BT Chuong 3, 4 CoVan

An toàn thông tin (Trường Đại học Sư phạm Kỹ Thuật Thành phố Hồ Chí Minh)

An toan thong tin_ Nhom 10

Nhà của tôi / Các khoá học của tôi / INSE330380_23_1_10 / Chapter 4 - Operation System Security / Test_C3-C4

Bắt đầu vào lúc	Friday, 6 October 2023, 1:45 PM
Trạng thái	Đã xong
Kết thúc lúc	Friday, 6 October 2023, 1:52 PM
Thời gian thực hiện	6 phút 58 giây
Điểm	9,00/30,00
Điểm	**3,00** trên 10,00 (**30**%)

Câu hỏi 1

Sai

Đạt điểm 0,00 trên 1,00

Which of the following protocols is the security administrator observing in this packet capture?
12:33:43, SRC 192.168.4.3:3389, DST 10.67.33.20:8080, SYN/ACK

Select one:

● a. HTTPS ✗

○ b. HTTP

○ c. SFTP

○ d. RDP

Your answer is incorrect.

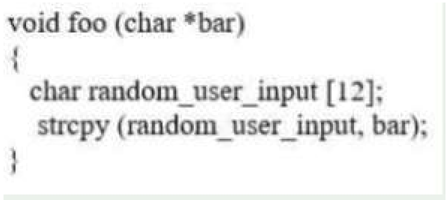
The correct answer is: RDP

Câu hỏi 2

Sai

Đạt điểm 0,00 trên 1,00

An analyst is reviewing a simple program for potential security vulnerabilities before being deployed to a Windows server. Given the following code:



```
void foo (char *bar)
{
   char random_user_input [12];
    strcpy (random_user_input, bar);
}
```

Which of the following vulnerabilities is present?

Select one:

● a. Backdoor ✗

○ b. Buffer overflow

○ c. Bad memory pointer

○ d. Integer overflow

Your answer is incorrect.

The correct answer is: Buffer overflow

Câu hỏi 3

Đúng một phần

Đạt điểm 0,50 trên 1,00

Which of the following, if properly implemented, would prevent users from accessing files that are unrelated to their job duties? (Select TWO).

Select one or more:

□ a. Job rotation

☑ b. Separation of duties ✓

☑ c. Time of day restrictions ✗

□ d. Mandatory vacation

□ e. Least privilege

Your answer is partially correct.

Bạn đã chọn đúng 1.
The correct answers are: Separation of duties, Least privilege

Câu hỏi 4

Đúng

Đạt điểm 1,00 trên 1,00

A vulnerability scan is reporting that patches are missing on a server. After a review, it is determined that the application requiring the patch does not exist on the operating system. Which of the following describes this cause?

Select one:

○ a. Baseline code review

○ b. Application hardening

○ c. False negative

● d. False positive ✓

Your answer is correct.

The correct answer is: False positive

Câu hỏi 5

Đúng

Đạt điểm 1,00 trên 1,00

Data execution prevention is a feature in most operating systems intended to protect against which type of attack?

Select one:

● a. Buffer overflow ✓

○ b. Cross-site scripting

○ c. SQL injection

○ d. Header manipulation

Your answer is correct.

The correct answer is: Buffer overflow

Câu hỏi 6

Sai

Đạt điểm 0,00 trên 1,00

If you declare an array as A[100] in C and you try to write data to A[555], what will happen?

Select one:

○ a. Nothing

○ b. Whatever is at A[555] will be overwritten

● c. There will always be a runtime error ✗

○ d. The C compiler will give you an error and won’t compile

Your answer is incorrect.

The correct answer is: Whatever is at A[555] will be overwritten

Câu hỏi 7

Đúng một phần

Đạt điểm 0,50 trên 1,00

What is likely to happen if you find a buffer overflow during testing by entering a random, long string for a C program?

Select one or more:

□ a. The C fairy sprinkles magic memory dust on the memory that was overwritten and makes everything okay again.

□ b. The program crashes

☑ c. The program gives you a “Buffer overflow at line X” error ✗

☑ d. Data is corrupted ✓

Your answer is partially correct.

Bạn đã chọn đúng 1.
The correct answers are: Data is corrupted, The program crashes

Câu hỏi 8

Đúng

Đạt điểm 1,00 trên 1,00

A web server hosted on the Internet was recently attacked, exploiting a vulnerability in the operating system. The operating system vendor assisted in the incident investigation and verified the vulnerability was not previously known. What type of attack was this?

Select one:

○ a. Botnet

○ b. Distributed denial-of-service

● c. Zero-day exploit ✓

○ d. Denial-of-service

Your answer is correct.

The correct answer is: Zero-day exploit

Câu hỏi 9

Đúng

Đạt điểm 1,00 trên 1,00

A malicious individual is attempting to write too much data to an application's memory. Which of the following describes this type of attack?

Select one:

● a. Buffer overflow ✓

○ b. XSRF

○ c. Zero-day

○ d. SQL injection

Your answer is correct.

The correct answer is: Buffer overflow

Câu hỏi 10

Sai

Đạt điểm 0,00 trên 1,00

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

Select one:

○ a. A biometric iris scanner rejects an authorized user wearing a new contact lens.

○ b. The IDS does not identify a buffer overflow

● c. A user account is locked out after the user mistypes the password too many times. ✖

○ d. Anti-virus identifies a benign application as malware.

Your answer is incorrect.

The correct answer is: Anti-virus identifies a benign application as malware.

Câu hỏi 11

Sai

Đạt điểm 0,00 trên 1,00

Which of the following provides the BEST application availability and is easily expanded as demand grows?

Select one:

○ a. RAID 6

○ b. Server virtualization

● c. Active-Passive Cluster ✖

○ d. Load balancing

Your answer is incorrect.

The correct answer is: Load balancing

Câu hỏi 12

Sai

Đạt điểm 0,00 trên 1,00

Which of the following ports is used for TELNET by default?

Select one:

○ a. 23

● b. 21 ✖

○ c. 22

○ d. 20

Your answer is incorrect.

The correct answer is: 23

Câu hỏi 13

Sai

Đạt điểm 0,00 trên 1,00

One of the system administrators at a company is assigned to maintain a secure computer lab. The administrator has rights to configure machines, install software, and perform user account maintenance. However, the administrator cannot add new computers to the domain, because that requires authorization from the Information Assurance Officer. This is an example of which of the following?

Select one:

○ a. Least privilege

○ b. Rule-based access control

● c. Mandatory access ✖

○ d. Job rotation

Your answer is incorrect.

The correct answer is: Least privilege

Câu hỏi 14

Sai

Đạt điểm 0,00 trên 1,00

Which of the following describes the process of removing unnecessary accounts and services from an application to reduce risk exposure?

Select one:

○ a. Error and exception handling

○ b. Application hardening

● c. Cross-site script prevention ✖

○ d. Application patch management

Your answer is incorrect.

The correct answer is: Application hardening

Câu hỏi 15

Sai

Đạt điểm 0,00 trên 1,00

Which of the following concepts allows an organization to group large numbers of servers together in order to deliver a common service?

Select one:

○ a. Clustering

○ b. Cold site

● c. RAID ✖

○ d. Backup Redundancy

Your answer is incorrect.

The correct answer is: Clustering

Câu hỏi 16

Sai

Đạt điểm 0,00 trên 1,00

Disabling unnecessary services, restricting administrative access, and enabling auditing controls on a server are forms of which of the following?

Select one:

○ a. System hardening

○ b. Application patch management

● c. Creating a security baseline ✗

○ d. Cross-site scripting prevention

Your answer is incorrect.

The correct answer is: System hardening

Câu hỏi 17

Sai

Đạt điểm 0,00 trên 1,00

Failure to validate the size of a variable before writing it to memory could result in which of the following application attacks?

Select one:

○ a. Cross-site scripting

○ b. Malicious logic

● c. SQL injection ✗

○ d. Buffer overflow

Your answer is incorrect.

The correct answer is: Buffer overflow

Câu hỏi 18

Sai

Đạt điểm 0,00 trên 1,00

A server administrator notes that a legacy application often stops running due to a memory error. When reviewing the debugging logs, they notice code being run calling an internal process to exploit the machine. Which of the following attacks does this describe?

Select one:

○ a. Buffer overflow

○ b. Zero-day

● c. Cross site scripting ✗

○ d. Malicious add-on

Your answer is incorrect.

The correct answer is: Buffer overflow

Câu hỏi 19

Đúng

Đạt điểm 1,00 trên 1,00

A recent audit had revealed weaknesses in the process of deploying new servers and network devices. Which of the following practices could be used to increase the security posture during deployment? (Select TWO).

Select one or more:

□ a. Implement an application firewall

□ b. Deploy a honeypot

□ c. Penetration testing

☑ d. Change default password ✓

☑ e. Disable unnecessary services ✓

Your answer is correct.

The correct answers are: Disable unnecessary services, Change default password

Câu hỏi 20

Sai

Đạt điểm 0,00 trên 1,00

Which of the following risk mitigation strategies will allow Ann, a security analyst, to enforce least privilege principles?

Select one:

○ a. Incident management

○ b. User rights reviews

● c. Annual loss expectancy ✖

○ d. Risk based controls

Your answer is incorrect.

The correct answer is: User rights reviews

Câu hỏi 21

Sai

Đạt điểm 0,00 trên 1,00

Which of the following preventative controls would be appropriate for responding to a directive to reduce the attack surface of a specific host?

Select one:

○ a. Disabling unnecessary services

○ b. Implementing an IDS

● c. Taking a baseline configuration ✖

○ d. Installing anti-malware

Your answer is incorrect.

The correct answer is: Disabling unnecessary services

Câu hỏi 22

Đúng một phần

Đạt điểm 0,50 trên 1,00

A recent audit has revealed weaknesses in the process of deploying new servers and network devices. Which of the following practices could be used to increase the security posture during deployment? (Select TWO).

Select one or more:

- □ a. Deploy a honeypot
- □ b. Change default passwords
- ☑ c. Implement an application firewall ✗
- ☑ d. Disable unnecessary services ✓
- □ e. Penetration testing

Your answer is partially correct.

Bạn đã chọn đúng 1.
The correct answers are: Disable unnecessary services, Change default passwords

Câu hỏi 23

Sai

Đạt điểm 0,00 trên 1,00

Which of the following is a software vulnerability that can be avoided by using input validation?

Select one:

- ○ a. Application fuzzing
- ○ b. Buffer overflow
- ● c. Error handling ✗
- ○ d. Incorrect input

Your answer is incorrect.

The correct answer is: Incorrect input

Câu hỏi 24

Đúng

Đạt điểm 1,00 trên 1,00

A security administrator is investigating a recent server breach. The breach occurred as a result of a zero-day attack against a user program running on the server. Which of the following logs should the administrator search for information regarding the breach?

Select one:

○ a. Authentication log

○ b. Setup log

● c. Application log ✓

○ d. System log

Your answer is correct.

The correct answer is: Application log

Câu hỏi 25

Đúng

Đạt điểm 1,00 trên 1,00

A network security engineer notices unusual traffic on the network from a single IP attempting to access systems on port 23. Port 23 is not used anywhere on the network. Which of the following should the engineer do to harden the network from this type of intrusion in the future?

Select one:

○ a. Implement password requirements on servers and network devices

○ b. Enable auditing on event logs

● c. Disable unnecessary services on servers ✓

○ d. Disable unused accounts on servers and network devices

Your answer is correct.

The correct answer is: Disable unnecessary services on servers

Câu hỏi 26

Sai

Đạt điểm 0,00 trên 1,00

An IT security technician needs to establish host based security for company workstations. Which of the following will BEST meet this requirement?

Select one:

○ a. Implement database hardening by applying vendor guidelines.

○ b. Implement perimeter firewall rules to restrict access.

● c. Implement IIS hardening by restricting service accounts. ✗

○ d. Implement OS hardening by applying GPOs.

Your answer is incorrect.

The correct answer is: Implement OS hardening by applying GPOs.

Câu hỏi 27

Sai

Đạt điểm 0,00 trên 1,00

A Human Resources user is issued a virtual desktop typically assigned to Accounting employees. A system administrator wants to disable certain services and remove the local accounting groups installed by default on this virtual machine. The system administrator is adhering to which of the following security best practices?

Select one:

○ a. Black listing applications

○ b. Mandatory Access Control

● c. Patch Management ✗

○ d. Operating System hardening

Your answer is incorrect.

The correct answer is: Operating System hardening

Câu hỏi 28

Sai

Đạt điểm 0,00 trên 1,00

Which of the following ports will be used for logging into secure websites?

Select one:

● a. 142 ✖

○ b. 80

○ c. 443

○ d. 110

Your answer is incorrect.

The correct answer is: 443

Câu hỏi 29

Sai

Đạt điểm 0,00 trên 1,00

Ann, the software security engineer, works for a major software vendor. Which of the following practices should be implemented to help prevent race conditions, buffer overflows, and other similar vulnerabilities prior to each production release?

Select one:

○ a. Input validation

○ b. Patch regression testing

● c. Product baseline report ✖

○ d. Code review

Your answer is incorrect.

The correct answer is: Code review

Câu hỏi 30

Đúng một phần

Đạt điểm 0,50 trên 1,00

After an assessment, auditors recommended that an application hosting company should contract with additional data providers for redundant high speed Internet connections. Which of the following is MOST likely the reason for this recommendation? (Select TWO).

Select one or more:

- □ a. To improve intranet communication speeds
- □ b. To allow load balancing for cloud support
- □ c. To eliminate a single point of failure
- ☑ d. To allow for a hot site in case of disaster ✗
- ☑ e. To allow for business continuity if one provider goes out of business ✓

Your answer is partially correct.

Bạn đã chọn đúng 1.
The correct answers are: To allow for business continuity if one provider goes out of business, To eliminate a single point of failure

◄ Chapter 4 - LAB_Step-by-Step Exploit OS Vulnerabilities

Chuyển tới...

Video: OS Security ►