INFORMATION SECURITY (Trắc nghiệm lt)

# C1

1. What security concept encourages administrators to install firewalls, malware scanners, and an IDS on every host?

1. Khái niệm bảo mật nào khuyến khích quản trị viên cài đặt tường lửa, trình quét phần mềm độc hại và IDS trên mọi máy chủ lưu trữ?

Endpoint security (Bảo mật điểm cuối)

1. Which of the following is a principle of the CIA Triad that means authorized subjects are granted timely and uninterrupted access to objects?

2. Nguyên tắc nào sau đây là nguyên tắc của Bộ ba CIA có nghĩa là các đối tượng được ủy quyền được cấp quyền truy cập kịp thời và không bị gián đoạn vào các đối tượng?

Availability (khả dụng)

1. Which one of the following identifies the primary a purpose of information classification processes?

3. Điều nào sau đây xác định mục đích chính của các quá trình phân loại thông tin?

Define the requirements for protecting sensitive data (Xác định các yêu cầu để bảo vệ dữ liệu nhạy cảm)

(A primary purpose of information classification processes is to identify security classifications for sensitive data and define the requirements to protect sensitive data. Information classification processes will typically include requirements to protect sensitive data at rest (in backups and stored on media), but not requirements for backing up and storing any data. Similarly, information classification processes will typically include requirements to protect sensitive data in transit, but not any data.)

1. Which one of the following data roles is most likely to assign permissions to grant users access to data?

4. Vai trò dữ liệu nào sau đây có nhiều khả năng chỉ định quyền để cấp cho người dùng quyền truy cập vào dữ liệu?

Administrator (Người quản lý)

(The administrator assigns permissions based on the principles of least privilege and need to know. A custodian protects the integrity and security of the data. Owners have ultimate responsibility for the data and ensure that it is classified properly, and owners provide guidance to administrators on who can have access, but owners do not assign permissions. Users simply access the data.)

1. If an organization contracts with outside entities to provide key business functions or services, such as account or technical support, what is the process called that is used to ensure that these entities support sufficient security?

5. Nếu một tổ chức ký hợp đồng với các tổ chức bên ngoài để cung cấp các chức năng hoặc dịch vụ kinh doanh chính, chẳng hạn như hỗ trợ tài khoản hoặc kỹ thuật, thì quy trình được gọi là gì được sử dụng để đảm bảo rằng các tổ chức này hỗ trợ đủ bảo mật?

Third-party governance (Quản trị của bên thứ ba)

1. What ensures that the subject of an activity or event cannot deny that the event occurred?

6. Điều gì đảm bảo rằng chủ thể của một hoạt động hoặc sự kiện không thể phủ nhận rằng sự kiện đó đã xảy ra?

Non repudiation (Không bác bỏ)

(Nonrepudiation ensures that the subject of an activity or event cannot deny that the event occurred.)

1. Which of the following contains the primary goals and objectives of security?

The CIA Triad

1. Which of the following is the weakest element in any security solution?

8. Yếu tố nào sau đây là yếu nhất trong bất kỳ giải pháp bảo mật nào?

Humans

1. Which one of the following would administrators use to connect to a remote server securely for administration?

Secure Shell (SSH)

(SSH is a secure alternative to Telnet because it encrypts data transmitted over a network. In contrast, Telnet transmits data in cleartext. SFTP and SCP are good methods for transmitting sensitive data over a network, but not for administration purposes.)

1. Which networking technology is based on the IEEE 802.3 standard?

Ethernet

1. What is encapsulation? Đóng gói là gì?

Adding a header and footer to data as it moves down the OSI stack

1. Vulnerabilities and risks are evaluated based on their threats against which of the following?

12. Các lỗ hổng và rủi ro được đánh giá dựa trên các mối đe dọa của chúng đối với yếu tố nào sau đây?

One or more of the CIA Triad principles

1. Which of the following is not considered a violation of confidentiality?

13. Nội dung nào sau đây không bị coi là vi phạm bí mật?

Hardware destruction

1. If a security mechanism offers availability, then it offers a high level of assurance that authorized subjects can Access the data, objects, and resources.
2. What type of plan outlines the procedures to follow when a disaster interrupts the normal operations of a business?

15. Loại kế hoạch nào nêu ra các thủ tục cần tuân theo khi rủi ro làm gián đoạn hoạt động bình thường của doanh nghiệp?

Disaster recovery plan (Kế hoạch khắc phục thảm họa)

(Disaster recovery plans pick up where business continuity plans leave off. After a disaster strikes and the business is interrupted, the disaster recovery plan guides response teams in their efforts to quickly restore business operations to normal levels.)

1. What is the first step that individuals responsible for the development of a business continuity plan should perform?

16. Bước đầu tiên mà các cá nhân chịu trách nhiệm phát triển một kế hoạch liên tục trong kinh doanh nên thực hiện là gì?

Business organization analysis Phân tích tổ chức kinh doanh

(The business organization analysis helps the initial planners select appropriate BCP team members and then guides the overall BCP process)

1. When an employee is to be terminate, which of the following should be done?

Disable the employee's network access just as they are informed of the termination

(You should remove or disable the employee's network user account immediately before or at the same time they are informed of their termination.)

1. When seeking to hire new employees, what is the first step?

Create a job description

(The first step in hiring new employees is to create a job description. Without a job description, there is no consensus on what type of individual needs to be found and hired)

1. What security control is directly focused on preventing collusion?

Separation Of duties

(The likelihood that a co-worker will be willing to collaborate on an illegal or abusive scheme is reduced because of the higher risk of detection created by the combination of separation of duties, restricted job responsibilities, and job rotation.)

1. Which of the following is the most important aspect of security?

Physical security

(Physical security is the most important aspect of overall security. Without physical security, none of the other aspects of security are sufficient)

1. Which of the following attacks specifically impact data availability?

DDoS

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

Availability

(Failover refers to the process of reconstructing a system or switching over to other systems when a failure is detected. In the case of a server, the server switches to a redundant server when a fault is detected. This strategy allows service to continue uninterrupted until the primary server can be restored. In the case of a network, this means processing switches to another network path in the event of a network failure in the primary path. This means availability)

1. Which of the following is the BEST reason to provide user awareness and training programs for organizational staff?

To reduce organizational IT risk

(Ideally, a security awareness training program for the entire organization should cover the following areas: Importance of security Responsibilities of people in the organization Policies and procedures Usage policies Account and password-selection criteria Social engineering prevention You can accomplish this training either by using internal staff or by hiring outside trainers. This type of training will significantly reduce the organizational IT risk.)

1. The method to provide end users of IT systems and applications with requirements related to acceptable use, privacy, new threats and trends, and use of social networking is:

Security awareness training.

(Security awareness and training are critical to the success of a security effort. They include explaining policies, procedures, and current threats to both users and management.)

1. 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?

Zero-day exploit

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

Defense in depth

1. The internal audit group discovered that unauthorized users are making unapproved changes to various system configuration settings. This issue occurs when previously authorized users transfer from one department to another and maintain the same credentials. Which of the following controls can be implemented to prevent such unauthorized changes in the future?

Least privilege

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

Security awareness training

(Security awareness and training include explaining policies, procedures, and current threats to both users and management. A security awareness and training program can do much to assist in your efforts to improve and maintain security. Ideally, a security awareness training program for the entire organization should cover the following areas: Importance of security Responsibilities of people in the organization Policies and procedures Usage policies Account and password-selection criteria Social engineering prevention)

1. Matt, a security administrator, wants to ensure that the message he is sending does not get intercepted or modified in transit. This concern relates to which of the following concepts?

Integrity

(Integrity means ensuring that data has not been altered. Hashing and message authentication codes are the most common methods to accomplish this. In addition, ensuring non repudiation via digital signatures supports integrity.)

1. 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).

To allow for business continuity if one provider goes out of business, To eliminate a single point of failure

1. A security administrator has just finished creating a hot site for the company. This implementation relates to which of the following concepts?

Availability

(Simply making sure that the data and systems are available for authorized users is what availability is all about. Data backups, redundant systems, and disaster recovery plans all support availability. And creating a hot site is about providing availability)

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

Availability

(Failover refers to the process of reconstructing a system or switching over to other systems when a failure is detected. In the case of a server, the server switches to a redundant server when a fault is detected. This strategy allows service to continue uninterrupted until the primary server can be restored. In the case of a network, this means processing switches to another network path in the event of a network failure in the primary path. This means availability)

1. 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?

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.)

1. Which of the following is a management control?

Written security policy

(Management control types include risk assessment, planning, systems and Services Acquisition as well as Certification, Accreditation and Security Assessment; and written security policy falls in this category)

1. 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).

Disable unnecessary services, Change default passwords

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

443

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

23

# C2

1. 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).

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

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

39. Việc không xác nhận kích thước của một biến trước khi ghi nó vào bộ nhớ có thể dẫn đến cuộc tấn công ứng dụng nào sau đây?

Buffer overflow

1. 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).

Disable unnecessary services, Change default password

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

Ngăn chặn thực thi dữ liệu là một tính năng trong hầu hết các hệ điều hành nhằm bảo vệ chống lại kiểu tấn công nào?

Buffer overflow

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

Incorrect input

1. 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?

Disable unnecessary services on servers

1. 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?

Code review

1. 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).

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

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

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.)

1. 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?

47. Một quản trị viên bảo mật đang điều tra một vụ vi phạm máy chủ gần đây. Vi phạm xảy ra do một cuộc tấn công zero-day nhằm vào một chương trình người dùng đang chạy trên máy chủ. Quản trị viên nên tìm kiếm thông tin liên quan đến vi phạm trong nhật ký nào sau đây?

Application log

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

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.)

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

Application hardening

1. 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?

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.)

1. 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?

False positive

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

Data is corrupted, The program crashes

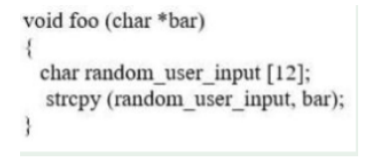
1. Which of the following risk mitigation strategies will allow Ann, a security analyst, to enforce least privilege principles?

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.)

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

Buffer overflow

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

Buffer overflow

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

Anti-virus identifies a benign application as malware.

(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.)

1. 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?

Buffer overflow

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

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.)

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

Load balancing

(Load balancing is a way of providing high availability by splitting the workload across multiple computers)

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

Separation of duties, Least privilege

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

Whatever is at A[555] will be overwritten

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

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).)

1. 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

RDP

# C3

1. A security Operations Center was scanning a subnet for infections and found a contaminated machine. One of the administrators disabled the switch port that the machine was connected to, and informed a local technician of the infection. Which of the following steps did the administrator perform?

Notification, Quarantine

1. Which of the following would be used to allow a subset of traffic from a wireless network to an internal network?

802.1x

1. What is the switch called in an 802.1x configuration?

Authenticator

1. Ann is a member of the Sales group. She needs to collaborate with Joe, a member of the IT group, to edit a file. Currently, the file has the following permissions: Ann: read/write

Sales Group: read

IT Group: no access

If a discretionary access control list is in place for the files owned by Ann, which of the following would be the BEST way to share the file with Joe?

Give Joe the appropriate access to the file directly.

(Joe needs access to only one file. He also needs to 'edit' that file. Editing a file requires Read and Write access to the file. The best way to provide Joe with the minimum required permissions to edit the file would be to give Joe the appropriate access to the file directly.)

1. Connections using point-to-point protocol authenticate using which of the following? (Select TWO).

PAP, CHAP

1. A password history value of three means which of the following?

Three different passwords are used before one can be reused.

(Password History defines the number of unique new passwords a user must use before an old password can be reused.)

1. A customer has provided an email address and password to a website as part of the login process. Which of the following BEST describes the email address?

Identification

1. A system administrator has noticed that users change their password many times to cycle back to the original password when their passwords expire. Which of the following would BEST prevent this behavior?

Enforce a minimum password age policy.

1. Which of the following is the best practice when secure a switch from physical access?

Disable unused ports

1. XYZ company has a database containing personally identifiable information for all its customer. Which of the following options would BEST ensure employee are only viewing information associated to the custom they support>

Access control

1. An incident occurred when an outside attacker was able to gain access to network resources. During the incident response, investigation security logs indicated multiple failed logins attempts for a network administrator. Which of the following controls, if in place could have BEST prevented this successful attack?

Account lockout

1. Jane, the security administrator, sets up a new AP but realizes too many outsiders are able to connect to that AP and gain unauthorized access. Which of the following would be the BEST way to mitigate this issue and still provide coverage where needed? (Select TWO).

Enable MAC filtering, Disable SSID broadcast

1. Which technology will give selective access to the network base upon authentication?

802.1x

1. Users require access to a certain server depending on their job function. Which of the following would be the MOST appropriate strategy for securing the server?

Role based access control Role-based

(Access Control is basically based on a user's job description. When a user is assigned a specific role in an environment, that user's access to objects is granted based on the required tasks of that role.)

1. A penetration tester was able to obtain elevated privileges on a client workstation and multiple servers using the credentials of an employee. Which of the following controls would mitigate these issues? (Select TWO)

Least privilege, Account expiration

1. A company wants to ensure that all credentials for various systems are saved within a central database so that users only have to login once for access to all systems. Which of the following would accomplish this?

Single Sign-On

(Single sign-on means that once a user (or other subject) is authenticated into a realm, re-authentication is not required for access to resources on any realm entity. Single sign-on is able to internally translate and store credentials for the various mechanisms, from the credential used for original authentication.)

1. A company determines a need for additional protection from rogue devices plugging into physical ports around the building. Which of the following provides the highest degree of protection from unauthorized wired network access?

802.1x

1. A user ID and password together provide which of the following?

Authentication

1. After a production outage, which of the following documents contains detailed information on the order in which the system should be restored to service?

Disaster recovery plan

(A disaster recovery plan, or scheme, helps an organization respond effectively when a disaster occurs. Disasters may include system failure, network failure, infrastructure failure, and natural disaster. The primary emphasis of such a plan is reestablishing services and minimizing losses.)

1. A quality assurance analyst is reviewing a new software product foe security, and has complete access to the code and data structures used by the developers. This is an example of which of the following types of testing?

White box

1. Which of the following controls would allow a company to reduce the exposure of sensitive system from unmanaged devices on internal network?

802.1x

1. Internet banking customers currently use an Incorrect account number and password to access their online accounts. The bank wants to improve security on high value transfers by implementing a system which call users back on a mobile phone to authenticate the transaction with voice verification. Which of the following authentication factors are being used by the bank?

Something you are, something you do and something you know

1. A company requires that a user's credentials include providing something they know and something they are in order to gain access to the network. Which of the following types of authentications is being described?

Two-factor

(Two-factor authentication is when two different authentication factors are provided for authentication purposes. In this case, "something they know and something they are".)

1. A process in which the functionality of an application is tested without any knowledge of internal mechanisms of the application is known as:

Black box testing

1. security administrator must implement all requirements in the following corporate policy: Passwords shall be protected against offline password brute force attacks. Passwords shall be protected against online password brute force attacks. Which of the following technical controls must be implemented to enforce the corporate policy? (Select THREE).

Account lockout, Password complexity, Minimum password length

1. The method to provide end users of IT systems and applications with requirements related to acceptable use, privacy, new threats and trends, and use of social networking is:

Security awareness training

1. Which of the following would allow users from outside of an organization to have access to internal resources?

VPN

1. Which of the following is a management control?

Written security policy

(Management control types include risk assessment, planning, systems and Services Acquisition as well as Certification, Accreditation and Security

Assessment; and written security policy falls in this category)

1. Pete, a developer, writes an application. Jane, the security analyst, knows some things about the overall application but does not have all the details. Jane needs to review the software before it is released to production. Which of the following reviews should Jane conduct?

Gray Box Testing

(Gray box testing, also called gray box analysis, is a strategy for software debugging in which the tester has limited knowledge of the internal details of the program.)

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

Preventive

(A preventive access control helps stop an unwanted or unauthorized activity from occurring. Detective controls discover the activity after it has occurred, and corrective controls attempt to reverse any problems caused by the activity. Authoritative isn't a valid type of access control.)

1. During the information gathering stage of a deploying role-base access control model, which of the following information is MOST likely required?

Matrix of job titles with required access privileges

1. At an organization, unauthorized users have been accessing network resources via unused network wall jacks. Which of the following would be used to stop unauthorized access?

Configure port security.

(Port security in IT can mean several things. It can mean the physical control of all connection points, such as RJ-45 wall jacks or device ports, so that no unauthorized users or unauthorized devices can attempt to connect into an open port. This can be accomplished by locking down the wiring closet and server vaults and then disconnecting the workstation run from the patch panel (or punch down block) that leads to a room's wall jack. Any unneeded or unused wall jacks can (and should) be physically disabled in this manner. Another option is to use a smart patch panel that can monitor the MAC address of any device connected to each and every wall port across a building and detect not just when a new device is connected to an empty port, but also when a valid device is disconnected or replaced by an invalid device.)

1. A recent online password audit has identified that stake accounts are at risk to brute force attacks. Which the following controls would best mitigate this risk?

Account lockouts

1. An auditing team has found that passwords do not meet best business practices. Which of the following will MOST increase the security of the passwords? (Select TWO)

Password Complexity, Password Length

1. What is the end device that sends credentials for 802.1x called?

Supplicant

1. RADIUS provides which of the following?

Authentication, Authorization, Accounting

1. A vulnerability scan is reporting

False positive

2. Void foo( char \* bar)

{

Char random\_user\_input [12];

strepy

}

Buffer overflow

3. Directive to reduce the attack surface of a specific host?

Disabling unnecessary services

4. Data execution prevention is the a feature in most operating sytems intended to protect against which type of attack?

Buffer overflow

5. If you declare an array as A[100} in C

Whatever is at A[555] will be overwritten

6. A recent audit had revcealed weakness in the process of deploying new servers and nerwork devices

Disable unnecessary services

Change default password

7. Which of following risk mitigation strategies will allow Ann, a security annalyst, to enforce least privilege principles

User rights reviews

8. A Human Resources user is issued a virtual desktop typically assigned to Accounting employess

Operating System hardening

9. An IT security technician needs to establish host based security for company workstation

Implement OS hardening by applying GPOs

10. Failure to validate the size of a variable before writing it to memory

Buffer overflow

11. Which of the following ports will be used for logging into secure wedsites

443

12. Which of the following describes the process of removing unnecessary accounts and sevices

Application hardening

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

Incorrect input

14. Which of the following ports is used for TELNET by default

23

15. A server administrator notes that a legacy application often stops running due to memory error

Buffer overflow

16. A network security engineer notices unusual traffic on the network form a single IP attemping to access systems on port 23

Disable unnecessary services on servers

17. Entering a random, long string for a program

The program crashes

Data is corrupted

18. Which of the following protocols is the security administrator

RDP

19. Which of the following, if properly implemented,

Separation of duties

Least privilege

20. Which of the following concepts allows an organization to group large number of servers together in order

Clustering

21. One of the system administrators at a company is assigned to maintain a secure computer lad

Least privilege

22. A wed server hosted on the Internet was recently attacked

Zero-day exploit

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

Anti-virus indentifes a begin application as malware

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

Load balancing

25. A security administrator is investigating recent server breach.

Application log

26. Disabling unnecessary services, restricting administrative access,

System hardening

27. A malicious individual is attempting to write too much data to an application’s memory

Buffer overflow

28. Affer an assessment, auditors recommended that an application hosting company

To allow for business continuity if one provider goes out of business

To eliminate a single point of failure

29. Ann, the software security engineer.

Code review