

# An toan thong tin\_ Nhom 03

<b>Started on</b>	Tuesday, 16 June 2020, 12:24 PM
<b>State</b>	Finished
<b>Completed on</b>	Tuesday, 16 June 2020, 12:46 PM
<b>Time taken</b>	21 mins 25 secs
<b>Marks</b>	27.50/30.00
<b>Grade</b>	<b>9.17</b> out of 10.00 ( <b>92%</b> )

## Question 1

Correct

Mark 1.00 out of 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. Change default passwords
- ☒ b. Disable unnecessary services
- ☐ c. Implement an application firewall
- ☐ d. Penetration testing
- ☐ e. Deploy a honeypot

Your answer is correct.

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

## Question 2

Correct

Mark 1.00 out of 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. Buffer overflow
- ☐ b. SQL injection
- ☐ c. Malicious logic
- ☐ d. Cross-site scripting

Your answer is correct.

The correct answer is: Buffer overflow

**Question 3**

Correct

Mark 1.00 out of 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. Change default password
- ☐ b. Implement an application firewall
- ☐ c. Penetration testing
- ☒ d. Disable unnecessary services
- ☐ e. Deploy a honeypot

Your answer is correct.

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

**Question 4**

Correct

Mark 1.00 out of 1.00

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

Select one:

- ☐ a. Cross-site scripting
- ☐ b. Header manipulation
- ☒ c. Buffer overflow
- ☐ d. SQL injection

Your answer is correct.

The correct answer is: Buffer overflow

**Question 5**

Correct

Mark 1.00 out of 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. Incorrect input
- ☐ d. Error handling

Your answer is correct.

The correct answer is: Incorrect input

**Question 6**

Correct

Mark 1.00 out of 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. Disable unused accounts on servers and network devices
- ☐ b. Implement password requirements on servers and network devices
- ☒ c. Disable unnecessary services on servers
- ☐ d. Enable auditing on event logs

Your answer is correct.

The correct answer is: Disable unnecessary services on servers

**Question 7**

Correct

Mark 1.00 out of 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. Patch regression testing
- ☐ b. Product baseline report
- ☒ c. Code review
- ☐ d. Input validation

Your answer is correct.

The correct answer is: Code review

**Question 8**

Correct

Mark 1.00 out of 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 allow load balancing for cloud support
- ☒ b. To eliminate a single point of failure A high-speed internet connection to a second data provider could be used to keep an up-to-date replicate of the main site. In case of problem on the first site, operation can quickly switch to the second site. This eliminates the single point of failure and allows the business to continue uninterrupted on the second site.
- ☐ c. To improve intranet communication speeds
- ☐ 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 correct.

The correct answers are: To allow for business continuity if one provider goes out of business, To eliminate a single point of failure

**Question 9**

Correct

Mark 1.00 out of 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. Application patch management
- ☐ b. Creating a security baseline
- ☒ c. System hardening Hardening is the process of securing a system by reducing its surface of vulnerability. Reducing the surface of vulnerability typically includes removing or disabling unnecessary functions and features, removing or disabling unnecessary user accounts, disabling unnecessary protocols and ports, and disabling unnecessary services.
- ☐ d. Cross-site scripting prevention

Your answer is correct.

The correct answer is: System hardening

**Question 10**

Correct

Mark 1.00 out of 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. Application log
- ☐ c. System log
- ☐ d. Setup log

Your answer is correct.

The correct answer is: Application log

**Question 11**

Correct

Mark 1.00 out of 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 Preventive controls are to stop something from happening. These can include locked doors that keep intruders out, user training on potential harm (to keep them vigilant and alert), or even biometric devices and guards that deny access until authentication has occurred. By disabling all unnecessary services you would be reducing the attack surface because then there is less opportunity for risk incidents to happen. There are many risks with having many services enabled since a service can provide an attack vector that someone could exploit against your system. It is thus best practice to enable only those services that are absolutely required.
- ☐ b. Installing anti-malware
- ☐ c. Taking a baseline configuration
- ☐ d. Implementing an IDS

Your answer is correct.

The correct answer is: Disabling unnecessary services

**Question 12**

Correct

Mark 1.00 out of 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. Application hardening
- ☐ b. Application patch management
- ☐ c. Cross-site script prevention
- ☐ d. Error and exception handling

Your answer is correct.

The correct answer is: Application hardening

**Question 13**

Correct

Mark 1.00 out of 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. Mandatory Access Control
- ☐ b. Patch Management
- ☐ c. Black listing applications
- ☒ d. Operating System hardening    Operating System hardening is the process of securing the operating system by reducing its surface of vulnerability. Reducing the surface of vulnerability typically includes removing unnecessary functions and features, removing unnecessary usernames or logins and disabling unnecessary services.

Your answer is correct.

The correct answer is: Operating System hardening

**Question 14**

Correct

Mark 1.00 out of 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. Application hardening
- ☐ b. False negative
- ☐ c. Baseline code review
- ☒ d. False positive

Your answer is correct.

The correct answer is: False positive

**Question 15**

Correct

Mark 1.00 out of 1.00

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

Select one:

- ☒ a. 23
- ☐ b. 21
- ☐ c. 20
- ☐ d. 22

Your answer is correct.

The correct answer is: 23

**Question 16**

Partially correct

Mark 0.50 out of 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.

You have correctly selected 1.

The correct answers are: Data is corrupted, The program crashes

**Question 17**

Correct

Mark 1.00 out of 1.00

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

Select one:

- ☐ a. Risk based controls
- ☐ b. Incident management
- ☒ c. User rights reviews A least privilege policy should be used when assigning permissions. Give users only the permissions and rights that they need to do their work and no more.
- ☐ d. Annual loss expectancy

Your answer is correct.

The correct answer is: User rights reviews

**Question 18**

Incorrect

Mark 0.00 out of  
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. Zero-day
- ☐ b. XSRF
- ☐ c. SQL injection
- ☐ d. Buffer overflow

Your answer is incorrect.

The correct answer is: Buffer overflow

**Question 19**

Correct

Mark 1.00 out of  
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. Distributed denial-of-service
- ☐ b. Denial-of-service
- ☒ c. Zero-day exploit
- ☐ d. Botnet

Your answer is correct.

The correct answer is: Zero-day exploit



**Question 20**

Correct

Mark 1.00 out of 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. Integer overflow
- ☐ b. Backdoor
- ☐ c. Bad memory pointer
- ☒ d. Buffer overflow

Your answer is correct.

The correct answer is: Buffer overflow

**Question 21**

Correct

Mark 1.00 out of 1.00

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

Select one:

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

Your answer is correct.

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

**Question 22**

Correct

Mark 1.00 out of 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    A least privilege policy should be used when assigning permissions. Give users only the permissions that they need to do their work and no more.
- ☐ b. Rule-based access control
- ☐ c. Job rotation
- ☐ d. Mandatory access

Your answer is correct.

The correct answer is: Least privilege

**Question 23**

Incorrect

Mark 0.00 out of 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. Malicious add-on
- ☒ b. Zero-day
- ☐ c. Buffer overflow
- ☐ d. Cross site scripting

Your answer is incorrect.

The correct answer is: Buffer overflow

**Question 24**

Correct

Mark 1.00 out of 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 Anytime you connect multiple computers to work/act together as a single server, it is known as clustering. Clustered systems utilize parallel processing (improving performance and availability) and add redundancy (but also add costs). Clustering is done whenever you connect multiple computers to work and act together as a single server. It is meant to utilize parallel processing and can also add to redundancy.
- ☐ b. Cold site
- ☐ c. RAID
- ☐ d. Backup Redundancy

Your answer is correct.

The correct answer is: Clustering

**Question 25**

Correct

Mark 1.00 out of 1.00

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

Select one:

- ☐ a. Active-Passive Cluster
- ☐ b. RAID 6
- ☒ c. Load balancing Load balancing is a way of providing high availability by splitting the workload across multiple computers.
- ☐ d. Server virtualization

Your answer is correct.

The correct answer is: Load balancing

**Question 26**

Correct

Mark 1.00 out of 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. Mandatory vacation
- ☐ b. Time of day restrictions
- ☒ c. Least privilege
- ☒ d. Separation of duties
- ☐ e. Job rotation

Your answer is correct.

The correct answers are: Separation of duties, Least privilege

**Question 27**

Correct

Mark 1.00 out of 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. The C compiler will give you an error and won't compile
- ☐ b. There will always be a runtime error
- ☐ c. Nothing
- ☒ d. Whatever is at A[555] will be overwritten

Your answer is correct.

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

**Question 28**

Correct

Mark 1.00 out of 1.00

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

Select one:

- ☒ a. 443
- ☐ b. 110
- ☐ c. 142
- ☐ d. 80

Your answer is correct.

The correct answer is: 443

**Question 29**

Correct

Mark 1.00 out of 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 perimeter firewall rules to restrict access.
- ☐ b. Implement database hardening by applying vendor guidelines.
- ☒ c. Implement OS hardening by applying GPOs. Hardening is the process of securing a system by reducing its surface of vulnerability. Reducing the surface of vulnerability typically includes removing or disabling unnecessary functions and features, removing or disabling unnecessary user accounts, disabling unnecessary protocols and ports, and disabling unnecessary services. This can be implemented using the native security features of an operating system, such as Group Policy Objects (GPOs).
- ☐ d. Implement IIS hardening by restricting service accounts.

Your answer is correct.

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

**Question 30**

Correct

Mark 1.00 out of  
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. RDP
- ☐ d. SFTP

Your answer is correct.

The correct answer is: RDP

[◀ Download - video buổi học qua Zoom ngày 17/4/2020 \(tuần 3\)](#)[Q&A - C2 ▶](#)[Return to: Chapter 2. Soft... ➡](#)