worm
- d. Rootkit

Your answer is incorrect.

The correct answer is:
Rootkit

Question 46

Not answered

Marked out of 1.00

Diffie - Hellman là thuật toán dùng để

a. Tạo khoá

b. Giải mã khóa

c. Mã hóa khóa

d. Hash khóa

e. Trao đổi khóa

Your answer is incorrect.

The correct answer is:
Trao đổi khóa

Question 47

Not answered

Marked out of 1.00

Ma trận điều khiển truy cập (Access control matrix) thể hiện mối quan hệ giữa các thành phần nào sau đây?

- a. Subject
- b. Object
- c. Database
- d. Rights/Permissions
- e. Security policy
- f. Users

Your answer is incorrect.

The correct answers are:
Subject,

Object,

Rights/Permissions

Question 48

Not answered

Marked out of 1.00

Điều nào sau đây mô tả tốt nhất cơ chế kiểm soát truy cập trong đó các quyết định kiểm soát truy cập dựa trên trách nhiệm của người dùng trong một tổ chức?

- a. RBAC (Role Based Access Control)
- b. MAC (Mandatory Access Control)
- c. Rule Based Access Control
- d. Attribute Based Access Control
- e. DAC (Discretionary Access Control)

Your answer is incorrect.

The correct answer is:
RBAC (Role Based Access Control)

Question 49

Not answered

Marked out of 1.00

Tấn công một máy tính bằng cách gửi các gói TCP handshake không đúng thứ tự đến đích (wrong order) xảy ra ở tầng nào?

- a. Internet layer
- b. Network layer
- c. Application layer
- d. Transport layer
- e. Network Interface layer

Your answer is incorrect.

The correct answer is:
Transport layer

Question 50

Not answered

Marked out of 1.00

Thuật toán mật mã nào sau đây dựa trên độ khó của bài toán phân tích các số lớn thành tích của hai thừa số nguyên tố ban đầu?

- a. DES
- b. RSA
- c. Diffie-Hellman
- d. ECC

Your answer is incorrect.

The correct answer is:
RSA

THẦY CHÍNH

Access control liên quan đến 2 chức năng chính là?=>C,R

Câu hỏi 1

Chưa trả lời

Đạt điểm 1,00

Đặt cờ

Access control liên quan đến 2 chức năng chính là?

- a. Role Based Access Control
- b. Least privilege principle
- c. Authentication
- d. Rule Based Access Control
- e. Authorization

authentication
authorization

Mục đích chính của chương trình nâng cao nhận thức bảo mật là?=>B

Câu hỏi 2

Chưa trả lời

Đạt điểm 1,00

Đặt cờ

Mục đích chính của chương trình nâng cao nhận thức bảo mật là?

- a. Thông báo cho người dùng để tuân thủ các quy định liên quan đến bảo vệ dữ liệu và thông tin
- b. Đảm bảo rằng mọi người đều hiểu chính sách và thủ tục của tổ chức yup
- c. Thông báo cho mọi người rằng quyền truy cập vào thông tin sẽ được cấp khi người sử dụng có yêu cầu
- d. Cảnh báo tất cả người dùng truy cập vào tất cả các hệ thống sẽ được theo dõi hàng ngày

Ma trận điều khiển truy cập thể hiện mối quan hệ giữa các thành phần nào sau đây? => A,D,E

Câu hỏi 3

Chưa trả lời

Đạt điểm 1,00

Đặt cờ

Ma trận điều khiển truy cập (Access control matrix) thể hiện mối quan hệ giữa các thành phần nào sau đây?

- [ ] a. Rights/Permissions yup
- [ ] b. Security policies
- [ ] c. Data
- [x] d. Objects yup
- [x] e. Subjects yup

Giải pháp StackGuard giúp phòng chống tấn công tràn bộ đêm trên stack thực hiện như sau: =>D tạo 1 vùng đệm trc return add để ktra

Câu hỏi 4

Chưa trả lời

Đạt điểm 1,00

Đặt cờ

Giải pháp StackGuard giúp phòng chống tấn công tràn bộ đệm trên stack thực hiện như sau:

- a. Lưu trữ giá trị Return Address ở một nơi khác và sử dụng nó để kiểm tra xem giá trị ở Return Address có bị sửa đổi hay không.
- b. Kiểm tra chiều dài dữ liệu nhập trước khi thực hiện việc gán dữ liệu
- c. Kiểm tra giá trị Return Address có bị sửa đổi hay không
- d. Sử dụng một vùng nhớ đệm an toàn giữa Return Address và Buffer. Sử dụng vùng nhớ đệm an toàn này để kiểm tra xem Return Address có bị sửa đổi hay không. yup

Frank rất quan tâm……. =>C sql injection là việc mà người tấn công nhập nhưng dãy không mong muốn vào dữ liệu vào để lấy quyền ks của 1 user hay admin

Câu hỏi 5

Chưa trả lời

Đạt điểm 1,00

Đặt cờ

Frank rất quan tâm đến các cuộc tấn công vào máy chủ thương mại điện tử của công ty. Ông đặc biệt lo lắng về tấn công SQL Injection. Điều nào sau đây sẽ bảo vệ tốt nhất trước cuộc tấn công cụ thể này?

- a. IDS
- b. Lưu lượng truy cập web được mã hóa
- c. Lọc dữ liệu người dùng nhập vào yep
- d. Firewall

Từ ma trận điều khiển truy cập, ta có thể suy ra các thông tin nào sau đây?=>A,C

Câu hỏi 6

Chưa trả lời

Đạt điểm 1,00

Đặt cờ

Từ ma trận điều khiển truy cập, ta có thể suy ra các thông tin nào sau đây?

- a. Access control lists ACL: những quyền mà người đó có trên 1 file, 1 folder (1 object đối với nhiều subject)
- b. Objects orientation list
- c. Capability lists CL: những quyền người dó có trên các file liệt kê (subject) (nhiều obect cho 1 subject_
- d. Group policy objects
- e. Subjects orientation lists

Cho mô tả sau:

Câu hỏi 7

Chưa trả lời

Đạt điểm 1,00

Đặt cờ

Cho mô tả sau: User Nam có quyền đọc và ghi trên file bt1. Nam cũng có quyền đọc trên file bt2 và có quyền thực thi trên file bt3.

User Ha có quyền đọc trên file bt1. Hà có quyền đọc và ghi trên file bt2. Hà không có quyền truy cập trên file bt3.

Xác định ACL (Access control list) đối với file bt2?

- a. ACL(bt2) = Nam: {read, write}, Ha: {read}
- b. ACL(bt2) = Nam: {read}, Ha: {read, write} yep
- c. ACL(bt2) = Nam: {read, write}, Ha: {read, write}
- d. ACL(bt2) = Nam: {read, execute}, Ha: {read, write}
- e. ACL(bt2) = Nam: {read}, Ha: {read}

	Bt1	Bt2	Bt3
Nam	Read, write	Read	Execute
Ha	Read	Read, write	-

ACL(bt2) = Nam: {Read}, Ha: {Read, write}

Câu nào sau đây không phải là một mô hình điều khiển truy cập?=>B

Câu hỏi 8
Chưa trả lời
Đạt điểm 1,00
Đặt cờ

Câu nào sau đây không phải là một mô hình điều khiển truy cập?

- a. Discretionary Access Control (DAC)
- b. Subjective Access Control yep
- c. Role Based Access Control
- d. Mandatory Access Control (MAC)
- e. Attribute Based Access Control

Mô hình AAA liên quan đến các chức năng nào sau đây?=>B,C,F

Câu hỏi 9
Chưa trả lời
Đạt điểm 1,00
Đặt cờ

Mô hình AAA liên quan đến các chứng năng nào sau đây?

- [ ] a. Automation
- [ ] b. Authorization yep
- [ ] c. Authentication yep
- [ ] d. Authenticity
- [ ] e. Accessing
- [ ] f. Accounting yep

Nếu bạn chưa sẻ quá nhiều thông tin trên phương tiện truyền thông xã hội, bạn có thể gặp rủi ro gì?=>C

Câu hỏi 10
Chưa trả lời
Đạt điểm 1,00
Đặt cờ

Nếu bạn chia sẻ quá nhiều thông tin trên phương tiện truyền thông xã hội, bạn có thể gặp rủi ro gì?

- a. Đánh cắp danh tính (Identity theft)
- b. Ransomware
- c. Tấn công giả mạo (Phishing) yep: tấn công dựa trên những gì nhười dùng chia sẽ trên các mxh
- d. Mã độc (malware)

Điều nào sau đây xảy ra khi một chuỗi dữ liệu được gửi đến bộ đệm lớn hơn bộ đệm được thiết kế để xử lý?=>A

Câu hỏi 11
Chưa trả lời
Đạt điểm 1,00
Đặt cờ

Điều nào sau đây xảy ra khi một chuỗi dữ liệu được gửi đến bộ đệm lớn hơn bộ đệm được thiết kế để xử lý?

- a. Buffer overflow yep
- (•) b. Brute Force attack
- c. Man in the middle attack lằng nghe
- d. SYN flood gửi nhiều gói syn liên tiếp khiến server ko còn khà năng phản hồi lại gói thực tế của user
- e. Spoofing attack

Clear my choice

Theo bạn giải pháp nào cần được áp dụng với các tài khoản người dung trong hệ thống của một nhân viên nghỉ việc?=>A

Câu hỏi 12

Chưa trả lời

Đạt điểm 1,00

Đặt cờ

Theo bạn giải pháp nào cần được áp dụng với các tài khoản người dùng trong hệ thống của một nhân viên nghỉ việc?

- a. Vô hiệu hóa các tài khoản của nhân viên đó và giữ lại các dữ liệu được lưu trữ trong một thời gian yep
- b. Vô hiệu hóa các tài khoản của nhân viên đó và xóa ngay lập tức các dữ liệu được lưu trữ
- c. Duy trì các tài khoản người dùng và giữ lại các dữ liệu được lưu trữ trong một thời gian
- d. Không sử dụng các lựa chọn nào ở đây

Điều nào sau đây không đúng khi nói về lỗ hổng 0-day? =>C

Câu hỏi 13

Chưa trả lời

Đạt điểm 1,00

Đặt cờ

Điều nào sau đây không đúng khi nói về lỗ hổng 0-day?

- a. Là lỗ hổng nhà sản xuất chưa kịp vá
- b. Là lỗ hổng hacker chưa công bố rộng rãi
- c. Là lỗ hổng phá hoại hệ thống trong vòng một ngày yep
- d. Là lỗ hổng nguy hiểm khi tấn công vào hệ thống chưa có giải pháp bảo vệ

Điều nào sau đâu mô tả đúng nhất cơ chế kiểm soát truy cập cho phép chủ sở hữu dữ liệu tạo và quản lý kiểm soát truy cập? =>DACS

Câu hỏi 14

Chưa trả lời

Đạt điểm 1,00

Đặt cờ

Điều nào sau đây mô tả đúng nhất cơ chế kiểm soát truy cập cho phép chủ sở hữu dữ liệu tạo và quản lý kiểm soát truy cập?

- a. RBACs (Role Based Access Control)
- b. DACs (Discretionary Access Control) yep
- c. Rule Based Access Control
- d. LBACs (List Based Access Control)
- e. MACs (Mandatory Access Control)

Mục tiêu chính của an toàn thông tin là đảm bảo các tính chất theo mô hình C-I-A là? =>A,C,D

Câu hỏi 15

Chưa trả lời

Đạt điểm 1,00

Đặt cờ

Mục tiêu chính của an toàn thông tin là đảm bảo các tính chất theo mô hình C-I-A là?

- a. Tính bí mật yep
- b. Tính dễ mở rộng
- c. Tính toàn vẹn yep
- d. Tính sẵn sàng yep
- e. Tính chống chối bỏ
- f. Tính xác thực

Đâu là mục tiêu chủ yếu của kiểu tấn công Social Engineering?=>D

Câu hỏi 16
Chưa trả lời
Đạt điểm 1,00
Đặt cờ

Đâu là mục tiêu chủ yếu của kiểu tấn công Social Engineering?

- a. Email
- b. Peer to Peer Network
- c. Local Area Network
- d. Con người here

Trong tổ chức bộ nhớ của chương trình C, phần Data-Segment lưu các thông tin gì của chương trình? =>B

Câu hỏi 17
Chưa trả lời
Đạt điểm 1,00
Đặt cờ

Trong tổ chức bộ nhớ của chương trình C, phần Data-Segment lưu các thông tin gì của chương trình?

- a. Lưu mã nguồn thực thi
- b. Lưu các biến static/global đã được khởi tạo trong chương trình yep
- c. Lưu các đối số của một hàm
- d. Lưu các biến cục bộ trong chương trình
- e. Lưu các biến static/global chưa được khởi tạo trong chương trình

Clear my choice

Rủi ro chính từ việc sử dụng phần mềm lỗi thời (outdated software) là gì?=>D

Câu hỏi 18
Chưa trả lời
Đạt điểm 1,00
Đặt cờ

Rủi ro chính từ việc sử dụng phần mềm lỗi thời (outdated software) là gì?

- a. Có thể dễ dàng xâm nhập hơn phần mềm mới hơn
- b. Nó có thể không có tất cả các tính năng bạn cần
- c. Nó có thể không có các tính năng bảo mật hiện đại nhất
- d. Nó có thể không còn được hỗ trợ bởi các nhà cung cấp yep

Clear my choice

Điều nào sau đây là rủi ro tiềm ẩn khi chương trình chạy ở chế độ đặc quyền? =>A

Câu hỏi 19
Chưa trả lời
Đạt điểm 1,00
Đặt cờ

Điều nào sau đây là rủi ro tiềm ẩn khi chương trình chạy ở chế độ đặc quyền?

- a. Nó có thể cho phép mã độc được chèn vào yep
- b. Nó có thể phục vụ cho việc tạo ra các đoạn mã phức tạp không cần thiết
- c. Nó có thể không thực hiện việc phân chia xử lý các tác vụ
- d. Nó có thể tạo ra việc loại bỏ các ứng dụng không cần thiết

Đảm bảo dữ liệu không bị sửa đổi trong quá trình lưu trữ hay trong quá trình truyền qua mạng bởi những người dùng không hợp pháp gọi là? =>C

Câu hỏi 20

Chưa trả lời

Đạt điểm 1,00

Đặt cờ

Đảm bảo dữ liệu không bị sửa đổi trong quá trình lưu trữ hay trong quá trình truyền qua mạng bởi những người dùng không hợp pháp gọi là?

- a. Availability
- b. Nonrepudiation
- c. Integrity yep
- d. Confidentiality

Bạn là người tư vấn giải pháp an toàn thông tin, một khách hàng của bạn quan tâm đến việc chống lại giả mạo và nhiễm đọc ARP trong mạng của họ. Giải pháp nào dưới đây KHÔNG áp dụng cho mục đích này?

D

Tại sao các nhà phát triển phầm mềm đính kèm theo các giá trị băm bằng hàm MD5 của các gói cập nhật cho phần mềm cùng với các gói đó để các khách hàng của họ có thể download từ Internet?

(Khách hàng có thể xác thực tính toàn vẹn của gói cập nhật cho phần mềm sau khi download về)

Một kiểu tấn công DoS sử dụng cơ chế bắt tay ba bước (three-way handshake) của TCP là? (SYN Flood)

Câu hỏi 3

Câu trả lời đã được lưu

Đạt điểm 1,00

Xóa cờ

Một kiểu tấn công DoS sử dụng cơ chế bắt tay ba bước (three-way handshake) của TCP là?

- a. SQL Injection
- b. SYN Flood here
- c. Ping of Death
- d. Brute force
- e. Buffer Overflow

Clear my choice

Công cụ nào dưới đây có thể dùng để xác định các kết nối mạng đang có trên máy tính? (Netstat)

Câu hỏi 4

Câu trả lời đã được lưu

Đạt điểm 1,00

Đặt cờ

Công cụ nào dưới đây có thể dùng để xác định các kết nối mạng đang có trên máy tính?

- a. Netstat yup
- b. Tracert
- c. Ipconfig
- d. Ping

Clear my choice

Một quản trị mạng mới thay thế hub bằng switch. Khi sử dụng phần mềm Sniffer bắt các gói tin trên mạng, người quản trị thấy được dữ liệu trao đổi giữa máy tính của anh ta và máy chủ, nhưng không thấy được các trao đổi giữa những máy khác nhau trong mạng với máy chủ. Coi như switch hoạt động tốt, điều gì đó đã tạo ra hiện tượng trên. (a)

Câu hỏi 5

Chưa trả lời

Đạt điểm 1,00

Xóa cờ

Một quản trị mạng mới thay thế hub bằng switch. Khi sử dụng phần mềm Sniffer bắt các gói tin trên mạng, người quản trị thấy được dữ liệu trao đổi giữa máy tính của anh ta và máy chủ, nhưng không thấy được các trao đổi giữa những máy khác trong mạng với máy chủ. Coi như switch hoạt động tốt, điều gì đó đã tạo ra hiện tượng trên?

- a. Trừ thông tin broadcast và unknown unicast, switch không gửi thông tin ra tất cả các cổng
- b. Switch được cấu hình VLAN
- c. Phần mềm Sniffer cấu hình sai
- d. Phần mềm Sniffer không bắt được thông tin qua cổng Ethernet

Clear my choice

Khái niệm bảo mật nào khuyến khích quản trị viên cài đặt tường lửa, chương trình quét phần mềm đọc hại (malware scanner) và IDS trên các host? (Endpoint security)

Câu hỏi 6
Chưa trả lời
Đạt điểm 1,00
Đặt cờ

Khái niệm bảo mật nào khuyến khích quản trị viên cài đặt tường lửa, chương trình quét phần mềm độc hại (malware scanner) và IDS trên các host?

- a. Endpoint security
- b. RADIUS
- c. VLAN
- d. Network access control (NAC)
- e. SAFE

Email Server nên được đặt ở vùng mạng nào? **(d. DMZ)**

Câu hỏi 7
Câu trả lời đã được lưu
Đạt điểm 1,00
Đặt cờ

Email Server nên được đặt ở vùng mạng nào?

- a. INSIDE
- b. DZM
- c. OUTSIDE
- d. DMZ

Clear my choice

Máy chủ web của một công ty được cấu hình những dịch vụ sau: HTTP, SSI, FTP, SMTP. Máy chủ này được đặt trong vùng DMZ. Đâu là những cổng cần phải mở trên tường lửa để cho phép các máy trạm có thể sử dụng dịch vụ trên máy này? (80, 20, 21, 25, 443)

Câu hỏi 8
Câu trả lời đã được lưu
Đạt điểm 1,00
Xóa cờ

Máy chủ web của một công ty được cấu hình những dịch vụ sau: HTTP, SSI, FTP, SMTP. Máy chủ này được đặt trong vùng DMZ. Đâu là những cổng cần phải mở trên tường lửa để cho phép các máy trạm có thể sử dụng dịch vụ trên máy này?

- a. 119, 23, 21, 80, 23
- b. 80, 20, 21, 25, 443
- c. 434, 21, 80, 25, 20
- d. 110, 443, 21, 59, 25

Clear my choice

Loại malware nào sau đây có thể ẩn các tiến trình và các tập tin trên hệ thống? **(Rookit)**

Câu hỏi 9
Chưa trả lời
Đạt điểm 1,00
Đặt cờ

Loại malware nào sau đây có thể ẩn các tiến trình và các tập tin trên hệ thống?

- a. Rootkit
- b. Trojan
- c. Adware
- d. Worm

Kiểu tấn công nào sau đây không phải kiểu tấn công từ chối dịch vụ? a. MITM

Câu hỏi 10
Chưa trả lời
Đạt điểm 1,00
Đặt cờ

Kiểu tấn công nào sau đây không phải kiểu tấn công từ chối dịch vụ?

- a. Main-In-The-Middle (MITM)
- b. Teardrop
- c. Ping of Death
- d. Sử dụng Botnet
- e. ICMP Flood

Clear my choice

Muốn thay thế telnet với một giao thức an toàn hơn để quản lý các thiệt bị mạng, ta cần sử dụng giao thức nào sau đây? **(SSH)**

Câu hỏi 11
Chưa trả lời
Đạt điểm 1,00
Đặt cờ

Muốn thay thế telnet với một giao thức an toàn hơn để quản lý các thiết bị mạng, ta cần sử dụng giao thức nào sau đây?

- a. HTTP
- b. SFTP
- c. SNMP
- d. SMTP
- e. SSH

Clear my choice

Phát biểu nào sau đây không đúng về vùng DMZ? **(c)**

Câu hỏi 12
Chưa trả lời
Đạt điểm 1,00
Đặt cờ

Phát biểu nào sau đây không đúng về vùng DMZ?

- a. Là nơi đặt các public server
- b. Thường chứa email server hoặc web server
- c. Chứa các server chỉ phục vụ cho người dùng bên trong
- d. Để nâng cao sự bảo mật cho hệ thống

Thuật toán nào dưới đây không phải là một thuật toán mã hoá khối? **(RC4)**

Câu hỏi 13
Chưa trả lời
Đạt điểm 1,00
Đặt cờ

Thuật toán nào dưới đây không phải là thuật toán mã hóa khối?

- a. 3DES
- b. AES
- c. RC4
- d. DES

Mã hóa khối: AES, DES, 3DES

Mã hóa dòng: RC4

Trong mật mã khoá công khai (PKI), để xác nhận mình là người gửi thông tin, người gửi sẽ sử dụng khoá nào? **(Public key)**

Câu hỏi
14
Chưa trả lời
Đạt điểm 1,00
Đặt cờ

Trong mật mã khóa công khai (PKI), để xác nhận mình là người gửi thông tin, người gửi sẽ sử dụng khóa nào?

- a. Secret key
- b. Session key
- c. Public key
- d. Private key

Clear my choice

Mặc dù báo cáo quét lỗ hổng cho thấy không có lỗ hổng nào được phát hiện, nhưng một cuộc kiểm tra thâm nhập tiếp theo cho thấy có các lỗ hổng trên mạng. Thuật ngữ nào sau đây mô tả cho trường hợp này? **(c. False negative)**

Câu hỏi
15
Chưa trả lời
Đạt điểm 1,00
Đặt cờ

Mặc dù báo cáo quét lỗ hổng cho thấy không có lỗ hổng nào được phát hiện, nhưng một cuộc kiểm tra thâm nhập tiếp theo cho thấy có các lỗ hổng trên mạng. Thuật ngữ nào sau đây mô tả cho trường hợp này?

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

Giao thức nào sau đây thuộc mã khoá công khai? **(RSA)**

Câu hỏi 16
Chưa trả lời
Đạt điểm 1,00
Đặt cờ

Giao thức nào sau đây thuộc mã khóa công khai ?

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

Kiểu tấn công nào sau đây không phải khai thác các lỗ hổng của ứng dụng Web? **(Social Engineering)**

Câu hỏi 17
Chưa trả lời
Đạt điểm 1,00
Đặt cờ

Kiểu tấn công nào sau đây không phải khai thác các lỗ hổng của ứng dụng Web ?

- a. Cross Site Request Forgery
- b. Cross-site scripting
- c. Social Engineering yes
- d. SQL Injection

Clear my choice

Quản trị viên bảo mật thiết lập một AP mới nhưng nhận ra quá nhiều người bên ngoài có thể kết nối AP đó và truy cập trái phép. Các cách nào sau đây sẽ là cách TỐT NHẤT để giảm thiểu vấn đề này?

(Disable SSID broadcast + MAC filtering)

Câu hỏi 18
Chưa trả lời
Đạt điểm 1,00
Đặt cờ

Quản trị viên bảo mật thiết lập một AP mới nhưng nhận ra quá nhiều người bên ngoài có thể kết nối với AP đó và truy cập trái phép. Các cách nào sau đây sẽ là cách TỐT NHẤT để giảm thiểu vấn đề này?

- a. Tắt cổng kết nối có dây
- b. Disable SSID broadcast
- c. Sử dụng kênh 1, 4, 7 trong cấu hình AP
- d. Sử dụng 802.11ax
- e. MAC filtering

Việc tắt các port không sử dụng trên switch hay gỡ bỏ các dịch vụ, giao thức, phần mềm không cần thiết gọi là gì? (Hardening)

Câu hỏi 19
Chưa trả lời
Đạt điểm 1,00
Đặt cờ

Việc tắt các port không sử dụng trên switch hay gỡ bỏ các dịch vụ, giao thức, phần mềm không cần thiết gọi là gì?

- a. Hashing
- b. Non-repudiation
- c. Unused-removing
- d. Auditing
- e. Hardening

Clear my choice

Việc tắt các port không sử dụng trên switch hay gỡ bỏ các dịch vụ, giao thức, phần mềm không cần thiết gọi là gì?
a. Hardening
b. Unused-removing
c. Non-repudiation

a. Hardening

Hardening là một quy trình bảo mật mà người quản trị mạng có thể thực hiện để làm cho hệ thống hoặc thiết bị mạng của họ được bảo vệ tốt hơn và khó riêng lẻ tấn công mục tiêu độc gián tuyến. Hardening có thể bao gồm việc tắt các port không sử dụng trên switch hoặc gỡ bỏ các dịch vụ, giao thức, phần mềm không cần thiết, cũng như các hoạt động bảo mật khác như cấu hình tường lửa, cài đặt các bản cập nhật bảo mật, và sử dụng các tiêu chuẩn bảo mật để đảm bảo rằng hệ thống hoặc thiết bị mạng được bảo vệ tốt nhất có thể.

Hệ thống IDS/IPS phát hiện xâm nhập dựa vào các kỹ thuật nào sau đây? **(A, B)**

Câu hỏi
20

Chưa trả lời

Đạt điểm 1,00

Đặt cờ

Hệ thống IDS/IPS phát hiện xâm nhập dựa vào các kỹ thuật nào sau đây?

- [x] a. Anomaly-based detection
- [x] b. Signature-based detection
- [ ] c. Attribute-based detection
- [ ] d. Classify-based detection
- [x] e. Role-based detection

CÔ VÂN

An toan thong tin_ Nhom 10

Câu hỏi 1

Câu trả lời đã được lưu

Đạt điểm 1,00

Attackers exploit buffer overflows to...

- a. insert code that allows them access to the system
- b. copy data into the system
- c. get data from the system
- d. modify data in the system

Clear my choice

Câu hỏi 2

Câu trả lời đã được lưu

Đạt điểm 1,00

Thời gian còn lại 0:05:02

A canary value is used in computer security to detect and prevent buffer overflow attacks. It is placed on the stack just before the return address to act as a guard. If a buffer overflow occurs and attempts to overwrite the return address, the canary value will be altered. By checking the canary value before returning from the function, the system can detect that a buffer overflow has occurred and take appropriate action, such as terminating the program to prevent exploitation

A random canary value is .....

- a. written just before a return address is stored in a stack frame

kết hợp với stack shielf để lưu return address so sánh

- b. written just after a return address is stored in a stack frame
- c. written just after a register address is stored in a stack frame
- d. written just before a register address is stored in a stack frame

Clear my choice

Câu hỏi 3

Câu trả lời đã được lưu

Đạt điểm 1,00

Encryption using private key to ensure:

Select one:

- a. Authentication and Non-repudiation
- b. Availability
- c. Confidentiality and Integrity
- d. Confidentiality and authentication

Clear my choice

Hash of the message to be encrypted using sender's private key (to ensure authentication/nonrepudiation)
-Message to be encrypted using receiver's public key (to ensure confidentiality)

Câu hỏi 4

Câu trả lời đã được lưu

Đạt điểm 1,00

Which types of Stack overflow that overwrite the saved frame pointer?

- a. stack canary
- b. stack buffer
- c. stack smash
- d. stack off-by-one

Clear my choice

kiểu tấn công bảo mật mà trong đó kẻ tấn công lợi dụng lỗ hổng trong việc quản lý bộ nhớ ngăn xếp (stack) để ghi đè dữ liệu trên ngăn xếp

Câu hỏi 5

Câu trả lời đã được lưu

Đạt điểm 1,00

Which one is not overwritten when buffer overflow ?

- a. other program's variables or parameters
- b. return addresses
- c. pointers to previous stack frames
- d. program's data

Clear my choice

không liên quan đến vùng nhớ của chương trình

Câu hỏi 6

Câu trả lời đã được lưu

Đạt điểm 1,00

Which one is used to store the memory address to which the frame pointer is pointing to?

- a. Register esp
- b. Register ebp
- c. Return address
- d. Register eip

Clear my choice

esp: stack pointer
ebp: frame pointer
eip: next instrusion pointer (câu lnh tip theo thc hin)

Câu hỏi 7

Câu trả lời đã được lưu

Đạt điểm 1,00

false negative: phát hiện là đúng nhưng thực tế sai (phần mềm virus không phá hiện virus)
false positive: phát hiện là sai nhưng thực tế đúng (phần mềm virus phát hiện virus nhưng khong có virus)

Which of the following is an example of a false positive?

- a. The IDS does not identify a buffer overflow
- b. Anti-virus identifies a benign application as malware.
- c. A user account is locked out after the user mistypes the password too many times.
- d. A biometric iris scanner rejects an authorized user wearing a new contact lens.

Clear my choice

Câu hỏi 8

Câu trả lời đã được lưu

Đạt điểm 1,00

Encryption using public key to ensure:

Select one:

- a. Non-repudiation
- b. Confidentiality
- c. Integrity
- d. Availability

Clear my choice

Encryption using a public key can be used to ensure confidentiality.

Confidentiality refers to the protection of data from unauthorized disclosure. When data is encrypted using a public key, it can only be decrypted by someone who has the corresponding private key. This ensures that the data is only accessible to those who are authorized to view it, providing confidentiality.

Non-repudiation refers to the inability of a sender to deny having sent a message. It can be achieved through the use of digital signatures, which use a private key to create a unique signature that can be verified using the corresponding public key.

Integrity refers to the protection of data from unauthorized modification. It can be ensured through the use of cryptographic hash functions, which create a unique signature for a piece of data that can be used to detect any changes to the data.

Availability refers to the ability of authorized users to access data when needed. It can be ensured through the use of measures such as redundant servers and backup systems to ensure that data is always accessible.

Câu hỏi 9

Câu trả lời đã được lưu

Đạt điểm 1,00

Given the security levels TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories A, B, and C, specify what type of access (read, write, or both) is allowed in situation: "John, cleared for (SECRET, {C}). John want to access to a document classified (TOP SECRET, {A, B})". Which true statement?

Select one:

- a. John cannot read and can write
- b. John cannot write and cannot read
- c. John can read and cannot write
- d. John can read and can write

Clear my choice

The subject can communicate to the object if indeed the subject compartment dominates the object compartment, per a basic security property. The *-property states that the topic can write to an object if the item compartment dominates the subject sector. Let (L, C) and (L', C') be lockers for separate things.

subject sector. Let **(L, C)** and **(L', C')** be lockers for separate things. $((\mathbf{L}, \mathbf{C})\ \mathbf{dominates}\ (\mathbf{L}', \mathbf{C}') \Leftrightarrow \mathbf{L}' \leq \mathbf{L}\ \mathbf{and}\ \mathbf{C}' \subseteq \mathbf{C})$ is the concept we will use to characterize a **sort of access** that the following statements possess.

A can read document if A's clearance level dominates document 's classification level
A can write if document's classification level dominate A's clearance level.

Câu hỏi 10

Câu trả lời đã được lưu

Đạt điểm 1,00

John has write permission on bt1 file, read and execute permission on bt2 file, no permissions on bt3 file. Define Capability List (CList)?

- a. CList(John) = bt1: {write}, bt2: {read}, bt3: {}
- b. CList(John) = bt1: {read}, bt2: {execute}, bt3: {}
- c. CList(John) = bt1: {read, write}, bt2: {execute}, bt3: {}
- d. CList(John) = bt1: {write}, bt2: {read, execute}, bt3: {}

Clear my choice

◄ Access Control - Reference

Chuyển tới...

Survey midterm ►

dsds

An toan thong tin_ Nhom 10

Câu hỏi 11

Câu trả lời đã được lưu

Đạt điểm 1,00

Given the security levels TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories A, B, and C, specify what type of access (read, write, or both) is allowed in situation: "John, cleared for (SECRET, {A, C}), wants to access a document classified (SECRET, {B})". Which true statement?

Select one:

- a. John cannot write and cannot read
- b. John cannot read and can write
- c. John can read and cannot write
- d. John can read and can write

B not in {A,C}
=> two not same type

Clear my choice

Câu hỏi 12

Câu trả lời đã được lưu

Đạt điểm 1,00

Which one dynamically moves as contents are pushed and popped out of the stack frame?

- a. Register esp
- b. Register ebp
- c. esp
- d. ebp

Clear my choice

Câu hỏi 13

Câu trả lời đã được lưu

Đạt điểm 1,00

Rhonda registers the domain name "AddisonWesley.com" and refuses to let the publishing house buy or use that domain name

Select one:

- a. Integrity and confidentiality
- b. Integrity
- c. Confidentiality
- d. Availability

Clear my choice

https://quizlet.com/677143568/info-security-midterm-1-flash-cards/
Câu 7

Câu hỏi 14

Câu trả lời đã được lưu

Đạt điểm 1,00

Which of the following is not a valid means to improve the security offered by password authentication?

Thời gian còn lại 0:04:48

- a. Using password verification tools and password-cracking tools against your password database file
- b. Allowing users to reuse the same password
- c. Enabling account lockout controls
- d. Enforcing a reasonable password policy

Clear my choice

Of the options listed, retina scan is the least accepted form of biometric device because it requires touching a shared eye cup and can reveal personal health issues.

Câu hỏi 15

Câu trả lời đã được lưu

Đạt điểm 1,00

What policy they might be enforcing in this situation: "The login program will disallow logins of any students who enter their passwords incorrectly 3 times"

Select one:

- a. Authentication
- b. Confidentiality
- c. Integrity
- d. Access control

Clear my choice

ôn thêm:
https://quizlet.com/182809961/ch1security-flash-cards/

Câu hỏi 16

Câu trả lời đã được lưu

Đạt điểm 1,00

The subject is always the entity that receives information about or data from the object. The subject is also the entity that alters information about or data stored within the object. The object is always the entity that provides or hosts the information or data. A subject can be a user, a program, a process, a file, a computer, a database, and so on. The roles of subject and object can switch as two entities, such as a program and a database or a process and a file, communicate to accomplish a task.

Which of the following is true?

- a. A single entity can never change roles between subject and object.
- b. A subject is always a user account.
- c. The subject is always the entity that receives information about or data from the object.
- d. The subject is always the entity that provides or hosts the information or data.

Clear my choice

Câu hỏi 17

Câu trả lời đã được lưu

Đạt điểm 1,00

What does hashing preserve in relation to data

Select one:

- A. Repudiation
- B. Availability
- C. Confidentiality
- D. Integrity

https://quizlet.com/196871677/hod401-chapter-3-flash-cards/
câu 9

Clear my choice

Câu hỏi 18

Câu trả lời đã được lưu

Đạt điểm 1,00

Which of the following is the least acceptable form of biometric device?

- a. Retina scan
- b. Fingerprint
- c. Facial geometry
- d. Iris scan

Clear my choice

Câu hỏi 19

Câu trả lời đã được lưu

Đạt điểm 1,00

..... is the process of verifying or testing the validity of a claimed identity.

- a. Identification
- b. Accountability
- c. Authorization
- d. Authentication

Clear my choice

Câu hỏi 20

Câu trả lời đã được lưu

Đạt điểm 1,00

An implemented security controls, a user can only access a server with FTP. Which AAA component accomplishes this?

- a. Authorization
- b. Accounting
- c. Authentication
- d. Access Control

Clear my choice

◄ **Access Control - Reference**

Chuyển tới...

Survey midterm ►

An toan thong tin_ Nhom 10

Câu hỏi 21

Câu trả lời đã được lưu

Đạt điểm 1,00

No read up, no write down

Given the security levels TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories A, B, and C, specify what type of access (read, write, or both) is allowed in situation: "John, cleared for (TOP SECRET, {A, B}). John wants to access to a document classified (CONFIDENTIAL, {A})". Which true statement?

Select one:

- a. John can read and can write
- b. John cannot read and can write
- c. John can read and cannot write
- d. John cannot write and cannot read

Top Secret > Secret && {A} in {A,B}
=> John có have more permission than document
=> John has read permission (no read up, no write down)
http://cse.hcmut.edu.vn/~thanhtung/downloads/iss/lecture5.pdf

Thời gian còn lại 0:04:38

Clear my choice

Câu hỏi 22

Câu trả lời đã được lưu

Đạt điểm 1,00

What is the most important aspect of a biometric device?

Select one:

- a. Accuracy
- b. Enrollment time
- c. Acceptability
- d. Invasiveness

Clear my choice

Câu hỏi 23

Câu trả lời đã được lưu

Đạt điểm 1,00

Which true command to disable the security mechanism to prevent buffer overflows when compiling example.c?

- a. $ gcc -fno-execution-protector example.c
- b. $ gcc -fno-stack-execution example.c
- c. $ gcc -fno-disable-protector example.c
- d. $ gcc -fno-stack-protector example.c

Clear my choice

Câu hỏi 24

Câu trả lời đã được lưu

Đạt điểm 1,00

Given the security levels TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories A, B, and C, specify what type of access (read, write, or both) is allowed in situation: "John, cleared for (SECRET, {A, B}). John want to access to a document classified (TOP SECRET, {A, B, C})". Which true statement?

Select one:

- a. John can read and can write
- b. John can read and cannot write
- c. John cannot read and can write
- d. John cannot write and cannot read

Clear my choice

Câu hỏi 25

Câu trả lời đã được lưu

Đạt điểm 1,00

Carol changes the amount of Angelo's check from $100 to $1,000. Which violation occur?

Select one:

- a. Availability
- b. Integrity and confidentiality
- c. Integrity
- d. Confidentiality

Clear my choice

Câu hỏi 26

Câu trả lời đã được lưu

Đạt điểm 1,00

Results of buffer overflow **not** include...

- a. corruption of program data
- b. decrypt data in the system
- c. memory access violations
- d. unexpected transfer of control

Clear my choice

Câu hỏi 27

Câu trả lời đã được lưu

Đạt điểm 1,00

Given the security levels TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories A, B, and C, specify what type of access (read, write, or both) is allowed in situation: "John, cleared for (SECRET, {A, B}). John wants to access to a document classified (SECRET, {B, C})". Which true statement?

Select one:

- a. John cannot write and cannot read
- b. John can read and can write
- c. John cannot read and can write
- d. John can read and cannot write

{A,B} not in {B,C}

Clear my choice

Câu hỏi 28

Câu trả lời đã được lưu

Đạt điểm 1,00

Which one is used to store the memory address to which the stack pointer is pointing to?

- a. Register eip
- b. Register ebp
- c. Return address
- d. Register esp

Clear my choice

Câu hỏi 29

Câu trả lời đã được lưu

Đạt điểm 1,00

Which of the following best describes hashing

Select one:

- A. A cipher
- B. Nonreversible
- C. A cryptosystem
- D. An algorithm

Clear my choice

Câu hỏi 30

Câu trả lời đã được lưu

Đạt điểm 1,00

There are several security mechanisms to make the buffer-overflow attack difficult, which one of them?

- a. Address Space Protection
- b. Use an executable stack
- c. The StackGuard Protection
- d. Layout Randomization

Clear my choice

◄ Access Control - Reference

Chuyển tới...

Survey midterm ►

An toan thong tin_ Nhom 10

Câu hỏi 31

Câu trả lời đã được lưu

Đạt điểm 1,00

Given the security levels TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories A, B, and C, specify what type of access (read, write, or both) is allowed in situation: "John, cleared for (UNCLASSIFIED, {A, B}). John wants to access to a document classified (TOP SECRET, {A, B, C})". Which true statement?

Select one:

- a. John cannot write and cannot read
- b. John can read and can write
- c. John can read and cannot write
- d. John cannot read and can write

Clear my choice

Câu hỏi 32

Câu trả lời đã được lưu

Đạt điểm 1,00

Given the security levels TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories A, B, and C, specify what type of access (read, write, or both) is allowed in situation: " John, cleared for (CONFIDENTIAL, {}). John wants to access to a document classified (SECRET, {A, B, C})". Which true statement?

Select one:

- a. John can read and cannot write
- b. John can write and cannot read
- c. John can read and can write
- d. John cannot read and cannot write

Clear my choice

Câu hỏi 33

Câu trả lời đã được lưu

Đạt điểm 1,00

What is the first step of access control?

- a. ACL verification
- b. Subject identification
- c. Accountability logging
- d. Subject authorization

The first step of access control is subject identification. This involves identifying the entity (also known as the "subject") that is attempting to access a resource or perform an action. The subject can be a person, a computer program, or another system.

Clear my choice

Câu hỏi 34

Câu trả lời đã được lưu

Đạt điểm 1,00

In Linux OS, to **disable** uses address space randomization to randomize the starting address of heap and stack, use which of the following commands?

Thời gian còn lại 0:04:29

- a. $sudo sysctl –w kernel.randomize_store_space=0
- b. $sudo sysctl –w kernel.randomize_sa_space=0
- c. $sudo sysctl –w kernel.randomize_va_space=0
- d. $sudo sysctl –w kernel.randomize_ram_space=0

Clear my choice

Câu hỏi 35

Câu trả lời đã được lưu

Đạt điểm 1,00

Which of the following types of access control uses fences, security policies, security awareness training, and antivirus software to stop an unwanted or unauthorized activity from occurring?

- a. Authoritative
- b. Detective
- c. Corrective
- d. Preventive

Clear my choice

Câu hỏi 36

Câu trả lời đã được lưu

Đạt điểm 1,00

What can be used as an authentication factor that is a behavioral or physiological characteristic unique to a subject?

- a. ID
- b. Biometric factor
- c. Token
- d. Account ID

Clear my choice

Câu hỏi 37

Câu trả lời đã được lưu

Đạt điểm 1,00

Which of the following is true about subject in access control?

- a. always a user account
- b. always the entity that provides or hosts the information or data
- c. A single entity can never change roles between subject and object
- d. always the entity that receives information about or data from the object.

Clear my choice

Câu hỏi 38

Câu trả lời đã được lưu

Đạt điểm 1,00

Using Private key to

Select one:

- a. Verify signature and encrypt the message
- b. Create signature and decrypt the message
- c. Create signature and encrypt the message
- d. Verify signature and decrypt the message

Clear my choice

Câu hỏi 39

Câu trả lời đã được lưu

Đạt điểm 1,00

What is the primary function of the AAA authorization command?

- a. permit AAA server access to AAA client services
- b. limit authenticated user access to AAA client services
- c. limit AAA server access to AAA client services
- d. permit authenticated user access to AAA client services

ChatGPT

Clear my choice

Câu hỏi 40

Câu trả lời đã được lưu

Đạt điểm 1,00

.....access controls rely upon the use of labels.

Select one:

- a. Discretionary
- b. Nondiscretionary
- c. Mandatory
- d. Role-based

Mandatory access controls rely upon the use of labels. A system that employs discretionary access controls allows the owner or creator of an object to control and define subject access to that object. Nondiscretionary access controls are also called role-based access controls. Systems that employ nondiscretionary access controls define a subject's ability to access an object through the use of subject roles or tasks.

Clear my choice

◄ Access Control - Reference

Chuyển tới...

Survey midterm ►

An toan thong tin_ Nhom 10

Câu hỏi 41

Câu trả lời đã được lưu

Đạt điểm 1,00

Which types of Stack overflow that overwrite the saved instruction pointer

- a. stack buffer
- b. stack canary
- c. stack off-by-one
- d. stack smash

Clear my choice

A stack smash is a type of stack buffer overflow that occurs when an attacker is able to overwrite the saved instruction pointer and execute arbitrary code by overflowing a buffer on the stack.

A stack off-by-one is a type of stack overflow that occurs when a program writes one byte of data past the end of a buffer on the stack. This can cause the data to overwrite the saved instruction pointer and allow an attacker to execute arbitrary code.

A stack canary is a security mechanism that is used to detect stack buffer overflows and prevent them from being exploited. It involves placing a unique value, known as a "canary," on the stack before the saved instruction pointer. If an attacker attempts to overflow the buffer and overwrite the saved instruction pointer, they will also overwrite the canary. This can be detected and used to prevent the attack from succeeding.

Câu hỏi 42

Câu trả lời đã được lưu

Đạt điểm 1,00

Which of the following forms of authentication provides the strongest security?

- a. Passphrase and a smart card
- b. Fingerprint
- c. Password and a PIN
- d. One-time password

Clear my choice

Câu hỏi 43

Câu trả lời đã được lưu

Đạt điểm 1,00

What policies they might be enforcing in this situation: "The permissions of the file containing Carol's homework will p cheating and copying it"

Thời gian còn lại 0:04:19

Select one:

- a. Confidentiality and access control
- b. Access control and integrity
- c. Authentication and confidentiality
- d. Confidentiality and authentication

Clear my choice

Câu hỏi 44

Câu trả lời đã được lưu

Đạt điểm 1,00

What is Stack Canaries?

- a. Stack Control
- b. Stack Overflow
- c. Stack Protection
- d. Stack Prevention

Clear my choice

Câu hỏi 45

Câu trả lời đã được lưu

Đạt điểm 1,00

Jonah obtains Peter's credit card number and has the credit card company cancel the card and replace it with another card bearing a different account number

Select one:

- a. Integrity and confidentiality
- b. Availability and integrity
- c. Integrity, confidentiality and authentication
- d. Confidentiality, integrity and availability

Clear my choice

https://quizlet.com/7124785/computer-security-exam-1-flash-cards/
Câu 6

Câu hỏi 46

Câu trả lời đã được lưu

Đạt điểm 1,00

..... access controls are the hardware or software mechanisms used to manage access to resources and systems and to provide protection for those resources and systems.

Select one:

- a. Logical/technical
- b. Administrative
- c. Preventive
- d. Physical

Clear my choice

Câu hỏi 47

Câu trả lời đã được lưu

Đạt điểm 1,00

What requirements **not** must meet in a trusted computing base ?

- a. Verifiable
- b. Tamperproof
- c. Complete mediation
- d. Available

Clear my choice

Câu hỏi 48

Câu trả lời đã được lưu

Đạt điểm 1,00

When exploiting a buffer overflow the attacker needs...

- a. To understand how that buffer will be stored in the processes memory
- b. To understand how that buffer overflow
- c. to know the key to decrypt code
- d. To understand how that buffer will be encrypted in the processes memory

Clear my choice

Câu hỏi 49

Câu trả lời đã được lưu

Đạt điểm 1,00

Paul crashes Linda's system. Which violation occur?

Select one:

- a. Availability
- b. Confidentiality
- c. Integrity and confidentiality
- d. Integrity

Clear my choice

Câu hỏi 50

Câu trả lời đã được lưu

Đạt điểm 1,00

Which one typically points to a fixed address where the old frame pointer is stored?

- a. Register ebp
- b. esp
- c. Register esp
- d. ebp

Clear my choice

◄ Access Control - Reference

Chuyển tới...

Survey midterm ►

An toan thong tin_ Nhom 10

Thời gian còn lại 0:39:05

Câu hỏi 1

Câu trả lời đã được lưu

Đạt điểm 1,00

Chuẩn nào sau đây liên quan đến an toàn thông tin?

- a. ISO 2600
- b. ISO 27001
- c. ISO 9001
- d. ISO 2015

Clear my choice

Câu hỏi 2

Câu trả lời đã được lưu

Đạt điểm 1,00

Tấn công nào sau đây là tấn công chủ động (active)

- a. Scan port
- b. ping
- c. Sniffing
- d. DoS

Clear my choice

Câu hỏi 3

Câu trả lời đã được lưu

Đạt điểm 1,00

Chế độ hoạt động nào sau đây mã hóa các khối một cách riêng biệt?

- a. Cipher feedback mode - CFB
- b. Cipher block chaining mode - CBC
- c. Output feedback mode – OFB
- d. Electronic codebook mode - ECB

Clear my choice

Câu hỏi 4

Câu trả lời đã được lưu

Đạt điểm 1,00

Câu nào sau đây KHÔNG phải là một cơ chế điều khiển truy cập?

- a. Attribute Based Access Control (ABAC)
- b. Subjective Access Control (SAC)
- c. Discretionary Access Control (DAC)
- d. Mandatory Access Control (MAC)
- e. Role Based Access Control (RBAC)

Clear my choice

Câu hỏi 5

Câu trả lời đã được lưu

Đạt điểm 1,00

Điều nào sau đây xảy ra khi một chuỗi dữ liệu được gửi đến bộ đệm lớn hơn bộ đệm được thiết kế để xử lý?

- a. Buffer overflow
- b. SYN flood
- c. Spoofing attack
- d. Brute Force attack
- e. Blue Screen of Death
- f. Man in the middle attack

Clear my choice

Câu hỏi 6

Câu trả lời đã được lưu

Đạt điểm 1,00

Mô hình Bell La Padula (BLP) qui định cách truy xuất thông tin là gì

- a. No read up, no write up
- b. No read up, no write down
- c. No read down, no write up
- d. No read down, no write down

Clear my choice

Câu hỏi 7

Câu trả lời đã được lưu

Đạt điểm 1,00

Frank rất quan tâm đến các cuộc tấn công vào máy chủ thương mại điện tử của công ty. Ông đặc biệt lo lắng về tấn công SQL Injection. Điều nào sau đây sẽ bảo vệ tốt nhất trước cuộc tấn công cụ thể này?

- a. IDS
- b. Firewall
- c. Lọc dữ liệu người dùng nhập vào
- d. Lưu lượng truy cập web được mã hóa

Clear my choice

Câu hỏi 8

Câu trả lời đã được lưu

Đạt điểm 1,00

Hai dạng mã độc nào sau đây sống độc lập?

- [ ] a. Trojan
- [x] b. Worm
- [ ] c. Logic boom
- [x] d. Zombie
- [ ] e. Rootkit

Câu hỏi 9

Câu trả lời đã được lưu

Đạt điểm 1,00

What is the **confusion** property of Product ciphers

- a. hide the relationship between the ciphertext & the key
- b. hide the relationship between the key & the plaintext
- c. hide the relationship between the round keys
- d. hide the relationship between the ciphertext & the plaintext

Clear my choice

Câu hỏi 10

Câu trả lời đã được lưu

Đạt điểm 1,00

Given below figure, which mode in block cipher?

- a. cipher block chaining mode - CBC plain xor cipher trước mã hóa
- b. electronic codebook mode - ECB
- c. cipher feedback mode - CFB Khối ciphertext trước đó được phản hồi và kết hợp với khối plaintext tiếp theo trước khi mã hóa
- d. output feedback mode – OFB

Clear my choice

◄ **Chapter 12 - Hash - MAC - HMAC - Digital Signature**

Chuyển tới...

Review - Chapter 1,3,4,5,6 ►

An toan thong tin_ Nhom 10

Câu hỏi 11

Chưa trả lời

Đạt điểm 1,00

Ưu điểm của hệ thống phát hiện xâm nhập dựa vào dấu hiệu bất thường là gì?

- a. Phát hiện được các tấn công mới
- b. Kẻ tấn công không thể giả mạo được hành vi khác dấu hiệu tấn công
- c. Không bị cảnh báo sai
- d. Phát hiện chính xác các tấn công

Clear my choice

Câu hỏi 12

Chưa trả lời

Đạt điểm 1,00

Điều nào sau đây là rủi ro tiềm ẩn khi chương trình chạy ở chế độ đặc quyền?

- a. Nó có thể cho phép mã độc được chèn vào
- b. Nó có thể phục vụ cho việc tạo ra các đoạn mã phức tạp không cần thiết
- c. Nó có thể tạo ra việc loại bỏ các ứng dụng không cần thiết
- d. Nó có thể không thực hiện việc phân chia xử lý các tác vụ

Clear my choice

Câu hỏi 13

Chưa trả lời

Đạt điểm 1,00

In an Xmas Tree scan, what indicates that a port is open?

Select one:

- a. SYN
- b. ACK
- c. RST
- d. No return response

close

Clear my choice

Câu hỏi 14

Chưa trả lời

Đạt điểm 1,00

Điều nào sau đây mô tả tốt nhất cơ chế kiểm soát truy cập trong đó các quyết định kiểm soát truy cập dựa trên trách nhiệm của người dùng trong một tổ chức?

- a. Discretionary Access Control (DAC)
- b. Role Based Access Control (RBAC)
- c. Attribute Based Access Control (ABAC)
- d. Subjective Access Control (SAC)
- e. Mandatory Access Control (MAC)

Clear my choice

Câu hỏi 15

Chưa trả lời

Đạt điểm 1,00

Tấn công nào vượt qua được cơ chế bảo mật máy tính để truy cập vào máy tính không thông qua hệ thống xác thực?

- a. Front door
- b. Brute Force
- c. DoS
- d. Backdoor

Clear my choice

Thời gian còn lại 0:31:40

Câu hỏi 16

Chưa trả lời

Đạt điểm 1,00

Mục đích chính của các kỹ thuật điều khiển truy cập là?

- a. Cung cấp tất cả các quyền truy cập cho người dùng
- b. Ngăn chặn người dùng trái phép truy cập vào tài nguyên hệ thống
- c. Bảo vệ máy tính khỏi virus
- d. Giới hạn các quyền truy cập và các hành động cho người dùng hợp pháp được sử dụng

Clear my choice

Câu hỏi 17

Chưa trả lời

Đạt điểm 1,00

John muốn thêm luật (rule) vào ACL cho tệp script00.sh để cấp cho student04 quyền đọc và ghi đối với tệp đó. Lệnh nào sau đây được thực hiện?

- a. setfacl -x u:student04:rw- script00.sh
- b. getfacl -m u:student04:rw- script00.sh
- c. setfacl -m u:student04:rw- script00.sh
- d. getfacl -x u:student04:rw- script00.sh

Clear my choice

Câu hỏi 18

Chưa trả lời

Đạt điểm 1,00

Điều nào sau đây mô tả đúng nhất cơ chế kiểm soát truy cập cho phép chủ sở hữu dữ liệu tạo và quản lý kiểm soát truy cập?

- a. List Based Access Control (LBAC)
- b. Attribute Based Access Control (ABAC)
- c. Role Based Access Control (RBAC)
- d. Mandatory Access Control (MAC)
- e. Discretionary Access Control (DAC)

Clear my choice

Câu hỏi 19

Chưa trả lời

Đạt điểm 1,00

Firewall lọc gói dữ liệu dựa vào những yếu tố nào?

- a. Đường link
- b. IP nguồn, IP đích
- c. Vị trí đặt server
- d. Hệ điều hành của server

Clear my choice

Câu hỏi 20

Chưa trả lời

Đạt điểm 1,00

Which is the operation in DES function?

- a. Mixcolumn
- b. Compression P-box
- c. Shiftleft
- d. Straight P-box

Clear my choice

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

Chuyển tới...

Review - Chapter 1,3,4,5,6 ►

An toan thong tin_ Nhom 10

Câu hỏi 21

Chưa trả lời

Đạt điểm 1,00

Tấn công một máy tính bằng cách gửi các gói TCP handshake không đúng thứ tự đến đích (wrong order) xảy ra ở tầng nào?

- a. Network Interface layer
- b. Internet layer
- c. Transport layer
- d. Application layer

Clear my choice

Câu hỏi 22

Chưa trả lời

Đạt điểm 1,00

Một hệ thống xác thực sinh trắc học cho phép một người giả mạo hình thức nhân viên công ty khi vào hệ thống là hiện tượng gì sau?

- a. True positive
- b. True negative
- c. False negative
- d. False positive

Clear my choice

Câu hỏi 23

Chưa trả lời

Đạt điểm 1,00

Đảm bảo dữ liệu không bị sửa đổi trong quá trình lưu trữ hay trong quá trình truyền qua mạng bởi những người dùng không hợp pháp gọi là?

- a. Non-repudiation
- b. Confidentiality
- c. Availability
- d. Integrity

Clear my choice

Câu hỏi 24

Chưa trả lời

Đạt điểm 1,00

Ma trận điều khiển truy cập (Access control matrix) thể hiện mối quan hệ giữa các thành phần nào sau đây? (chọn 3)

- a. Database
- b. Object
- c. Subject
- d. Rights/Permissions
- e. Security policy
- f. Users

Câu hỏi 25

Chưa trả lời

Đạt điểm 1,00

Giả sử thuật toán RSA đã tạo ra cặp khóa pubic (7,187) và private (23,187). Muốn tạo chữ kí cho message M= 3 sẽ được tính là?

- a. 121
- b. 137
- c. 181
- d. 23

c = m^d mod n = 3^23 mod 187 = 181

Clear my choice

Thời gian còn lại 0:19:49

Câu hỏi 26

Chưa trả lời

Đạt điểm 1,00

Rủi ro chính từ việc sử dụng phần mềm lỗi thời (outdated software) là gì

- a. Nó có thể không có các tính năng bảo mật hiện đại nhất
- b. Nó có thể không có tất cả các tính năng bạn cần
- c. Có thể dễ dàng xâm nhập hơn phần mềm mới hơn
- d. Nó có thể không còn được hỗ trợ bởi các nhà cung cấp

Clear my choice

Câu hỏi 27

Chưa trả lời

Đạt điểm 1,00

Giải pháp StackGuard giúp phòng chống tấn công tràn bộ đệm trên stack thực hiện như sau

- a. Kiểm tra chiều dài dữ liệu nhập trước khi thực hiện việc gán dữ liệu
- b. Sử dụng một vùng nhớ đệm an toàn giữa Return Address và Buffer. Sử dụng vùng nhớ đệm an toàn này để kiểm tra xem Return Address có bị sửa đổi hay không
- c. Lưu trữ giá trị Return Address ở một nơi khác và sử dụng nó để kiểm tra xem giá trị ở Return Address có bị sửa đổi hay không
- d. Kiểm tra giá trị Return Address có bị sửa đổi hay không

Clear my choice

Câu hỏi 28

Chưa trả lời

Đạt điểm 1,00

Hệ thống phát hiện xâm nhập dựa vào bất thường (Anomaly-based IDS) hoạt động dựa vào yếu tố nào?

- a. Các tấn công
- b. Nội dung website xấu
- c. Các hành vi bình thường
- d. Các hành vi bất thường

Clear my choice

Câu hỏi 29

Chưa trả lời

Đạt điểm 1,00

Phương pháp nào sau đây là TỐT NHẤT để giảm hiệu quả của các cuộc tấn công lừa đảo trên mạng?

- a. Quét lỗ hổng cho hệ thống định kỳ
- b. Xác thực 2 yếu tố
- c. Đào tạo nâng cao nhận thức người dùng
- d. Phần mềm chống lừa đảo

Clear my choice

Câu hỏi 30

Chưa trả lời

Đạt điểm 1,00

Hệ thống phát hiện xâm nhập dựa vào dấu hiệu (Signature-based IDS) hoạt động dựa vào yếu tố nào?

- a. Các dấu hiệu bất thường
- b. Các dấu hiệu bình thường
- c. Các dấu hiệu tấn công
- d. Nội dung website

Clear my choice

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

Chuyển tới...

Review - Chapter 1,3,4,5,6 ►

An toan thong tin_ Nhom 10

Câu hỏi 41

Chưa trả lời

Đạt điểm 1,00

Trong mã hóa bất đối xứng (còn gọi là mã hóa hóa công khai). Alice cần **giải mã** văn bản mà Bob gửi cho thì Alice cần dùng khóa gì?

a. Khóa Private của Alice

b. Khóa Public của Bob

c. Khóa Private của Bob

d. Khóa Public của Alice

Clear my choice

Câu hỏi 42

Chưa trả lời

Đạt điểm 1,00

Tệp nào lưu trữ thông tin mật khẩu đã được mã hóa của hệ thống Unix?

Select one:

a. /etc/security.

b. /etc/passwd.

c. /etc/shadow.

d. /etc/pwlog

Clear my choice

Câu hỏi 43

Chưa trả lời

Đạt điểm 1,00

Việc gỡ bỏ những dịch vụ và giao thức không cần thiết gọi là?

a. Hardening

b. Auditing

c. Nonrepudiation

d. Hashing

Clear my choice

Câu hỏi 44

Chưa trả lời

Đạt điểm 1,00

Phần nào trong kiến trúc bộ nhớ lưu trữ biến cục bộ trong chương trình, các dữ liệu liên quan đến lời gọi hàm?

a. Data Segment

b. Stack

c. BSS segment

d. Text

e. Heap

Clear my choice

Câu hỏi 45

Chưa trả lời

Đạt điểm 1,00

Cho hai số nguyên tố p=13, q=19, giá trị e nào sẽ được chọn trong thuật toán mã hóa RSA từ số các giá trị sau:

e là SNT

a. 27

b. 21

c. 39

d. 35

Clear my choice

n = p.q = 13*19 = 247
N = (p-1)(q-1) = 216
GCD(e,216) = 1
=> e = 35 (public key)
e*d mod N = 1
=> e*d = 1 mod N
=> 35*d = 1 mod 216
=> d = 1 (private key)

Thời gian còn lại 0:04:51

Câu hỏi 46

Chưa trả lời

Đạt điểm 1,00

What is missing from a half-open scan?

Select one:

- a. RST
- b. FIN
- c. ACK
- d. SYN, ACK

Clear my choice

Câu hỏi 47

Chưa trả lời

Đạt điểm 1,00

Assume RSA has the pubic key (7,187) and private key (23,187). The ciphertext C= 3 will be decrypted to .....

- a. 171
- b. 133
- c. 181
- d. 121

m = c^d mod n = 3^23 mod 187 = 181

Clear my choice

Câu hỏi 48

Chưa trả lời

Đạt điểm 1,00

Các giải pháp mã hóa KHÔNG đảm bảo được tính chất nào sau đây

- a. Tính bí mật
- b. Tính xác thực
- c. Tính toàn vẹn
- d. Tính sẵn sàng

Clear my choice

Câu hỏi 49

Chưa trả lời

Đạt điểm 1,00

During an FIN scan, what indicates that a port is closed?

Select one:

- a. No return response
- b. SYN
- c. RST
- d. ACK

Clear my choice

Câu hỏi 50

Chưa trả lời

Đạt điểm 1,00

Given below table for encryption and decryption. Which is the plaintext of cypher = 010?

- a. 011
- b. 101
- c. 110
- d. 001

010 = 01 (ct) + 0 (hàng) = 110

Clear my choice

◄ **Chapter 12 - Hash - MAC - HMAC - Digital Signature**

Chuyển tới...

Review - Chapter 1,3,4,5,6 ►

An toan thong tin_ Nhom 10

Thời gian còn lại 0:01:02

Câu hỏi 51

Câu trả lời đã được lưu

Đạt điểm 1,00

Which are operations in Key generation of DES? (choose 2)

- a. Mixcolumn
- b. Compression P-box
- c. S-box
- d. Shift left

ChatGPT

Câu hỏi 52

Câu trả lời đã được lưu

Đạt điểm 1,00

Một hệ thống kiểm soát truy cập chỉ cấp cho người dùng những quyền cần thiết để họ thực hiện công việc đang hoạt động theo nguyên tắc bảo mật nào?

- a. Separation of Duties
- b. Discretionary Access Control
- c. Least Privilege
- d. Mandatory Access Control

Clear my choice

Câu hỏi 53

Câu trả lời đã được lưu

Đạt điểm 1,00

Kiểu tấn công nào sau đây không phải khai thác các lỗ hổng của ứng dụng Web?

- a. SQL Injection
- b. Social Engineering
- c. Cross-site scripting
- d. Cross Site Request Forgery

Clear my choice

Câu hỏi 54

Câu trả lời đã được lưu

Đạt điểm 1,00

Điều nào sau đây đúng khi nói về tấn công làm tràn bộ đệm (buffer Overflow)

- a. Xóa dữ liệu người dùng
- b. Kẻ tấn công gửi các chuỗi dữ liệu lớn làm tràn bộ đệm đã được thiết kế cho chương trình
- c. Ghi đè các giá trị lên các biến của chương trình nhằm thay đổi hành vi của chương trình theo mục đích của kẻ tấn công
- d. Xảy ra do kiểm tra dữ liệu đầu vào không đầy đủ hoặc bị bỏ qua

Clear my choice

Câu hỏi 55

Câu trả lời đã được lưu

Đạt điểm 1,00

Which are server involved in the Kerberos protocol? (choose 2)

- [x] a. Ticket-granting server
- [ ] b. Authorization Server
- [x] c. Authentication server
- [ ] d. Access control server

◄ **Chapter 12 - Hash - MAC - HMAC - Digital Signature**

Chuyển tới...

Review - Chapter 1,3,4,5,6 ►