Câu 1:

Sau đây là kết quả trả về của một lệnh **ping**.

PING vnexpress.net (111.65.250.2): 1500 data bytes

ping: sendto: Message too long

ping: sendto: Message too long

Từ kết quả trên, ta có thể kết luận: Mạng của website **vnexpress.net** không cho phép truyền gói tin có kích thước lớn hơn **1500** bytes.

A. Sai
B. Đúng

Câu 2: Cho ma trận điều khiển truy cập như sau.

Objects

Subjects

	File 1	File 2	File 3	...	File n
User 1	read	write	-	-	read
User 2	write	write	write	-	-
User 3	-	-	-	read	read
...					
User m	read	write	read	write	read

Cơ chế điều khiển truy cập **"Capability"** được cài đặt bằng cách lưu từng **cột** trong bảng trên cho mỗi tài nguyên.

A. Sai
B. Đúng

(Capability – Hàng; ACL – Cột)

Câu 3: Để có thể gây hư hại cho hệ thống thì mã độc phải thực hiện lời gọi hệ thống.

A. Sai
B. Đúng

Câu 4: Mô hình giám sát triển trình systrace có bộ lọc nhằm mục đích loại bỏ **tất cả** các lời gọi hệ thống.

A. Sai

B. Đúng

Câu 5: Các lời gọi **hàm, tham số đầu vào** và đầu ra của hàm được chứa trong thành phần nào sau đây

A. Text
B. Heap
C. Stack
D. Data

Câu 6: Hãy chọn câu giải thích đúng cho các tham số sau:

Đề	Đáp án
SUID	ID trước khi leo thang
RUID	ID người thực thi
EUID	ID người sở hữu

Câu 7: Đâu là điểm hạn chế của mã hoá đối xứng?

A. Việc phân phối khoá
B. Bẻ khoá bằng cách vét cạn
C. Thời gian xử lý
D. Kích thước khoá

(Đối xứng – bẻ khóa = vét cạn; Bất đ.xứng – t.gian x.lý)

Câu 8: Khi sticky bit được

Đề	Đáp án
Tắt	Ai cũng được xóa
Bật	Chủ mới được xóa

Câu 9: Cho hàm sinh chuỗi số như sau:

$X_{n+1} = (X_n + k) \bmod 5$

Biết $X_0 = 2$; $X_1=0$; $X_2=3$; $X_3=1$, giá trị nhỏ nhất của k là mấy

Answer: K=3

($X_1 = X_{0+1} = (X_0 + k) \bmod 5 = 0 <=> (2 + k) \bmod 5 = 0 => k = 3$

$X_2 = X_{1+1} = (X_1 + k) \bmod 5 = 3 <=> (0 + k) \bmod 5 = 3$ hoặc $= 8 => k = 3$

$X_3 = X_{2+1} = (X_2 + k) \bmod 5 = 0 <=> (3 + k) \bmod 5 = 1 => k = 3$)

Câu 10: Điều tra hệ thống (enumeration) là

A. Xác định các bộ vạch đường và tường lửa
B. Xác định người dùng và tên máy tính
C. Xác định các hệ thống đang hoạt động trong mạng
D. Bẻ khóa mật khẩu

Câu 11: Hệ thống máy tính có thể bị xâm nhập bất hợp pháp do

A. Lỗ hổng phần mềm.
B. Lừa đảo.
C. Bị nghe lén.
D. Tất cả các lựa chọn trên.

Câu 12:

Giả sử ta có biến c có chiều dài **08** bits được khai báo như sau:

char c;

Giả sử ta có phép gán

c = 0x80 + 0x80

thì giá trị được biểu diễn theo hệ thập phân của c sẽ là

A. 256
B. 180
C. 0
D. 128

(0x80 = 00000080 (Hex) => (Dec) = 128 mà c = 0x80 + 0x80 => (Dec) = 256 => (Bin) = 100000000; do c có chiều dài là 8 bits nên Bin = 00000000 => (Dec) = 0)

Câu 13: Thăm dò (footprinting) là gì?

A. Thu thập thông tin về mục tiêu
B. Ánh xạ sơ đồ vật lý của mạng máy tính mục tiêu
C. Quét hệ thống mục tiêu để tìm ra các loại hệ điều hành
D. Đo kích cỡ giày của hacker

Câu 14: Đâu là chuỗi các gói tin đúng dùng để bắt tay TCP?

A. SYN-SYN-ACK-ACK
B. SYN-ACK-FIN
C. SYN-ACK-RST
D. SYN-PSH-ACK

Câu 15: Công cụ nào sau đây có thể được dùng để thăm dò mục tiêu (footprinting) mà không bị phát hiện?

A. Host scanning
B. Ping

C. Traceroute

D. Whois search

Câu 16: Nguyên tắc "Quyền hạn tối thiểu" (Principle of Least Privilege) chỉ ra rằng:

A. Mỗi thành phần của hệ thống mặc định có toàn bộ quyền hạn, các luật an ninh theo sau sẽ giới hạn lại các quyền hạn này đủ cho thành phần của hệ thống hoạt động.

B. Mỗi thành phần của hệ thống nên được cấp phát số quyền hạn tối thiểu đủ cho nó hoàn thành mục tiêu đề ra

Câu 17: Trong trình duyệt Chromium thì thành phần nào sẽ được thực thi trong môi trường cô lập?

A. Nhân

B. Engine hiển thị nội dung

C. Plugin

D. Các kết nối mạng

Note: Các thành phần thực thi trong môi trường cô lập là Puppeteer – một thư viện của NodeJS. Câu lệnh cài đặt Puppeteer `npm install puppeteer puppeteer-extra puppeteer-extra-plugin-stealth puppeteer-extra-plugin-adblocker readline`

Câu 18: Việc tấn công tràn bộ đệm dựa trên một thực tế là địa chỉ trả về luôn nằm trên các biến cục bộ.

A. Sai

B. Đúng

Câu 19: Trong môi trường CentOS Linux, cấu trúc của thư mục **/tmp/test** được cho như sau:

```
[root@www test]# tree /tmp/test
/tmp/test
├── bin
│   ├── bash
│   └── ls
└── lib
    ├── ld-linux.so.2
    ├── libacl.so.1
    ├── libattr.so.1
    ├── libcap.so.2
    ├── libc.so.6
    ├── libdl.so.2
    ├── libpthread.so.0
    ├── librt.so.1
    ├── libselinux.so.1
    └── libtinfo.so.5

2 directories, 12 files
```

Giả sử: Trình thông dịch lệnh mặc định của hệ thống là **/bin/bash**; thư mục **/tmp/test/lib** chứa đầy đủ các thư viện cần thiết để chạy các lệnh trong **/tmp/test/bin**, người dùng **test** có UID **501** thuộc nhóm có GID **501**.

Sau khi người dùng root thực thi lệnh sau:

chroot --userspec=501:501 /tmp/test

thì trên cùng một cửa sổ lệnh, nếu ta thực thi tiếp lệnh

ls /

kết quả sẽ là:

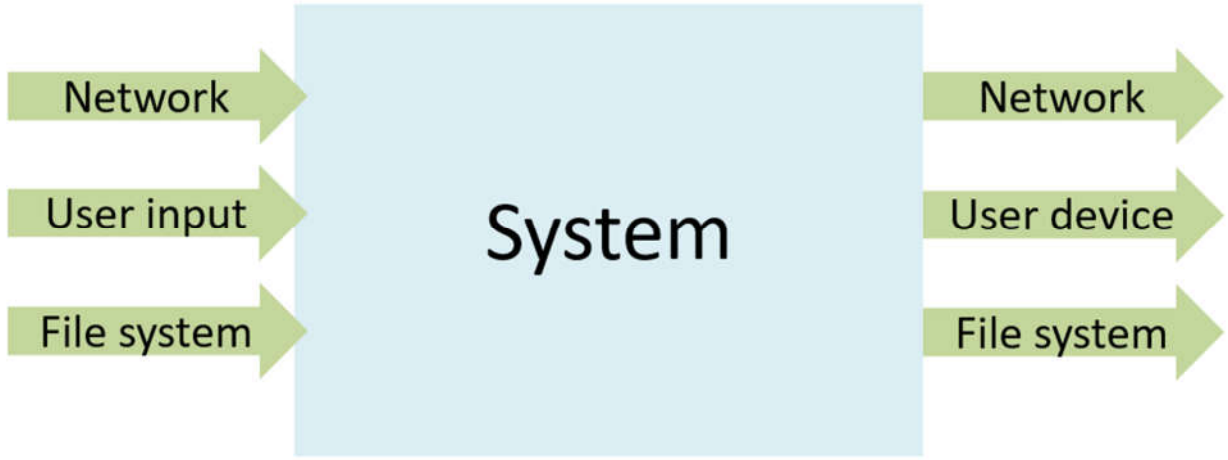
A. bin dev home lost+found mnt proc sbin srv tmp var boot etc lib media opt root selinux sys usr
B. bin lib
C. /tmp/test
D. Không hiển thị gì.

(hiện tại root đang đứng tại thư mục test, chroot --userspec=501:501 /tmp/test chỉ thay đổi quyền **root** không ảnh hưởng đề câu này , lệnh **ls /** hiển thị ra thư mục **bin** và **lib** như hình phía trên theo lệnh **tree**)

Câu 20: Điểm yếu của các hệ thống giao dịch bằng tài khoản-mật khẩu là

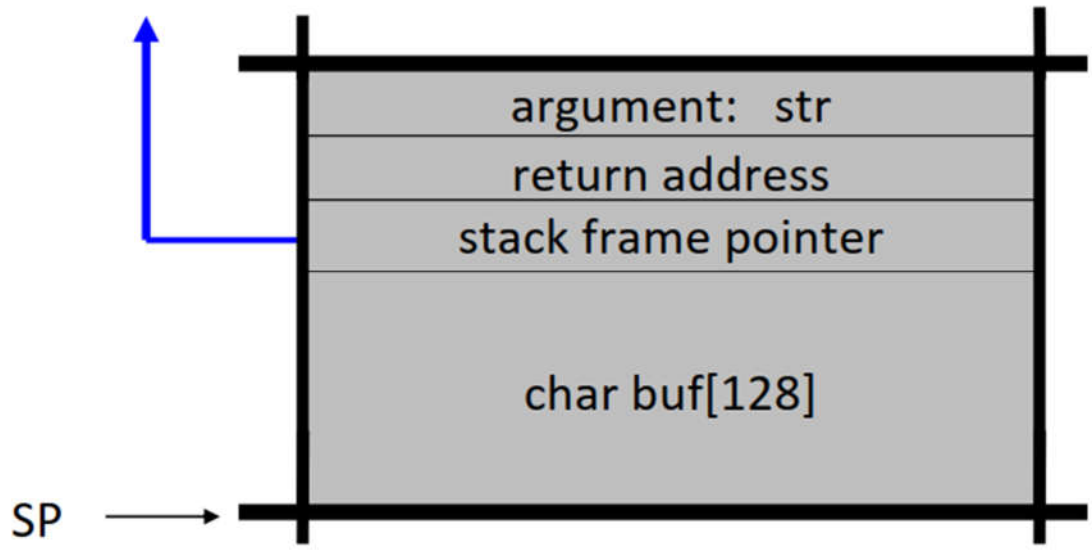
A. Mật khẩu có thể bị quên
B. Mật khẩu bị lộ
C. Dễ dàng dò tìm ra mật khẩu yếu
D. Tất cả các câu trả lời trên đều đúng

Câu 21: Thiết kế mô hình hệ thống sau đây **có thoả mãn** nguyên tắc "**Quyền hạn tối thiểu**" hay không?



A. Có
B. Không

Câu 22: Cho sơ đồ bộ nhớ của một hàm như sau:



Để chèn mã độc theo kiểu tràn bộ đệm (buffer overflow) thì mã độc phải **được chèn ít nhất đến phần nào trong khoảng bộ nhớ nêu trên** nhằm chuyển hướng điều khiển đến chương trình của kẻ tấn công?

A. return address
B. stack frame pointer
C. argument: str
D. char buf[128]

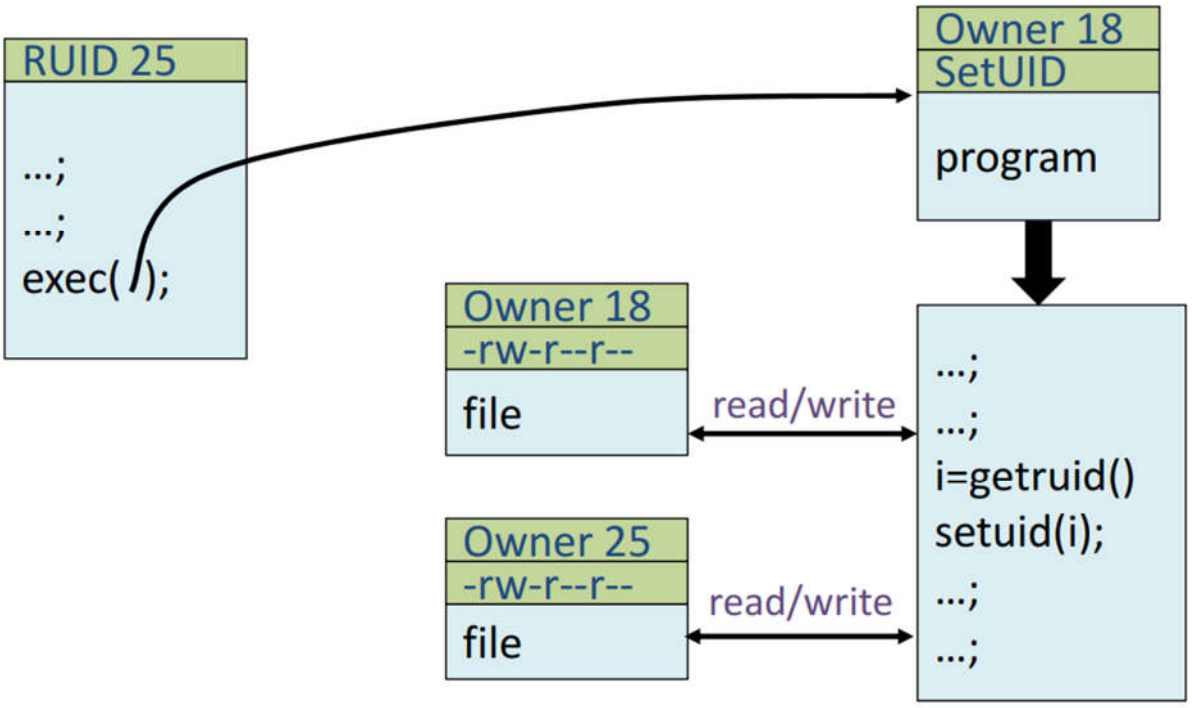
Câu 23: Khi xây dựng bộ giám sát máy ảo, người ta dựa trên giả thiết nào sau đây:

A. Mã độc có thể lây nhiễm các ứng dụng cũng như hệ điều hành khách (guest OS)
B. Mã độc không thể lây nhiễm các ứng dụng chạy trên các hệ điều hành khách (guest OS) khác.
C. Mã độc không thể lây nhiễm lên hệ điều hành chủ (host OS)
D. Bộ giám sát máy ảo phải biết cách tự bảo vệ chính nó.
E. Tất cả các giả thiết đều đúng.

Câu 24: Các **biến toàn cục** của chương trình được lưu ở thành phần nào sau đây

A. Heap
B. Data
C. Text
D. Stack

Câu 25: Cho lưu đồ thực thi các tiến trình như sau:



Sau khi chạy xong các tiến trình trên thì:

Đề	Đáp án
EUID	=25
RUID	=25

Câu 26: Bộ đóng gói (wrapper) là

A. Một hệ thống bị nhiễm Trojan
*B. Một chương trình được sử dụng để kết hợp một con Trojan và một **phần mềm** hợp pháp thành một tập tin thực thi được*
C. Một cách thức để truy cập một hệ thống bị nhiễm Trojan
D. Một chương trình được sử dụng kể kết hợp một con Trojan và một Backdoor thành một tập tin thực thi được

Câu 27: Một trong những cơ chế cô lập tiến trình là dung bộ giám sát truy cập tiến trình (reference monitor). Về nguyên tắc thì bộ giám sát truy cập không thể bị giết. Nếu bộ giám sát bị giết thì các tiến trình bị giám sát cũng bị giết theo.

A. Đúng
B. Sai

Câu 28: Một gói tin mà tất cả các cờ được bật lên là thuộc kiểu quét gì?

A. Syn scan

B. TCP connect
C. Full Open
D. XMAS

Câu 29: Với cơ chế điều khiển truy cập trong Unix thì quyền hạn truy cập của tiến trình trên các tài nguyên của hệ thống được mặc định thừa kế từ tiến trình cha của nó.

A. Đúng
B. Sai

Câu 30: Các hệ thống mã hoá sử dụng khóa dùng **một lần** (OTP) có an toàn đối với các cuộc tấn công nghe lén hay không?

A. Có
B. Không

Câu 31: Cổng mà dịch vụ HTTPS sử dụng là

A. 21
B. 80
C. 443
D. 53

(RMI: **1099**; Echo: **7**; SMTP: **25**; POP: **110**; Telnet: **23**; SNMP: **161**; RIP: **520**; IMAP: **143**; FTP: **21;** HTTP: **80**; HTTPS: **443**; DNS: **53**)

Câu 32: Đâu là kết quả của phép toán XOR từng bit trên hai chuỗi bit sau:

0101110010

1100011000

Answer: 1001101010

(**Gợi ý:** Cộng không nhớ)

Câu 33: Máy ảo có được xem là một cơ chế để cô lập tiến trình hay không?

A. Không
B. Có

Câu 34: Cho hàm sinh khóa như sau:

$X_{n+1} = (X_n + 7) \bmod 16$, với X_i, dài 04 bits.

Biết khóa ban đầu có giá trị nhị phân là 1010. Nếu dùng hàm trên để sinh khoá dài 16 bits thì giá trị nhị phân của khóa 16 bits này là gì?

Answer: 1010 0001 1000 1111

(Đổi $X_{0(Bin)} = 1010 \Rightarrow X_{0(Dec)} = 10$. Chỉ lấy **Thập phân (Dec) tính**

$X_1 = (X_0 + 7) \bmod 16 = (10 + 7) \bmod 16 \Rightarrow X_{1(Dec)} = 1 \Rightarrow X_{1(Bin)} = 0001$

$X_2 = (X_1 + 7) \bmod 16 = (1 + 7) \bmod 16 \Rightarrow X_{2(Dec)} = 8 \Rightarrow X_{2(Bin)} = 1000$

$X_3 = (X_2 + 7) \bmod 16 = (8 + 7) \bmod 16 \Rightarrow X_{3(Dec)} = 15 \Rightarrow X_{3(Bin)} = 1111$)

Câu 35: Bạn được thông báo là hệ thống đang bị tấn công. Khi giám sát lưu thông mạng, bạn nhận thấy hầu hết các gói tin đều được chuyển đến một số địa chỉ IP cố định. Tuy nhiên nhân viên trong công ty không có bất kỳ phàn nàn nào về các dấu hiệu truy cập trái phép hệ thống của họ hoặc hiệu năng mạng giảm. Server nào sau đây có thể đã bị tấn công?

A. DNS
B. DHCP
C. FTP
D. Web

Câu 36: Giả sử trang Web **site.com/index.php** chứa đoạn mã PHP như sau:

<?php echo "Hello".$_GET["name"]; ?>

Trang Web trên có lỗ hổng để cho phép tấn công SQL Injection.

A. Đúng
B. Không

Câu 37: Theo thống kê từ báo cáo Kaspersky Security Bulletin 2015, thành phần nào sau đây bị khai thác lỗ hổng nhiều nhất

A. Microsoft Office
B. Trình duyệt
C. Android
D. Adobe Flash Player

Câu 38: Chương trình độc hại trong môi trường bị giam hãm (jail, chroot) **vẫn có thể kết nối mạng** và **tác động** đến các máy tính khác

A. Sai
B. Đúng

Câu 39: Hàm nào sau đây là an toàn đối với kỹ thuật tấn công tràn bộ đệm (stack overflow)?

A. strcpy (char *dest, const char *src)
B. strcat (char *dest, const char *src)
C. gets (char*s)
D. scanf (const char *format, ...)
E. Không có hàm nào trong danh sách là an toàn.

(Hàm an toàn là: strncpy & strncat)

Câu 40: Mã lệnh của chương trình được chứa trong thành phần nào sau đây

A. Stack
B. Text
C. Heap
D. Data

Câu 41: Loại tấn công mật khẩu nào có khả năng thành công nhất để bẻ mật khẩu sau **T63k#s23A**?

A. Password guessing
B. Brute force
C. Hybrid
D. Dictionary

Câu 42: Cho hàm băm sau.

h = x mod 13

với **x** lần lượt là 27 và 130 thì giá trị tương ứng của **h** là:

A. 1, 10
B. 1, 0
C. 13, 0
D. 2, 3

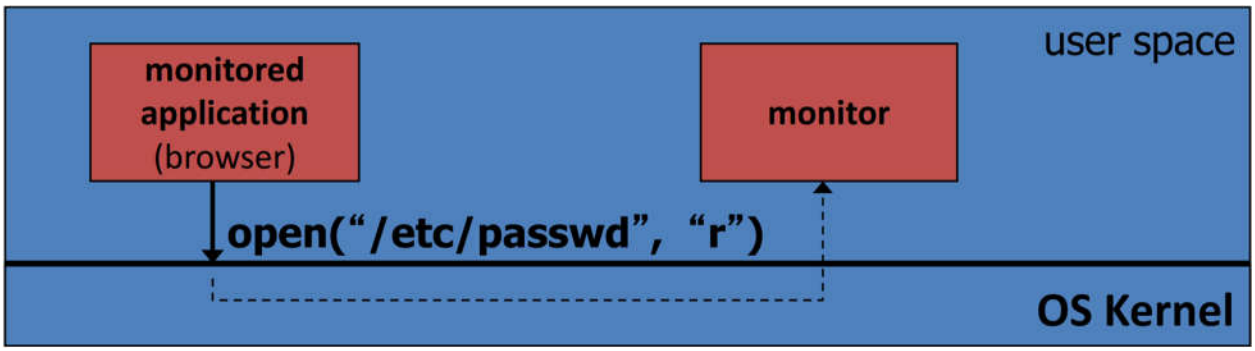
Câu 43: Cho dòng thông tin như sau:

drwxr-xr-x 4 phipham wheel 128 Nov 27 09:56 bin

Quyền hạn truy cập lên thư mục được biểu diễn thành dạng số sẽ là:

A. 766
B. 755
C. 744
D. 777

Câu 44: Mô hình giám sát tiến trình **ptrace** trong **Linux** có cấu trúc như sau:



Phát biểu nào sau đây là đúng.

A. Nếu tiến trình bị giám sát nhân bản thì bộ giám sát (monitor) cũng phải nhân bản.
B. Nếu bộ giám sát (monitor) chết thì tiến trình bị giám sát phải bị giết.
C. Bộ giám sát phải duy trì toàn bộ trạng thái liên quan đến tiến trình bị giám sát.
D. Tất cả các phát biểu đều đúng.

Câu 45: Rootkit là gì?

A. Một chương trình phá hoại mà nó lây nhiễm sang các tập tin hệ thống bao gồm cả nhân và các thư viện hệ thống
B. Một Trojan mà nó gởi thông tin qua bộ chuyển tiếp SMB
C. Một công cụ đơn giản để lấy quyền truy xuất đến thư mục gốc của hệ điều hành Windows
D. Một công cụ cho phép tấn công tràn bộ đệm

Câu 46: Các biến được **cấp phát động** được chứa trong thành phần nào sau đây

A. Text
B. Heap
C. Data
D. Stack

Câu 47: Mẫu tin DNS dùng để phân giải tên miền thành địa chỉ IP là mẫu tin kiểu:

A. CNAME
B. MX
C. PTR
D. NS
E. A

(CNAME: alias, MX:Mail Server; PTR; NS: tên miền; A: địa chỉ IP)

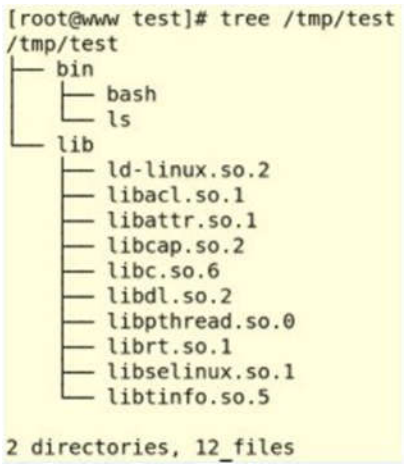
Câu 48: Một người dùng trong hệ thống lo lắng rằng ai đó đã dùng tài khoản của mình để truy cập dữ liệu nhạy cảm. Nhà quản trị hệ thống phải kiểm tra những sự kiện nào trong hệ thống để nhận định sự việc có xảy ra hay không?

A. Các hành động sửa đổi tài khoản thành công
B. Các hành động sử dụng tài khoản tăng bất thường trong giờ nghỉ
C. Các hành động truy cập máy in và các tài nguyên khác thành công và thất bại
D. Các hành động khởi động lại và tắt hệ thống thành công

Câu 49: Cơ chế cô lập tiến trình trong Android được thể hiện như sau.

A. Mỗi tiến trình được cấp một UID riêng và được chạy trên một máy ảo riêng.
B. Có một bộ giám sát lời gọi hệ thống cho mỗi tiến trình.
C. Hệ thống cấp sẵn một số lượng tối thiểu cho tiến trình.
D. Cung cấp bộ nhớ chia sẻ được giám sát bởi nhân để các tiến trình có thể giao tiếp với nhau.

Câu 50: Trong môi trường CentOS Linux, cấu trúc của thư mục **/tmp/test** được cho như sau:



Giả sử: Trình thông dịch lệnh mặc định của hệ thống là **/bin/bash**; thư mục **/tmp/test/lib** chứa đầy đủ các thư viện cần thiết để chạy các lệnh trong **/tmp/test/bin**, người dùng **test** có UID **501** thuộc nhóm có GID **501**.

Sau khi người dùng root thực thi lệnh sau:

chroot --userspec=501:501 /tmp/test

thì chuyện gì xảy ra?

A. Người dùng **root** sẽ được gán cho chạy trình thông dịch lệnh **/bin/bash**
B. Thư mục chủ của người dùng **root** trở thành **/tmp/test**
C. Người sở hữu thư mục **/tmp/test** là **test**
*D. Người dùng **test** sẽ được gán cho chạy trình thông dịch lệnh **/bin/bash***

Câu 51: Cho hàng thông tin sau:

drwxr-xr-x 4 phipham wheel 128 Nov 27 09:56 bin

Hãy chọn chú thích đúng cho các thông tin sau:

Đề	Đáp án
rwxr-xr-x	Phân quyền
wheel	Nhóm sở hữu
phipham	Người sở hữu
128	Kích thước

Câu 52: Cho ma trận điều khiển truy cập như sau:

Objects

Subjects

	File 1	File 2	File 3	...	File n
User 1	read	write	-	-	read
User 2	write	write	write	-	-
User 3	-	-	-	read	read
...					
User m	read	write	read	write	read

Cơ chế điều khiển truy cập "Access Control List" (ACL) được cài đặt bằng cách lưu từng cột trong bảng trên cho mỗi tài nguyên

A. Sai
B. Đúng

(Capability – Hàng; ACL – Cột)