CISSP Exam Review Questions

Domain 1: Information Security and Risk Management

1. A security model called "The State Machine Model" dictates that unless a system is protected in all of its states (Startup, Function, and Shutdown), then the system is not secure. This requirement includes the necessity of responding to security violations/failures in such a way that no further compromises can be successful. This is an example of what security concept?

a. Open Design

b. Closed Design

c. Trusted Recovery

d. Least Privilege

2. OpenSSL was compromised recently by the Heartbleed virus. Certain versions of OpenSSL were vulnerable to attempts to read memory content, which ultimately led to the exposure of private keys of services providers and other protected information. Many security professionals feel that open design is better than closed design. What one consideration is usually necessary to allow an open design to provide greater security?

a. Peer Review

b. Security through obscurity

c. Complexity of design

d. Trusted hierarchy

3. A security concern in an environment that uses private keys is that a user's private key may become corrupted. In order to mitigate the difficulties this corruption would cause, we often select a key recovery agent who is able to backup and recover those keys. However, by granting a single individual the ability to recover the private keys of users, we risk eliminating non- repudiation of actions. Which principle might best be implemented?

a. Separation of duties

b. Principle of least

c. Dual control

d. Need to know

Source Video

Skills Tested: Develop and implement documented security policy, standards, procedures, and guidelines. Additional focus on the need for Need for common baseline level of good practice.

4. In order for a Business Continuity Planning committee to be successful, they must have the support of senior management. The development of a BCP takes time, resources and money. At what phase of the BCP process does Senior Management provide (in writing) its commitment to support, fund and assist with the creation of this plan?

a. Project Initiation

b. Planning

c. Implementation

d. Development

5. A senior manager has requested that you take over the project to develop a business continuity plan. The previous project manager was removed from the project because he was behind schedule and over budget. The manager has asked that you get things back on track as quickly as possible. In reviewing documentation, you determine there no signed BCP policy. What should you do?

a. Begin work immediately and have senior management write a policy once the project is back on track.

b. Before beginning work, obtain a signed policy/charter from senior management.

c. Begin work immediately and use the Business Impact Analysis in lieu of a policy.

d. At this point in time, it is too late to worry about policy. Begin immediately and work towards correcting the course of the project.

6. Some organizations split the Business Impact Analysis and Risk Analysis as two separate processes. In this case, what is the difference between the two?

a. Risk analysis deals with a monetary potential for loss. The Business Impact Analysis provides a more qualitative assessment.

b. Risk analysis is authorized in the policy; the Business Impact Analysis is a function of the project manager.

c. Risk Analysis looks at threats and vulnerabilities, and the Business Impact Analysis looks that the impact the implemented security controls have on the organization.

d. The Business Impact Analysis looks at business processes and prioritizes them based on criticality. Risk Analysis looks at the probability and impact of a threat compromising an asset.

Source Video

Skills Tested: Understand advanced concepts of Disaster Recovery Planning and Business Continuity Planning.

7. Though Senior Management is responsible for ensuring that the BCP is thoroughly tested and

that the tests are reviewed, they are rarely involved in technical details. If senior management specifies that data is to be current within one hour's time, who is responsible for ensuring the technology is in place to achieve those goals?

a. The network administrator

b. The functional manager

c. The BCP committee

d. The salvage team

8. A disaster recovery plan should detail the criteria to be met in order to declare a disaster. Who

can make this decision and declare an organization-wide disaster?

a. Anyone

b. Board of Directors

c. Steering Committee

d. Senior Management

9. The BCP committee should be a cross-functional team that is representative of the departments within the organization. Of the following, what is the most important activity that the BCP team will perform?

a. Restore critical operations in the event of a disaster.

b. Conduct the Business Impact Analysis.

c. Promptly declare that a disaster has occurred and begin implementing phase one of the plan.

d. Create a testing strategy and review the tests for accuracy.

10. Which team is responsible for the restoration of services and operations at the organization's

permanent facility after a disaster has taken place?

a. Recovery Team

b. Salvage Team

c. Continuity Team

d. Senior management

Source Video

Skills Tested: Understand the advanced concepts of Disaster Recovery Planning and Business Continuity Planning and the individual and team roles and responsibilities

11. An organization may likely have employees with physical, or other impairments. In the event of a disaster, these employees may need assistance in getting to safety. Which plan would include detail on how these employees will get to safety?

a. Occupant Emergency Plan

b. Disaster Recovery Plan

c. Continuity of Operations Plan

d. Emergency Notification Plan

12. There are several sub-plans that are part of the overall Business Continuity Plan. These plans serve one of three purposes: Protect, Recover, Sustain. Which function does the Continuity of Operations Plan (COOP) provide?

a. Rescue

b. Recovery

c. Sustain

d. None of the Above

13. The plan that is responsible for describing the steps necessary to restore the most critical business operations in the event of a disaster is which of the following?

a. Disaster Recovery Plan

b. Business Impact Analysis

c. Contingency Plan

d. Business Recovery Plan

Source Video

Skills Tested: Understand the advanced concepts of Disaster Recovery Planning and Business

Continuity Planning specifically regarding the various necessities and corresponding plans necessary for comprehensive recovery and continuity.

14. In the event that a Business Continuity Plan needs to be implemented, its success is highly dependent on the employees' ability to carry out the actions defined in the plan. Which of the following focuses on employee response in the event of a disaster? To whom should the BCP be distributed?

a. All employees

b. Employees with roles specifically assigned in the BCP or DRP processes

c. Senior Management

d. Various sections of the BCP are distributed on a need-to-know basis

15. Because of the dynamic nature of businesses environments today, it is important that the BCP be kept up-to-date and relevant. How often should the BCP be reviewed for necessary changes?

a. Weekly

b. After a major change

c. Once every few years

d. Once per year, or following a major change

16. On Friday afternoon a junior network administrator reported to a team leader that he was concerned that network utilization was escalating slightly as the afternoon progressed, even continuing as users were leaving for the day. Because the increase was small, it was attributed to normal variance. However, on Monday morning, the network utilization was at 99%, and traffic was at a standstill. Though the organization had a contingency plan for a large-scale network outage, the only copy of this plan was located on the intranet server, which was unreachable. Which principle of continuity was not implemented?

a. Elasticity

b. Redundancy

c. Duplicity

d. Reconstitution

Source Video

Skills Tested: Understand the advanced concepts of Disaster Recovery Planning and Business Continuity Planning specifically regarding the next phases including development and review of the plan.

17. There are several types of tests that can be used to verify a recovery plan for accuracy and completeness. Some plans are paper-based, which are less risky to conduct than more intrusive tests. However, to get a true assessment of the completeness of a plan, one may want to surpass paper-based plans and determine if remote operations can be restored at an off-site facility and handle a small portion of business transactions. What type of test would this be?

a. Simulation

b. Full-Interruption

c. Structured Walkthrough

d. Parallel

18. In order to determine and provide procedures to implement controls allowing data transactions to be restored, the BCP committee will need to know how quickly the data must be restored and how current it should be. These metrics should be established in which document?

a. The DRP

b. The COOP

c. The BIA

d. The OEP

19. In the event of a disaster and the company facility is unreachable for a day or longer, some employees are tasked with working from home through VPN access to the corporate site. These details should be specified in what phase of the DRP?

a. Notification

b. Recovery

c. Reconstitution

d. Planning

Source Video

Skills Tested: Understand the advanced concepts of Disaster Recovery Planning and Business Continuity Planning specifically regarding the next phases including development and review of the plan.

Domain 2: Asset Security

1. An attacker gains access to the network with the hope of using a protocol analyzer to capture and view traffic that is unencrypted (also known as sniffing the network.) What is a PROACTIVE way to mitigate this risk with the minimum amount of effort?

a. Implement a policy that forbids the use of packet analyzers/sniffers. Monitor the

network frequently.

b. Scan the network periodically to determine if unauthorized devices are connected. If those devices are detected, disconnect them immediately and provide management a report on the violation

c. Provide security such as disabling ports and mac filtering on the switches to prevent an unauthorized device from connecting to the network. Implement software restriction policies to prevent unauthorized software from being installed on systems.

d. Install anti-spyware software on all systems on the network.

2. Confidentiality is very frequently breached through social engineering attacks. Though training is helpful in reducing the number of attacks, it still does not eliminate the risk. Which of the following would be an administrative policy that is most likely to help mitigate this risk?

a. Formal On-boarding Policies

b. Job Rotation

c. Formal Off-boarding Policies

d. Separation of Duties

3. Classification of resources indicates the value of the resources being protected. Classifications exist in both public and private sectors while still serving the same purpose. What is the purpose of classification?

a. To determine which baseline security controls should be implemented to protect the data

b. To indicate what steps should be taken if the information is compromised

c. To allow users to understand how critical the information is to an organization's existence

d. To indicate the damage done should the information be compromised

Source Video

Skills Tested: Protect Privacy of Data

4. Organizations that allow users to install applications or make other changes to their systems do so for to provide ease of use and greater flexibility. However, users may install inappropriate software or make harmful changes to their systems. Usually a well-documented and enforced policy of configuration/change management would prevent these changes without the review of a change control board through a well-controlled process. Of the answers below, what is the greatest benefit of configuration/change management?

a. To reduce the effort needed for end-users to maintain their systems

b. To provide stability of network systems and resources

c. To generate more paperwork for administrators to complete

d. To prevent any and all changes to a system's baseline images.

5. An emergency situation has required a change to a database server to prevent the loss of a sizeable amount. A lead technician has instructed the administrator to make the change. There was no time to submit a change request, as action had to be taken immediately. What is the next thing the administrator should do immediately?

a. Advise other network administrators to make the same change to all servers as a

proactive measure.

b. Nothing, since a lead technician authorized the change

c. Perform the change and then follow the company's emergency change control

procedure.

d. Ignore the request since change control is not being followed.

6. A vendor has developed the proprietary operating system that runs on 85% of your enterprise's network computers. They have just released a security patch that provides a safeguard for a recently discovered flaw that allows compromise of the operating system leading to the discovery of passwords. What should you do?

a. Test the patch in the lab and roll out the change immediately.

b. Since the patch is security-related and corrects a known vulnerability, push out the patch immediately.

c. Call the vendor to inquire about the specifics of the patch.

d. Review and follow your organization's patch management strategy.

Source Video

Skills Tested: Ensuring appropriate retention, controls and documentation for network systems through configuration management

7. Data can exist in various states. When we refer to data at rest, we are describing data in some form of permanent storage (hard drive, USB drive, DVD, etc.) You have a laptop system, and you are concerned that if it gets stolen, the data would be compromised. What is the best way to protect the data on your laptop?

a. Use a cable lock to protect against theft.

b. Encrypt your data.

c. Install monitoring software to detect changes to your data.

d. Review your audit logs each day.

8. Due to the high sensitivity of information stored on a specific system, there is a need to encrypt the entire hard drive, as opposed to just encrypting the data. This service is provided in Windows with a utility called BitLocker, as well as through 3rd party software by other vendors. This technique allows the key for the encrypted drive to be stored on a particular chip on the motherboard, so that if the drive is stolen it will be rendered inaccessible. What is the name of the chip on which the key will be stored?

a. Clipper Chip

b. L3 Cache

c. Trusted Platform Module

d. SD-ROM

9. Many protocols designed for transmission of data across a network are designed without integrated security. This vulnerability frequently means that credentials and data are transmitted across the network in plaintext and is true of protocols such as FTP, Telnet and the R-login (and other R utilities that UNIX uses to allow remote access.) Which protocol would provide a secure alternative to the above protocols for file transfer and remote access?

a. TFTP

b. SSH

c. SSL

d. TLS

Source Video

Skills Tested: Understanding how to protect data at rest, in process, and in transit

Domain 3 Security Engineering

SECTION 1—Security Architecture and Design

1. Certain components of a system determine the security of that system. The trust of the system is a reflection of the trust of these components. These components are collectively referred to as the _______________ of the system.

a. Ring 1 elements

b. Trusted Computing Base

c. Operating System Kernel

d. Firmware

2. In each instance where a subject attempts to access an object, that access must be authorized. In order to authorize the access, the set of conceptual requirements must be verified by the portion of the operating system kernel that deals with security. The conceptual ruleset is known as the __________, while the enforcement mechanism is referred to as the ____________

a. Access Control List, Security Enforcer

b. Security Enforcer, Access Control List

c. Reference Monitor, Security Kernel

d. Security Kernel, Reference Monitor

3. One of the foundational principles of security is that security controls must be aligned with business objectives. Based on the impact security has upon an organization's success, why is the concept of business alignment important?

a. There is always a tradeoff for security, so an organization has to weigh the cost vs. benefits of the security measures.

b. Security is cheap and easily implemented compared to the potential for loss. Security should be implemented everywhere possible.

c. Security is so important that every organization must implement as much as possible.

d. Security is too costly to implement in small organizations.

Source Video

Skills Tested: Implement and manage engineering processes using secure design principles, including security by design. Focus is on system architecture, trusted Computer Base (TCB), Security Perimeter, Reference Monitor, Security Kernel

4. IPv4 is a protocol that was designed many years ago with the purpose of transmitting data across physically secured lines in a localized environment. Because the threats were very different at this time and because the physical lines were secured, security was not built into the protocol. However, IPv6 was designed to include IPSec to provide confidentiality, integrity, authenticity, and non-repudiation. What is this concept utilized in IPv6 known as?

a. Security through obscurity

b. Principle of least privilege

c. Economy of design

d. Secure by design

5. At one point in time, it was common for organizations to have mainframe computers which were accessed by terminals on the users' workstations. Terminals were the ultimate thin clients. Now as we move towards cloud-based services, we are hearing the term "thin clients" again today more and more. What is the implication of using thin clients?

a. Localized processing so the user has direct access to resources on their system

b. An independent and stand-alone system that is not "weighed down" with connectivity issues

c. A Centralized environment in which software and resources can be installed, updated and managed.

d. Guaranteed access even in the event that the network is down

6. Coupling is an important concept in object-oriented programming, Service Oriented Architecture (SOA), and has other implementations as well. Loose coupling is preferred to high coupling. Why?

a. Loose coupling allows the ability of an application to focus on a single purpose and function.

b. Loose coupling limits the interactions between modules of code and allows them to interact without the necessity of the code, location, protocol of another module.

c. Loose coupling prevents the interaction between modules of code.

d. Coupling allows multiple applications to run in the same allocation of memory.

Source Video

Skills Tested: Implement and manage engineering processes using secure design principles

7. The Bell LaPadula security model was designed in order to protect the confidentiality of secrets for the US government. One of the security properties of the model is designed to prevent someone at a high level from leaking secrets to those who should not have access. This property is called the *_Security Property. Which of the following is indicated by the *_Security Property?

a. No write down

b. No write up

c. No read down

d. No read up

8. The Secure State Model essentially dictates if a system starts securely, operates securely and shuts down securely (even in failure) then it is a secure system. Which phase is the most difficult to secure?

a. Startup

b. Shutdown

c. Failure

d. Operations

9. The Clark-Wilson security model promotes the idea that trusted elements should be separated from untrusted elements. If, for example, an application (untrusted) needs to access memory (trusted) then the untrusted element gets access to an interface, and the interface has access to the application. Which of the following security principles does this enforce?

a. Dual control

b. Separation of duties

c. Open systems

d. Redundancy

Source Video

Skills Tested: Understand the fundamental concepts of security models and their role in secure design

SECTION 2—Assessing and Enforcing the Trustworthiness of Systems

1. There are various responsibilities in relation to safeguarding sensitive information. Who is responsible for the classification of data, as well as determining who should be able to access the data?

a. The Data Owner

b. The Authorizing Official

c. The Data Custodian

d. Senior Management

2. The minimum security baseline of a system references the lowest acceptable security configuration for a system in a specific environment. However, before the MSB can be determined, the system must be categorized based on the Confidentiality, Integrity, and Availability needs for the data. When evaluating a system where the potential impact of unauthorized disclosure is "high," the impact of an integrity breach is medium, and the impact if the data is temporarily unavailable is low, what is the overall categorization of a system?

a. High

b. Medium

c. Low

d. Medium-high

3. In evaluating a system per the TCSEC and the more recent Common Criteria, there are two elements that are assessed as part of the evaluation: Trust and Assurance. Which of the following best describes trust and assurance?

a. Trust describes how secure the system is, while assurance describes performance capabilities.

b. Assurance describes how secure the system is, while trust describes performance capabilities.

c. Trust describes the function of the product, while assurance describes the reliability of the process used to create the product.

d. Assurance describes the function of the product, while trust describes the reliability of the process used to create the product.

Source Videos: One / Two

Skills Tested: Select controls and countermeasures based on systems security evaluation model

4. A user logs in to a system at 8 am but has his credentials suspended at 10 am. A network administrator is surprised to find that this user is still logged on to the network at 2 pm. What type of attack is this?

a. TOC/TOU

b. Privilege Escalation

c. LDAP Injection

d. Exception Event

5. Syn Floods, Buffer overflows, and other resource exhaustion attacks are types of denial of service attacks that operate based on trying to access more resources than are currently available. What is the best defense against an attack of this nature?

a. Input validation

b. Throttling mechanisms

c. limiting the number of resources that an unauthorized user can cause to be expended

d. All of the above

6. An application stores sensitive data in memory that is not secured or has not been properly locked. Ultimately, this data is written to a swap file on disk by the virtual memory manager. The attacker is then able to access the information in the swap file and gain access to information that should have been confidential. What type of security design is being described in this case?

a. TOC/TOU

b. DoS

c. Improper Storage

d. Exception Handling

Source Video

Skills Tested: Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements

SECTION 3—Cryptography

1. The Caesar cipher was used during Caesar's time as a means of transferring information without disclosure. This cipher involved shifting the alphabet three characters. This method performs the substitution. For example, A is always substituted for D, B for E, and so on. What are the easiest means of cracking substitution ciphers?

a. Meet in the Middle Attacks

b. Man in the Middle Attacks

c. Sniffing/Analyzing the network

d. Pattern/Frequency analysis

2. In 1918, Gilbert Vernam created a means of providing mathematically unbreakable encryption by using a one-time pad that served as a key. Obviously, the keypad could only be used once. What technology today is based on the ideas implemented in the Vernam Cipher?

a. Asymmetric Cryptography

b. Digital Signatures that are used to provide authenticity

c. The handshake process used by IPSec and numerous other frameworks

d. Session keys

3. The Enigma machine was used by the Germans during World War II to exchange encrypted messages. It was a rotary-based system which used the rotor configuration as its secrecy mechanism. When the original system was compromised, the Germans added a fourth rotor to exponentially increase the complexity necessary to break the code. This concept is seen in the relationship between ___________.

a. AES and Kerberos

b. DES/3DES

c. RSA and DSA

d. RSA and DSA

Source Video: https://www.cybrary.it/video/part-09-security-services-of-crypto/

Skills Tested: Security services provided by cryptography

4. A user receives an email that they believe to have been sent by a colleague. In actuality, the email was spoofed by an attacker. What security services would have indicated that the message was spoofed?

a. Privacy

b. Authorization

c. Integrity

d. Non-repudiation

5. Two users are exchanging information across an unreliable link. There is frequently interference, and other issues causing packets to be dropped. These individuals need a means to detect that their data has not been corrupted as part of the change. Which security services would detect corruption?

a. Privacy

b. Authenticity

c. Integrity

d. Non-repudiation

6. The reasonable guarantee that someone can't dispute a message, nor the contents of the message are referred to as ________.

a. Privacy

b. Authenticity

c. Integrity

d. Non-repudiation

Source Video:

Skills Tested: Historical uses of cryptography and their influence on today's cryptographic mechanisms

7. Because the user-created passwords rarely provide the necessary security, and because many algorithms still used to protect these passwords have been broken, what should be added to passwords?

a. A keys

b. A certificate

c. An algorithm

d. A salt

8. RC-4 is the algorithm used by WEP and WPA to provide encryption for Wi-Fi networks. RC-4 is a stream cipher. What are a common means of providing encryption in stream algorithms?

a. XOR

b. Blocking

c. Chaining

d. Feedback modes

9. A crypto-variable provides the instructions for utilizing the math functions used to encrypt data. What is another name for this term?

a. Key

b. Algorithm

c. Cipher

d. Initialization Vector

Source Video

Skills Tested: Definitions of cryptographic terms

10. The Rijndael algorithm was designed to replace DES as the de facto standard algorithm for most applications. It is also the result of a government standard required to provide protection for data that is sensitive, but unclassified. What is it more frequently known as?

a. RC-6

b. 3DES

c. AES

d. Kerberos

11. What is the most trusted way to ensure only the intended recipient obtains the key in a purely symmetric system?

a. Manager hand-delivers the key

b. Encrypt the key with the receiver's public key

c. Encrypt the key with a passphrase

d. Encrypt the key with the sender's private key

12. A certain type of symmetric algorithm "chunks" data into blocks and sends each block through a series of math functions based on the key. What type of symmetric cipher is this called?

a. Stream

b. Block

c. Chained

d. Feedback

Source Video

Skills Tested: Symmetric cryptography's limitations and benefits

13. Asymmetric algorithms provide some of the security services that are lacking from asymmetric algorithms. Which security service can an asymmetric algorithm provide that a symmetric algorithm cannot?

a. Privacy

b. Authenticity

c. Integrity

d. Non-Repudiation

14. How do asymmetric algorithms solve the problem of key distribution as seen in symmetric algorithms?

a. Asymmetric encryption requires an out-of-band key exchange.

b. Asymmetric algorithms do not provide encryption for privacy. Therefore no key exchange is needed.

c. Asymmetric algorithms post private keys to a Key Distribution Server.

d. The relationship between public and private keys prevents the need to send a protected key across the network.

15. When using Asymmetric cryptography, what should an administrator do if they become aware of public key compromise?

a. Revoke the private key

b. Revoke the public key

c. Revoke the key pair

d. Do nothing

Source Video

Skills Tested: Asymmetric cryptography's limitations and benefits

16. Symmetric ciphers are known to have the ability to provide comparable encryption several thousands times faster than asymmetric algorithms. Why is this?

a. Symmetric ciphers don't use keys but instead use one-way math.

b. Symmetric ciphers can provide security equivalent to asymmetric ciphers but with much shorter keys.

c. Asymmetric ciphers can provide security equivalent to symmetric ciphers but with much shorter keys

d. Symmetric algorithms are implemented in hardware devices which are much faster than software implementations which asymmetric algorithms use.

17. Though Symmetric algorithms can provide encryption services much quicker than asymmetric ciphers, what is the greatest drawback of using these ciphers?

a. Symmetric ciphers need a longer key in order to provide the same encryption.

b. Symmetric ciphers cannot utilize an initialization vector.

c. Symmetric ciphers require an out-of-band key exchange.

d. Symmetric Ciphers require a public key infrastructure.

18. Alice gives a copy of her private key to the crypto admin, Bob for backup. Which problem below would most likely affect the accountability of the system?

a. Bob could read documents destined for Alice.

b. Bob could sign documents as Alice.

c. Bob could leave the company, and Alice's backup of her key could be unavailable.

d. Bob could update the CRL claiming Alice's key was lost.

Source Video

Skills Tested: Comparison of asymmetric algorithms vs. symmetric algorithms

19. Due to the difficulty of key exchange with symmetric cryptography, key exchange is often performed out-of-band. In the implementation of a digital envelope, the contents of the message are encrypted with a symmetric session key that is included with the message. How is the session key protected?

a. It is encrypted with the sender's public key.

b. It is encrypted with the Sender's private key.

c. It is encrypted with the receiver's public key.

d. It is encrypted with the receiver's private key.

20. When a client connects to a secure web server using the https protocol, what is the response of the server?

a. The server will send the client its private key.

b. The server will send the client its public key.

c. The server will request the private key of the client.

d. The server will request the public key of the client.

21. Often in mail messages, the contents of the message are provided by a symmetric algorithm, likely AES. Non-repudiation, however, is obtained through a combination of hashing and an asymmetric algorithm. How is non-repudiation accomplished?

a. By encrypting the document with the sender's private key, then hashing document

b. By encrypting the document with the sender's public key, then hashing the document

c. By hashing the document and then encrypting the hash with the sender's private key

d. By hashing the document then encrypting the hash with the receiver's public key

Source Video

Skills Tested Understand how asymmetric, and symmetric algorithms work together to provide benefits of each.

22. Diffie-Hellman was the first asymmetric algorithm and was developed in the late 1970's. Which of the following services does the Diffie-Hellman algorithm provide?

a. Privacy

b. Authenticity

c. Key Exchange

d. Key Agreement

23. Handheld devices such as some cell phones and tablets are incapable of providing the processing power necessary to use many of today's secure algorithms. In order to address this problem, an efficient algorithm was developed which provides very good encryption with a minimum of resource usage in specific environments. What is this algorithm?

a. Elliptical Curve Cryptography

b. RSA

c. Diffie-Hellman

d. AES

24. Digital signatures provide non-repudiation through a hash encrypted with a sender's private key. Which asymmetric algorithm is most frequently used to encrypt the hash?

a. AES

b. SHA-1

c. DSA

d. RSA

Source Video

Skills Tested: Understand the function of the Diffie-Hellman, RSA, and ECC algorithms.

25. A fundamental concept of hashing is that hash should not be able to be reversed to reveal the contents of the message or file. What provides this secrecy in a hashing algorithm?

a. A public key

b. A private key

c. One-way math

d. A digital signature

26. In order to ensure integrity, a hashing algorithm creates a unique representation of the data or file that was hashed. This value is called a message digest. In the event that the message or file should change, the hash should change. However, because the possible values for all hashes are finite, there will be a very small likelihood that two different files could produce the same digest. What is this called?

a. Collision

b. Key clustering

c. Chaining

d. Escrow

27. What is a birthday attack?

a. An attack on passwords based on the idea that many users choose bad passwords based on personal information such as birthdays

b. A logic bomb that is triggered on the date of the attacker's birthday

c. An attack that attempts to find collisions in separate messages

d. An attack which focuses on personnel databases in an attempt to compromise personal information for the purpose of identity theft

Source Video

Skills Tested: Understand the functionality and basic concepts of hashing

28. What prevents spoofing during the transmission of a hashed document?

a. Nothing

b. The shared key

c. The private key

d. The public key

29. A digital signature provides non-repudiation, whereas a MAC (Message Authentication Code) only provides reasonable authentication and integrity. What is the reason that a MAC cannot provide non-repudiation?

a. It doesn't include a hash or integrity check value.

b. MACs use asymmetric encryption.

c. MACs use symmetric encryption.

d. There is nothing unique to the sender and/or receiver in a MAC.

30. Which key is used to produce a digital signature and which key is used to verify a digital signature?

a. Sender's public creates, sender's private verifies

b. Sender's private creates, sender's public verifies

c. Sender's public creates, receiver's private verifies

d. Receiver's public creates, receiver's private verifies

Source Video

Skills Tested: Determine the distinctions between hashes, MACs, and Digital Signatures

31. In order to initiate a secure connection with a web server, the client uses the https protocol.When the server receives the request for a secure connection, it sends a certificate to the client. Which of the following information would not be on a server's certificate?

a. Public Key

b. Private Key

c. Signature of a Certification Authority

d. Class

32. When a user gets a message stating that the server to which they are connecting has a certificate that has not been signed by a trusted certificate authority. What does this mean?

a. The web server has not been issued a certificate.

b. The Certificate Authority who issued the server's certificate is not registered with IANA.

c. The Certificate Authority, who issued the server's certificate does not have its certificate installed on the server.

d. The Certificate Authority, who issued the server's certificate does not have its certificate

installed on the client computer.

33. When a client receives a certificate as a means of authenticating a server, the client will check to ensure that the certificate has not expired. The client also needs to verify that the certificate has not been revoked. How is this information obtained?

a. The client locates this information on the certificate.

b. The next step of the SSL/TLS handshake requires the server to provide proof of revocation status.

c. The client queries an OCSP (Online Certificate Status Protocol)server.

d. The client verifies this information with their ISP (Internet Service Provider.)

Source Video

Skills tested: Understand the purpose and function of elements within a public key infrastructure.

34. In relation to IPSec and other protocols, encapsulation is often confused with encryption. Out of the below choices, which best describes the difference between the two?

a. Encapsulation provides privacy; Encryption adds headers to an existing protocol packet.

b. Encryption provides privacy; Encapsulation adds headers to an existing protocol packet.

c. Encapsulation is only used by tunneling protocols; encryption is used universally.

d. Encapsulation is used for transporting data; encryption is used for protecting data's confidentiality.

35. Which mode of IPSec encapsulates the entire IP packet?

a. AH

b. ESP

c. Tunnel

d. Transport

36. Which mode of IPSec would be used for a site-to-site VPN connection (For example, from one VPN concentrator to another?)

a. AH

b. ESP

c. Tunnel

d. Transport

Source Video

Skills Tested: Encapsulation options with IPSec

37. AH and ESP provide the security services most people have come to associate with IPSec. However, another sub-protocol of IPSec, called IKE (Internet Key Exchange.) is concerned with managing the handshake process and negotiating keys. What asymmetric algorithm does IKE use for key agreement?

a. Diffie-Hellman

b. Knapsack

c. DSA

d. RSA

38. A user needs to provide protected IP communications across his local network. He needs encryption, as well as authentication and integrity. Which sub-protocol of IPSec offers encryption?

a. AH

b. ESP

c. SKIP

d. IKE

39. AH (Authentication Header) is a sub-protocol that provides non-repudiation. AH runs an ICV (Integrity Check Verification) on the entire packet (header, data, and trailer.) Because the Integrity check is run on the entire IP packet, including the header, AH guarantees that no portion of the pack has been modified. As helpful as this is, there is a network service whose primary function is to modify the headers of packets before they leave the local network. What is this service?

a. NAT

b. TCP

c. DNS

d. LDAP

Source Video

Skills Tested: IPSec sub-protocols, handshake, and Security Associations

40. An organization is considering designing a facility for a newly acquired business unit. They want to make sure that the site is designed to be as secure as possible, with the intent of adding additional security if needed. Which of the following would NOT be an element of secure building design for organizations that have medium level security needs?

a. Ensure that the building is obscured from view, so as to not attract attention.

b. Ensure the building is in a prominent location, as opposed to being less visible.

c. Ensure that plants and shrubbery are planted underneath windows.

d. Plan secure design strategies in a layered method of defense.

41. An organization has invested a sizeable amount of money in provided badged access to their secured data center. However, upon observation, numerous employees are allowing individuals without badges to "piggyback" into the facility. What should an employee do when someone without a badge attempts to gain access to the building on someone else's card swipe?

a. Explain to the individual that you cannot allow the individual to enter the building without using their badge.

b. Allow them to enter, as long as you recognize them as an employee.

c. Allow them to enter, but notify security at your earliest convenience.

d. Escort that individual to security, even if you recognize them as an employee.

42. Your organization has decided to implement a Wi-Fi network for internal employees. You have been asked to perform a site survey of your current facility and recommend the best location for the access points, with the primary consideration of preventing access outside the building. As a general rule, what are the main considerations when deciding where to put Access Points in your facility?

a. The Access points should be in the corners of the building to provide the best-unobscured access signal.

b. Access points need to be placed in the locked server room at all times.

c. Access points should be located in areas of public access to ensure guests have easy access.

d. Access points should be placed in the center of the building.

Source Video

Skills Tested: Apply secure principles to site and facility design

43. Prosecuting computer crime can be very difficult, even if numerous technical controls are in place. One of the greatest difficulties requires the placement of an individual at the source of the crime. For internal employees, we use digital signatures and smart cards to link actions to individuals. However, this is not fail-proof, as an employee determined to commit fraud can simply say that their card or key was compromised. Another cause for reasonable doubt is that while the employee may acknowledge the attack originated from their computer, but deny they were the one responsible. The employee can make the case that they occasionally forget to log out of their systems, or remove their smart cards. At that time anyone could've accessed the system and initiated the attack. Which physical security mechanism could help prove no one else accessed the employee computer?

a. Door locks to the data center

b. Badged access to the building

c. Closed Circuit TV cameras

d. A policy that dictates all systems must be locked and smart cards must be removed anytime the system is unmanned.

44. Doors provide an important barrier to sensitive areas within a building. Which of the following provides the least protection from an intruder gaining access by compromising a door to the area?

a. Pick-resistant locks

b. A kick plate

c. Enforced and protected hinges

d. Strike-plate

45. To provide protection to employees and to preserve human life, positive pressurization should be provided by a company's HVAC system. What does positive pressurization mean?

a. Air flows into a room, instead of outside the room.

b. Air flows out of a room rather than in.

c. The HVAC system starts up automatically if it detects a change in air pressure.

d. The HVAC system shuts down immediately in the event of fire to limit smoke spreading from room to room.

Source Video

Skills Tested: Design and implement physical security

Domain 4 Telecommunications and Network Security

1. When discussing a connectivity issue between two networked systems, the technician tells you that he suspects a Layer 1 issue has caused the lack of communication between hosts. What would be best described as a "Layer1" issue?

a. Cable

b. Router

c. Switch

d. NIC

2. In choosing cable in a highly secure environment, which type is resistant to eavesdropping and immune to EMI (Electromagnetic Interference) and RFI (Radio Frequency Interference?)

a. Thick Coaxial Cable

b. Thin Coaxial Cable

c. Fiber Optic Cable

d. Shielded Twisted Pair

3. Most devices that function at the lower Layers of the OSI have less "intelligence" than devices at other Layers. By this, it is meant that they do nothing to direct, address, or correct packets on the network. However, lower Layer devices usually have which of the following benefits over upper Layer devices?

a. Lower layer devices provide better inspection of traffic.

b. Lower layer devices are better able to encapsulate data, so it is better able to traverse the physical network.

c. Lower layer devices are usually faster than their upper layer counterparts.

d. Lower Layer devices are easier to monitor and provide greater insight into network activity, as they are less complex.

Source Video

Skills Tested: Understanding the OSI Reference models with a focus on Layer1, the physical layer.

4. The Data Link Layer is the only sublayer of the OSI Model that has two sublayers. One of the sublayers is the MAC (Media Access Control) sublayer. Media Access Control provides a means for determining which system or systems can have access to the media and be allowed to transmit at any given time. Ethernet uses a method called CSMA/CD (Carrier Sense Multiple Access with Collision Detection.) What does this imply?

a. Ethernet environments avoid collisions by detecting their likelihood before transmitting.

b. Ethernet environments only allow an individual host to access the cable at any given time and are capable of detecting collisions as they happen.

c. Even though Ethernet traffic is prone to collisions, a hub can all but eliminate them.

d. Though multiple systems can access the media simultaneously, the result will be a collision, which should be immediately detected.

5. MAC (Media Access Control) addresses are physical hardware addresses assigned to each network interface for each host on the network. Though IP addressing is used to locate hosts from anywhere in the world, MAC addresses must be used locally. How does resolution occur from an IP address to a MAC address?

a. The host queries through DNS lookup.

b. The MAC addresses are published in the Global Catalog Server.

c. The hosts use an ARP broadcast to learn the MAC address of the destination.

d. Clients broadcast their MAC addresses every 30 seconds.

6. Wi-Fi networks have no collisions, as they follow the Media Access Method of CSMA/CA. How does this method eliminate collisions?

a. CSMA/CA uses a control frame to traverse the network. Systems are wishing to communicate capture the frame. Since there is only one frame and a host can't communicate without the frame, there are no collisions.

b. Though technically there are still a small number of data collisions with CSMA/CA, drastically reduces their number by assessing the likelihood of a collision before transmission.

c. In CSMA/CA a host signals its intent to transmit, rather than sending its data immediately.

d. In CSMA/CA collisions are avoided by utilizing hardware, like switches, to isolate the network into collision domains.

Source Video

Skills Tested: Understanding the OSI Reference models with a focus on Layer2, the data link layer. Understanding media access control

7. Switches have replaced hubs in most standard environments years ago. Switches are better at directing traffic and are also more secure. However, there is an attack called MAC flooding that essentially causes a switch to fall back to the functionality of a hub. This is caused by overwhelming a switch's CAM table with bogus MAC addresses. What is the greatest security concern with a switch that reverts back to the functionality of a hub?

a. Traffic will be slower, and performance will be degraded.

b. All traffic will be forwarded out all ports and will likely give an attacker access to a greater amount of data than the specific port to which he or she is connected.

c. Because hubs work at Layer 1, they will be unable to use MAC addresses to direct traffic.

d. Network collisions will increase.

8. A user complains that connectivity to the network is slow. This network is rarely used, and its hardware is quite dated. You notice that the NIC on the user's system is an amber color, instead of green. As a general rule, this indicates collision on the network. What would be the best way of mitigating this problem?

a. Change your media access method to CSMA/CA.

b. Implement a switch.

c. Implement a hub.

d. Implement a router.

9. In earlier times, when an attacker plugged a sniffer into a port on a hub, the attacker had access to all data on that hub. Now that switches have replaced hubs, what traffic will an attacker "see" when connected to a port on a switch?

a. ARP broadcasts

b. Absolutely none

c. Only traffic passing through that particular switch

d. All non-encrypted traffic

Source Video

Skills Tested: Understanding the role switches play on a network, as well as the vulnerabilities they can introduce.

10. Though many certification tests and assessments place network devices and protocols in single Layers of the OSI Model. In reality, most devices and protocols function across multiple Layers, as they satisfy requirements across these Layers. For example, many people consider routers to be Layer 3 devices, but across which layers does a router actually work?

a. 2-5

b. 3-7

c. 1-3

d. 3-4

11. Natively, switches provide collision domain isolation a network, basically improving performance by (almost) eliminating collisions. However, most production switches offer VLAN (Virtual LAN) capabilities. What primary function does a VLAN provide on a switch?

a. Routing

b. Broadcast isolation

c. Connectivity to a WAN switch

d. The ability to connect multiple media types

12. Most Layer2 and Layer3 switches are capable of supporting VLANs. What would be the purpose, then, of using a Layer3 switch?

a. A Layer 3 switch is faster than a Layer2 switch.

b. A Layer 3 switch is cheaper than a Layer2 switch.

c. A Layer 3 switch can allow inter-VLAN communication.

d. A Layer 3 switch inspects traffic based on content.

Source Video

Skills Tested: Understanding routers, VLANs and Layer 3 switches

13. Upper Layer protocols rely upon Layer four protocols for end-to-end connection. Two main Layer4 protocols are TCP and UDP. TCP provides guaranteed, connection-oriented services. UDP provides unreliable, connectionless services, with the benefit of faster speed. What service might be best suited for UDP instead of TCP?

a. Media Streaming

b. Small File downloads

c. Web traffic

d. Email exchange

14. In examining a TCP vs. a UDP packet, you notice that the TCP packet has fields that are not present in the UDP packet. Which of the following fields would appear on both the TCP and the UDP packet?

a. Syn

b. Ack

c. Window-size

d. Port number

15. There are two separate protocols that are frequently used for file transfer: FTP and TFTP. FTP requires connection-oriented delivery, while TFTP uses connectionless delivery for faster performance. What provides the difference in the delivery?

a. FTP uses UDP, while TFTP uses TCP.

b. FTP uses TCP, while TFTP uses UDP.

c. The SYN numbers on the FTP packet guarantee the delivery

d. FTP uses IP for connection-oriented delivery.

Source Video

Skills Tested: OSI Model Layer4, focus on TCP and UDP, Layer4 exploits

16. Only one Layer of the OSI Model has no protocols associated with it. Although the standards and formatting for multimedia files such as JPEG, GIFs, MP4s and other multimedia types are handled at this layer, there are no specific protocols. At which Layer of the OSI model is this true?

a. Application Layer (7)

b. Presentation Layer (6)

c. Session Layer (5)

d. Transport (4)

17. Which of the following attacks occur at Layer 5 of the OSI Reference Model?

a. Syn Flood

b. Smurf Attack

c. Fraggle attack

d. Session Hijack

18. Many websites today use SSL to protect login pages, but use the standard, unencrypted HTTP protocol once the client has been authenticated. An attack called sidejacking takes advantage of this vulnerability. How can sidejacking be mitigated by the web server?

a. Multi-factor authentication should be required.

b. Mutual authentication should be required.

c. The server should use certificates for authentication.

d. The server should use https:// for all pages that it provides.

Source Video

Skills Tested: Understanding Layers 5 and 6 of the OSI Reference Model

19. A network administrator has been told that employee performance has decreased in the last few months and management is convinced part of the reason for this decrease is that people are spending more and more time browsing websites that are not necessary for work. What device is needed to block websites that provide gaming services?

a. An application proxy

b. screening router

c. A stateful firewall

d. IDS

20. A junior network administrator has recommended that an application proxy should be the first line of defense for traffic coming into the organization's LAN from the internet. How should you respond?

a. You should agree. Deep packet inspection is necessary to provide the greatest degree of security.

b. You should disagree. Application proxies are too slow to be the first line of defense and may be better suited elsewhere.

c. You should agree. Application proxies provide thorough inspection very quickly and at lower costs.

d. You should disagree. Application proxies are too expensive to be used on most networks, and the stated requirements can be accomplished at Layer 3.

21. Viruses on the network are increasing at an alarming rate. Management suspects that users are downloading files from untrusted websites. Also, of concern is that even legitimate websites that users must access could become compromised. You want to ensure that only trusted content is downloaded. Which of the following rules is most likely to provide the necessary protection, without affecting necessary business activity?

a. Block all downloads from the internet.

b. Configure a rule that does deep packet inspection of outgoing traffic.

c. Configure a rule that prohibits all downloads, except those files that are digitally signed.

d. Educate users and remind them of corporate policy regarding file downloads.

Source Video

Skills Tested: Understanding Application (7) Layer protocols and services.

22. An organization has been hesitant to spend additional money to upgrade its existing infrastructure. However, with ever-increasing threats, they've decided to ask your advice. They're considering upgrading their existing wireless equipment which they purchased many years ago. These devices were purchased as soon as the 802.11g standard was released. What benefit would be gained by moving to 802.11n or 802.11ac?

a. The later devices are backward compatible with all 802.11 standards.

b. The newer standards have a shorter range capability natively, so they would be less resistant to war-driving.

c. The 802.11g devices most likely only support WEP or WPA. The newer devices support WPA II.

d. The 802.11g devices use AES for encryption, while the 802.11n or 802.11ac devices use RC-4.

23. When configuring a client system to use WPA II, you are then asked to choose “Personal” or “Enterprise.” Choosing WPA II selects how the data will be encrypted, while “Personal” or “Enterprise” sets the framework for authentication. What type of authentication would “Enterprise” mode support?

a. RADIUS

b. Challenge-Response

c. Kerberos

d. LDAP

24. WEP can be broken in a mere matter of seconds with today’s technology. Even when it was first implemented, it was known that WEP did not provide a high degree of security. After WEP, WPA was introduced as a “quick fix.” Even though it didn’t solve many of the existing problems, it offered a slight improvement in the length of the initialization vector and key exchange process. However, it wasn’t until WPA II that we saw a significant improvement. What was the major improvement from WEP/WPA to WPA II?

a. Better performance with WPA II

b. Self-synchronization with WPA II

c. A stronger encryption algorithm with WPA II

d. WPA II uses symmetric encryption whereas WEP/WPA II used asymmetric encryption.

Source Video

Skills Tests: Wireless standards, encryption, and authentication

25. As you are considering migrating resources to the cloud, you want to ensure the Cloud Service Provider has the ability to provision and de-provision resources in an autonomic manner, such that at each point in time the available resources match the current demand as closely as possible. This technique is referred to as:

a. Scalability

b. Elasticity

c. Availability

d. Reliability

26. An organization has historically outsourced the management of its IT resources to another company for service management and maintenance. They are now considering moving to a cloud-based solution and would like to ensure that the network components, such as routers, switches, and storage components are all handled by the cloud provider. Which type of cloud framework is this?

a. IaaS

b. Paas

c. SaaS

d. DRaaS

27. A medical organization has decided that in order to maintain compliance with HIPAA, they would need to update their environment. Specifically, in order to be in compliance, they would need to upgrade their storage devices and increase their security controls to provide the necessary security to protect their patients' information. Additionally, they do not want to take on any more administrative duties. Among other options, they are considering storing their data in the cloud. Which deployment would likely satisfy their needs in the most cost-effective manner?

a. Private cloud

b. Public cloud

c. Hybrid cloud

d. Community cloud

Source Video

Skills tested: Understanding of the different cloud benefits, infrastructures, and frameworks

28. The TCP handshake is a three-way process that allows the hosts to establish a connection. The 3-way handshake consists of SYN, SYN-ACK, ACK. When a malicious host sends numerous SYN packets to the recipient (called a SYN Flood), what happens on the recipient?

a. The recipient sends a TCP reset to avoid a DoS (Denial of Service) Attack.

b. As each SYN packet is received, the recipient opens space in memory to process the data indicated by the SYN packet.

c. The client returns an ACK packet to indicate that the SYNs are received. If there are enough SYN packets, and return ACK packets the network performance will be degraded.

d. The recipient will close the port from which the incoming packets are coming as a means of self-protection.

29. An older attack called a Smurf attack is a Layer 3 DoS (Denial of Service) using ICMP directed broadcasts from a spoofed source address. Later, an attack that was very similar called a Fraggle attack, became successful as a DoS. Instead of using ICMP, however, the Fraggle attack used UDP packets. Which of the following is true regarding defense against these attacks?

a. Since Fraggle attacks use UDP, they generate many false negatives for Intrusion Detection Systems.

b. Since Smurfs use ICMP, they are harder to detect than Fraggle attacks. Most Layer3 firewalls can't examine ICMP packets.

c. Smurf attacks are more likely to be successful than Fraggles because ICMP shouldn't be blocked by the firewall. Otherwise, troubleshooting utilities like PING and Trace Route will not work.

d. Fraggle attacks are more likely to be successful than Smurf attacks because blocking UDP at the firewall is not practical, as it would prevent many other services from running.

30. A means of redirecting hosts to rogue devices on a network is frequently done through modifying information in the cache memory of a system. When a client system is compromised in such a way that its table that maps IP addresses to MAC addresses is modified, what type of attack is being used?

a. DNS Pollution

b. ARP Poisoning

c. IP Redirection

d. ARP flood

Source Video

Skills Tested: Network-based attacks and protocol exploits

31. When a client sends a recursive query to a DNS server, that DNS server looks to other name resolution servers to help resolve the query. Each time the DNS server learns something from other naming servers, it adds that information to its cache. However, if there were rogue DNS servers responding, that information may be compromised. What security mechanism can DNS servers use to get a reasonable assurance that the servers they are querying are legitimate and authorized servers?

a. Configure the "Secure Cache from Poisoning" option in DNS properties.

b. Use DNSSec

c. Use IPSec for authentication

d. Disable recursion

32. In a security awareness training class, the trainer mentioned the term "rootkit" and explained that this was a type of malware that can be difficult to detect and to eradicate from a system, as it installs itself at the same layer as the operating system kernel. If you detect a rootkit on your system, what steps should be taken to remove it with the least effort?

a. Restore your data from backup.

b. Fully restore your system from backup.

c. Format the system, restore operating system from backup then restore the data from backup.

d. Format the system, re-install the operating system from original media, and then restore data from backup.

33. Even though performance was typical and there was no indication of any problems on Friday afternoon, on Monday morning, network utilization was at 98%. What type of malware has most likely caused this severe degradation of network availability?

a. Virus

b. Worm

c. Logic Bomb

d. Teardrop

Source Video

Skills Tested: Understanding mitigating techniques for common network attacks

34. A packet-filtering firewall can make decisions on which of the following type of information?

a. IP address, port number, and protocol

b. Hostnames, usernames, and content

c. IP addresses, content, signature files,

d. Context of protocols and session information

35. NAT devices provide the ability to hide an organization's internal IP addresses from the untrusted entities on the internet. The NAT device intercepts the outgoing packet, strips its true source address, and replaces that address with the IP address of the external interface of the NAT device. Based on how NAT operates, it is incompatible with a particular sub-protocol of IPSec. With which sub-protocol is NAT incompatible?

a. IKE

b. ISAKMP

c. AH

d. ESP

36. A security administrator wants to monitor his internal users and determine which sites they visit. He also wants to restrict certain users' access to particular sites after 5 pm and to ensure that users do not have access to pages with violent content. Which type of firewall should he implement?

a. Dynamic

b. Stateful

c. Application Proxy

d. Circuit level Proxy

Source Video

Skills Tested: Understand the different types of firewalls and NAT devices and their capabilities.

37. Many older types of WAN connections utilized circuit-switching technology that provided access to the phone provider's networks. With circuit switching, packets follow the same path all the way from source to destination. However, many more modern WAN technologies divide traffic into "chunks," and each "chunk" finds its own best path to the destination, with the idea that the fastest path at the beginning of the communication is not necessarily the fastest path later. What is the technology called?

a. Frame routing

b. Packet Switching

c. Block sourcing

d. Directional forwarding

38. Though analog and digital are two different signaling types, we've always wanted have these two disparate signals use the same cable. In the past, we've used modems to convert the digital signal from our computers to analog, in order to allow computers to communicate across analog phone lines. Now that phone lines are digital, we want the analog voice to run across digital lines (VOIP, or IP Telephony.) What is the greatest security threat on a VOIP network?

a. Smurf attacks

b. Toll Fraud

c. Spam

d. Eavesdropping

39. In organizations that have a large amount of VOIP traffic, QoS (Quality of Service) is very important. VOIP traffic can place high demands on available bandwidth. Which of the following WAN technologies provides QoS and prioritization for data packets?

a. Frame Relay

b. FIOS

c. MPLS

d. DSL

Source Video

Skills tested: Understand the basic concepts behind WAN connectivity

Domain 5 Identity and Access Management

1. In the realm of security, most people first think of malicious threats to their systems. However, when we consider the three tenets of security: Confidentiality, Integrity, and Availability, we realize that environmental issues could render a system unavailable quite easily. Which of the following would help control the environment in which servers are stored?

a. Hot/Cold aisles

b. Drop ceilings

c. High humidity

d. High temperature

2. Just as in logical security, an important idea in the world of physical security is security by design. CPTED (Crime Prevention through Environmental Design) presents four concepts that help an organization secure their facility by choosing secure materials and environmental surroundings to secure a physical building. Which of the following would be an aspect of CPTED?

a. Using surveillance cameras to detect threats

b. Implementing fencing and lighting

c. Planting bushes underneath windows

d. Security through obscurity

3. Physical security must be both proactive and reactive. It important to deter and prevent intruders, but we know that determined intruders can circumvent any system if they have the resources. In that instance, detective and corrective controls help us recover from a successful breach. Which of the following is a detective control?

a. Fence

b. Burglar alarm

c. “Beware of Dog” sign

d. Lighting

Source Video

Skills Tested: Control physical and logical access to assets

4. The decision to use simple password-based authentication can expose an organization to numerous threats. Users write down passwords, reuse then, and unfortunately share them with others. Which of the following would allow and administrator to enforce passwords of a certain complexity and lifespan?

a. Access control lists

b. Group policy

c. Firewall rules

d. Password policies

5. Often in applications that allow a password reset function, cognitive passwords are used to get a reasonable verification of a user's identity. Which of the following would be considered a cognitive password?

a. P@$$w0rd

b. Mother's maiden name c

c. Last four digits of a credit card

d. Account number

6. Often social engineers find it infinitely easier to trick someone into giving away their password than to crack that password. However, in the event that social engineering does not work, there are technical tools that are very successful. Which of the following revolutionized the speed with which a password can be broken?

a. Brute force attacks

b. Hybrid attacks

c. Rainbow tables

d. Dictionary attacks

Source Video Skills Tested: Understand the IAAA of Access control and Type I authentication techniques.

7. Type II authentication is based on something a user has. What the user has can be a physical or technical possession. Which of the following is a technical Type II means of authentication?

a. Public key

b. Password

c. Cookie

d. Thumbprint

8. The only mathematically unbreakable form of cryptography is called the Vernam cipher created by Gilbert Vernam in the early 1900's. One time keys and passwords are very valuable because they drastically reduce an attacker's chance of reusing passwords or keys. However, asking users to change their passwords each time they log in would not be received well. How can one-time passwords be implemented in today's environments?

a. Using group policy, configure the system to assign a random password to the user for each login.

b. Provide users with token devices that display a different set of characters every sixty seconds.

c. Implement the use of certificates within your organization.

d. Use Smart cards for login.

9. Though there are many ways that users authenticate today, multi-factor authentication provides the strongest form of authentication. Which of the following environments implements multi- factor authentication?

a. A user is required to log in with a smart card.

b. A user is required to show both a passport and a driver's license.

c. A user is required to log in with a password and a thumbprint

d. A user is required to provide both and iris scan and a retina scan.

Video Source

Skills Tested: Understand the various kinds of Type II Authentication

10. An organization has asked for your consulting services in order to help them implement a biometric system for authentication prior to being allowed to access to data. What should you recommend as the strongest form of authentication?

a. Iris scanning system

b. Retina scanning system

c. Thumbprint and password

d. Palm scanning system

11. An organization wants to implement a biometric system but doesn't know enough to make a good decision. What is of least concern when choosing a biometric system to implement?

a. Cost

b. User acceptance

c. Technology type

d. Accuracy

12. In configuring the settings on a fingerprint reader, you've determined that protecting your network from intruders is your first priority. Therefore you want to ensure that you have an extremely low likelihood of an illegitimate user to gain access. What should you configure?

a. Low FAR (False Acceptance Rate)

b. Low FRR (False Rejection Rate)

c. High FAR

d. High FRR

Source Video Skills Tested:

Understand the specifics of type III authentications

13. One of the many benefits of using Kerberos for network authentication is that the users' passwords don't traverse the network during the authentication process. Without sending the password to the authentication server, how does the client prove the correct password was entered?

a. The client sends its digitally signed certificate to the authentication server.

b. The client's password is verified locally, and the verification information is sent to the authentication server.

c. The server challenges the client by encrypting a ticket with the user's password. If the password was entered correctly, the client is able to decrypt the ticket.

d. The client sends a challenge to the server. The server responds to the challenge with a session key that can only be decrypted with the client's private key.

14. Kerberos is a ticket-based authentication protocol that many network operating systems use.

The client is granted a TGT (Ticket Granting Ticket,) if it authenticates properly. Next, the client requests a ticket from the TGS (Ticket Granting Service.) What is the most important information contained on a ticket?

a. Two copies of the exact same session key

b. The digital signature of a trusted authority

c. A single session key

d. An authentication token for access to a system

15. When a user logs on to a Windows environment, they receive an authentication token. What information is included in an authentication token?

a. The user's digital certificate

b. The user's list of accessible hosts

c. The user's access control lists

d. The user's group memberships

Source Video

Skills Tested: Understand the concepts of Kerberos and SSO (Single Sign On)

16. A member of the Human Resources team frequently assists with payroll. She is granted full access to all payroll information during the workday. However, after 5 pm she is restricted and has no access at all. What type of access control is this?

a. Content-based control

b. Context-based control

c. Constrained interface

d. Access control list

17. A senior network administrator creates a "toolbox" of technical tools for his junior trainee.

These tools can be used to administer the network. The senior admin has limited the toolbox to only those utilities he wants the junior admin to have access to. This is an example of what type of restriction?

a. Content-based

b. Context-based

c. Constrained interface

d. Access control list

18. Which of the following is the most basic type of firewall that is still capable of using rule-based access control?

a. Circuit Proxy

b. Proxy server

c. Packet filtering firewall

d. Web application firewall

Source Video

Skills Tested: Different ways to control access to network resources

19. The IEEE (Institute of Electrical and Electronics Engineers) specifies the 802.1x standards as EAPoL (Extensible Authentication Protocol over LAN) as having three elements. What are those three elements?

a. Client, network access server, authentication server

b. Supplicant, authenticator, authenticating server

c. Applicant, supplicant, authenticator

d. Client, Authenticator, LDAP server

20. RADIUS offers centralized authentication for access to a network. A benefit of having centralized access is greater consistency, and ease of administration. However, some environments work better in a decentralized environment. Which of the following is a benefit of decentralized access?

a. Security

b. Easier distribution

c. Granularity

d. Scalability

21. PAP (Password Authentication Protocol) is an obsolete protocol that provided password-based authentication but sent the password across the network in plaintext. PAP was replaced by CHAP (Challenge Handshake Authentication Protocol.) Which of the following is the benefit of CHAP?

a. CHAP offers better performance.

b. The password is encrypted as it travels the network.

c. CHAP can support smart cards and other means of authentication.

d. The password never travels the network

Source Video

Skills Tested: Understand the significance and function of authentication protocols and central authentication servers

22. An organization that processes highly confidential information is concerned about data leakage from their laptop systems. In order to prevent this leakage of information, what should you do?

a. Encase the systems in heavy metal to absorb the signal.

b. Ensure the laptops are not using CRTs.

c. Unplug the laptops when not in use.

d. Ensure no one is within 30 feet, as that is the limit for data emanations.

23. TEMPEST was a government study from the 1950's designed to analyze emanations from

devices and to subsequently prevent eavesdroppers and attackers from gaining information from this type of analysis. As a result of this study, several suggestions were made for preventing sensitive information from being leaked. Which of the following is NOT recommended as part of TEMPEST

a. Data encryption

b. Control zones

c. White noise

d. Faraday cages

Video Source

Skills Tested: Understand the threats associated with data emanations

24.. As identity management continues to become more complex, and as users need access to more systems, IdaaS (Identity as a Service) is becoming increasingly popular. Which of the following is NOT a benefit from managing identity solutions in the cloud?

a. IdaaS allows users to have fewer usernames and passwords for users to remember

b. Identity service providers are required to be in compliance with government standards, so there is the assurance that information is protected.

c. IdaaS provides centralized management of usernames and passwords.

d. IdaaS makes it easy to remove the credential of a user when he leaves the organization.

25. Typically, with IDaaS (Identity as a Service,) where is the LDAP/Active Directory database most likely to be stored? Choose the best answer from below.

a. On the clients' computers

b. On each server to be accessed

c. On the organization's internal network

d. In the cloud

26.. Which of the following is an XML-based, open standard data format for exchanging authentication and authorization data between an identity provider and a service provider?

a. SPML

b. XML

c. LDAP

d. SAML

Source Video

Skills Tested: Identity as a service

27. User account provisioning is best described as:

a. The business process for creating and managing access to resources in an information technology (IT) system

b. Creating federated trusts to allow authentication tokens to be passed from one domain to another

c. Securing the user environments through group policy management

d. Implementing authentication strategy for users.

28. As part of the Identity Provisioning Lifecycle, an Identity Policy must be created. What information would normally be contained as part of an organization's Identity Policy?

a. How users are granted credentials based on their identities

b. Which types of authentication users will be required to use

c. How a user's identification is verified and screened before the user is granted an account and credentials

d. How the identities of users are protected and how disclosure is prevented

29. A user's manager requests access to various systems for a new employee in his department. After the individual is approved and access granted, the requests are stored and will be used in future audits. What type of provisioning model does this scenario follow?

a. Role-based

b. Rule-based

c. Request-based

d. Identity-based

Domain 6 Security Assessment and Testing

1. As part of a yearly audit, you are required to conduct a review of the security controls implemented on your network and to ensure that known security vulnerabilities have been mitigated. You've been told that due to the critical nature of your business, your review must have a minimal effect on the network's performance, as well as the performance on any individual systems. What type of test should be conducted in order to meet these requirements?

a. Penetration test

b. Vulnerability assessment

c. Process review

d. Gap analysis

2. Bob is hired to conduct a penetration test for a local organization. After Bob had conducted a penetration test on a critical server, he learned that management was furious that performance was degraded during key business hours. Which document would have made clear which systems should have been tested and the acceptable times and techniques to be used?

a. Rules of engagement

b. Concept of operations

c. Statement of work

d. Exception reports

3. What is the purpose of a "full knowledge" penetration test?

a. To determine if an attacker can gain full knowledge of the network from external sources

b. To determine if full knowledge of a system can lead to a greater network compromise

c. To determine if controls are in place to protect the organization in the event that an administrator attempts to compromise the network

d. To determine the minimum amount of information that would need to be collected to obtain full knowledge of resources within a network.

Source Video

Skills Tested: Understand vulnerability assessments and penetration tests at a high level

4. Your company has been selected to conduct a vulnerability assessment and penetration test for a medium-sized organization. Which step should be taken first before proceeding?

a. Get management's approval for the test in writing.

b. Determine which tools you will use.

c. Begin with social engineering attacks, as employees are usually the easiest pathway onto a network.

d. Meet with management and determine the goals of the penetration test.

5. Penetration testers attempt to find weaknesses in systems just as attackers do. Often an attacker starts with no knowledge of the network and is forced to perform reconnaissance in order to learn information from publicly available sources. Which of the following is NOT likely to be found from publicly available sources?

a. Office Locations

b. Phone numbers of other locations

c. Names of managers

d. Internal IP addressing schemes

6. An attacker has intercepted a DNS zone transfer in the hopes of finding which hosts are running critical services such as Active Directory, Kerberos, Mail Services, etc. What is the name of the technique which gathers information about the network?

a. Fingerprinting

b. Footprinting

c. Reconnaissance

d. Escalation

Source Video

Skills Testing: Understanding of the steps and procedures used in conducting a penetration test

7. A network administrator wants to ensure that there is no improper access to his company's web server, so he sets up a honeypot to distract attackers from legitimate company resources. He has designed a fake website that advertises "free music downloads" to those that access the page. When users access the page, they are then reported to law enforcement for accessing a system without the appropriate permissions. What can be said of this practice?

a. It is a good security practice, and the administrator is likely to catch numerous attackers.

b. It is a good security practice because it "nudges" attackers in the direction to compromise the system so that they can be caught.

c. It is a poor security practice and an example of entrapment.

d. It is a poor security practice as attackers will not be interested in downloading free music if they are looking for company information.

8. Similar to a honeypot, some applications are written with apparent vulnerabilities that are actually designed by the developer. These apparent loopholes are designed to trap an attacker and thus, provide greater protection for the system. What are these vulnerabilities called?

a. Honey-app

b. Virtual application

c. Maintenance hook

d. Pseudo-flaw

9. As a detective measure, your organization has decided to implement a honeypot. You would like to gain insight into the tools and techniques that attackers are using. However, you know that a risk of using a honeypot is that they may become compromised and used to gain access to protected resources. Given the above information, where should your honeypot be placed?

a. Inside the DMZ

b. The company's internal network

c. Outside the company's firewall

d. Inside the company's firewall

Video Source

Skills tested: Understanding the placements, purpose, and risks associated with honeypots

10. A security technician is complaining that he has spent the majority of his afternoon responding to alerts from his intrusion detection system. The company has incorporated a new application that is generating requests that the IDS does not recognize, and therefore assumes that they are malicious in nature. What type of analysis engine is likely being used?

a. Pattern matching

b. Profile matching

c. Host-based

d. Network-based

11. Because of the number of false positives created by the IDS previously used by your organization, you've decided to use a signature-based system. Which of the following characteristics is NOT true of signature-based IDS?

a. Signature-based systems must update their signature files frequently or risk becoming outdated.

b. Signature-based systems are less likely to create false positive alerts than behavior based systems.

c. Signature-based systems are particularly good at detecting zero-day attacks.

d. Signature-based systems can be fooled by polymorphic code.

12. Which of the following best describes how an anomaly based analysis engine detects an attack?

a. The IDS compares the network activity to a known attack.

b. The IDS looks for patterns of behavior that seem suspicious.

c. The IDS evaluates network activity against a baseline.

d. The IDS uses rules manually configured by a network administrator.

Source Video

Skills tested: Understand the analysis engines that provide IDS/IPS to identify potential attacks.

13. While conducting a penetration test, you discover a significant security vulnerability that could allow an attacker to compromise the passwords of the payroll database and gain access to sensitive information. What should you do?

a. Research and apply a corrective means for this vulnerability.

b. Follow the procedures in the Rules of Engagement document.

c. Stop testing and immediately report the flaw to management.

d. Contact the payroll system administrator and pull the system offline immediately.

14. Your organization uses an internal addressing scheme on the 10.x.x.x network. This was chosen because the 10.x.x.x network consists of internal private IP addresses. When analyzing your IDS logs for suspicious activity, you notice that traffic is leaving your network from an external source IP address. What might this indicate?

a. Your network is being used to launch a downstream attack.

b. A denial of service attack directed at your network.

c. An external host is using a spoofed source address.

d. Employees are bypassing the proxy by manually configuring their IP addresses.

15. Upon completion of a penetration test for a new client, you provide them with your findings in a report. The main contact at the client company says that the report is too technical for him to understand and he would like the information in "plain language" that is easy to understand. To what section of your report should you refer him?

a. Scope Statement

b. Executive Summary

c. Attack Narrative

d. Metrics

Source Videos: One / Two

Skills tested: Analyze and report test outputs

Domain 7 Security Operations PART 1 Investigations and Daily Processes

1. After weeks of training, you have just joined your company's forensics investigation team. You've been asked to investigate a system that has possibly been compromised. You are the first member of the team to access the system in question. As the first person on the scene, what is your top priority?

a. Begin investigations immediately so that no time is lost.

b. Reboot the system to terminate the attack.

c. Search the date and time stamps and determine if any new applications or processes have been installed recently.

d. Focus on ensuring that the evidence is preserved and start the chain of custody.

2. In evidence collection, we must work from most volatile to least. Volatility describes the capability of the evidence to change or become lost—often due to system shutdown or loss of power. Which of the following elements would be most volatile?

a. RAM

b. CPU registers

c. Virtual memory

d. Hard drive

3. In computer forensics what is an important requirement of evidence collection?

a. The analysis should begin the moment evidence is identified.

b. Anyone who discovers evidence can begin the process or collection and examination.

c. Evidence should not be modified as a result of the collection.

d. The analysis should be performed on the original system or device whenever possible, as it is more likely to be admissible in court.

Source Video

Skills Tested: Understand the purpose and process of forensics investigations

4. Your organization purchased a server from a vendor who provided a signed SLA guaranteeing performance metrics. Within the warranty provided by the SLA, the server failed, and the vendor refused to meet their obligations. What type of evidence would describe a signed SLA?

a. Real evidence

b. Hearsay

c. Best evidence

d. Direct evidence

5. Your client's sensitive information was leaked via email to an outside source. The digital signature on the message indicated that a particular employee was responsible for the compromise. A cryptography expert was retained to testify on the techniques used for digital signatures and their reliability. What type of evidence would this expert's testimony be considered?

a. Primary

b. Best Evidence

c. Hearsay

d. Secondary evidence

6. A police officer locates a USB drive of an employee who is suspected of fraudulent activity. The officer asks for the employee to turn over the drive, but that individual refuses. If law enforcement were to seize evidence without the proper permission, that would be a violation of the employee's fourth amendment rights. In which of the following situations can evidence be seized without causing such a violation?

a. The evidence appears to incriminate the employee.

b. The evidence appears to exonerate the employee.

c. The evidence is in immediate danger of being destroyed.

d. The evidence is part of a federal crime.

Video Source

Skills Tested: Types of evidence and their implications

7. Hearsay is rarely admissible in court, as it usually describes second-hand evidence. Why might a print-out of an audit log, be ruled hearsay and thus inadmissible?

a. The actual information resides on the system in the 1's, and 0's recorded. The information often must be printed out which is a copy of the digital evidence.

b. Audit logs are unreliable and often don't track the necessary information.

c. Audit logs are not admissible because they are computer generated and there is no way to attest to their accuracy and integrity.

d. Often audit logs are misconfigured and would include more information than necessary, making them difficult to sift through.

8. Several years ago, an organization created a policy to allow security administrators to intercept messages and monitor their contents. They informed employees of this policy, had each sign a waiver acknowledging the new policy. The further implemented login banners indicating that there is no expectation of privacy. Will evidence collected in this manner be admissible in court?

a. No, because if the policy is created before users are notified, then it may not be admissible.

b. No, because employees were not trained on the policy, evidence may not be admissible.

c. If the policy isn't applied universally and the information is not collected as part of normal business processes, then it may not be admissible.

d. Yes, the company has done all it is required to do, and the evidence it collects as a result of this practice should be admissible in court.

9. Once an intruder has compromised a system, they usually attempt to delete any signs of their access. One frequent technique is to erase entries in audit logs. Which of the following will help lessen the risks of manipulation of audit logs?

a. Sending audit logs to write-once media

b. Hashing audit logs

c. Regular review of the contents of logs

d. All of the above

Video Source

Skills Tested: Conduct Monitoring and Logging Activities

10. Which of the following is the best description for resource provisioning?

a. A business process to create trusts between organizations

b. A Business process which creates and manages access to resources in an information technology environment

c. An automated process of sharing information across boundaries

d. Means of automating permissions for shared objects in a network environment

11. In an organization with a large number of employees, it is necessary to offload some basic activities to users. For instance, the IT department can be overwhelmed with tasks such as resetting passwords and creating new accounts. Which of the following would best assist with reducing the IT staff's workload?

a. Delegate administrative access to users.

b. Add users to power user group.

c. Transfer these processes to the help desk.

d. Implement self-service account provisioning.

12.. Users in your organization have access to a large number of applications and network-based services. The IT department is overwhelmed with ensuring consistent access to resources. You want to find a way to make sure accounts are created, and permissions granted as part of the onboarding process and that accounts are deleted and permissions revoked as part of off- boarding. Which of the following would enable this functionality?

a. Workflow provisioning

b. Discretionary account provisioning

c. Self-service provisioning

d. Automated provisioning

Sources: One / Two / Three / Four

Skills Tested: Secure the provisioning of resources

13. You have become concerned that your company's switch is not as secure as perhaps it could be. The switch is located in a locked room. Mac Filtering is enabled, and you have prevented all remote access protocols and require anyone accessing the switch to use console access only. You're now concerned with Man-In-The-Middle attacks, particularly those that poison the cache tables which contain mappings of IP addresses to MAC address. What security feature may you want to add?

a. DHCP Snooping

b. Dynamic ARP Inspection

c. Network Address Translation

d. Static IP addressing

14. In order to protect against leakage of sensitive information in the Human Resources Department, you've been asked to recommend an effective means of separating this department's traffic from the rest of the network. Which of the following would be the most cost-efficient method to create this isolation?

a. Implement a switch.

b. Implement a VLAN.

c. Implement a gateway

d. Implement IPSec in transport mode.

15. Firewalls are designed to separate zones based on the security requirements of each zone. Traffic is inspected and, based on the configured rule-set, traffic is allowed or denied. A generally accepted best practice is that firewalls should use which of the following?

a. Whitelisting

b. Blacklisting

c. Rules-based access control

d. Permit Any

Video Sources: One / Two / Three

Skills Tested: Employee resource protection through network segmentation

16. While training a new member of the incident response team, you've been asked to define the primary purpose of incident response? Which of the following is the best answer?

a. To collect information to be used in the prosecution of an attacker

b. To track, document and respond to network events

c. To eliminate the damage caused by a cyber attack

d. To reduce the impact of cyber incidents on the business.

17. A network administrator wants to be notified in the event that baseline performance metrics are exceeded. What is the best way for an administrator to learn of these events in a timely manner?

a. Review the audit logs on a regular basis.

b. Contact the audit log administrator and ask to be notified via email in the event described above.

c. Configure an alert within the software that monitors the system.

d. Run frequent queries on the performance metrics of the system in question.

18. DDoS (Distributed Denial of Service) attacks take advantage of compromised systems which are commandeered to launch an attack on another system or network. Which of the following is the most likely indicator that your internal hosts are being used (unintentionally) to launch a downstream attack on another network or system?

a. Traffic coming into the internal network with an internal address

b. Traffic coming into the internal network with an external address

c. Traffic leaving the internal network with an external address

d. Traffic leaving the internal network with an internal address

Video Source

Skills Tested: Perform Incident Response

19. A member of the evidence collection team retrieves audit logs from Monday, Wednesday and Thursday which indicate suspicious activity. No other logs are provided. Which of the following rules of evidence might prohibit those logs to be admitted in court?

a. Digital evidence must be complete.

b. Digital evidence must be authentic.

c. Digital evidence must be convincing.

d. Digital evidence must be accurate.

20. In forensic investigations, identification of evidence is the first step. Once an item has been identified as evidence, the incident response team should be notified. What is the most important responsibility of the first responder?

a. Examination of the evidence

b. Analysis of the evidence

c. Collection of the evidence

d. Preservation of the evidence

21 During a forensics investigation, it has been determined that an examination and analysis of the hard drive will be required. In order to demonstrate that the hard drive was not modified, you've been instructed to create hashes. How many hashes of the hard drive are necessary for the investigative process?

a. One

b. Two

c. Three

d. Four

Video Source

Skills Tested: Conduct incident management and understand basic concepts of forensics

22. Bob is attempting to connect to the hotel's wireless network to access his company's mail server. He is instructed by the hotel staff to use the SSID "HOTELX" where X is his floor number. Hours later, he discovers that his email has been uploaded to a malicious website. Which of the following would have (most likely) prevented this problem?

a. RADIUS

b. Mutual authentication

c. Two-factor authentication

d. Extensible Authentication Protocol

23. Your organization has a great number of sales people who travel from client site to client site. Their laptops are connected many different networks including home and unsecured networks. Before allowing these laptops to connect to your network, you want to ensure that the laptop is protected (as much as possible) from becoming affected by malware or exploits to the operating system. Which of the following network services should you employ?

a. NAC (Network Access Control)

b. RADIUS

c. Group policy

d. Firewall services

24. Access-list 102 deny TCP any any eq 23" serves what purpose on a router or firewall?

a. Blocks all TCP traffic

b. Blocks TCP traffic but allows traffic on port 23

c. Blocks all telnet traffic

d. Limits remote connections to 23 connections

Video Source: One / Two

Skills Tested: Operate and maintain preventative measures

25. A system audit indicates that the payroll system is not in compliance with the security policy due to several missing operating system security patches. After review, it seems that the system has not been patched in over a year. When you contact the vendor, he tells you that the payroll system is supported only on the current operating system patch level. Which of the following strategies should be used to lessen the vulnerability of the missing OS patches on this system?

a. Isolate the system on a separate network to limit its interaction with other systems

b. Implement an application layer firewall to protect the payroll system interface

c. Monitor the system's security log and look for unauthorized access to the payroll application

d. Perform reconciliation of all payroll transactions on a daily basis.

26. You've been placed in charge of developing a patch management strategy. You want to ensure systems stay up to date with the current patches and updates, and know that you can't rely on users to take the time to update their systems. You want to ensure that the patches are tested first, and prevent users from downloading files before they've been approved. What solution might best solve these problems?

a. Download the patches to a lab environment. Test the updates and patches and, once approved, install them on the client computers.

b. Create a group policy that forces users to download security patches as soon as these updates become available. Other updates can be approved when possible and then distributed to user systems when appropriate.

c. Only download patches from the particular vendor's website. Once the vendor has made the patches available, it can be assumed that they've been tested.

d. Implement a patch management server. Test and approve appropriate patches. Configure group policy so that the clients will contact this server and download the approved updates.

27. In your organization, new systems connect to a network server and download an operating system. After the operating system has been installed, patches and updates must then be applied. Which of the following describes a more efficient way of ensuring these newly installed operating systems are patched?

a. Implement Rolling updates

b. Implement Slipstreaming

c. Implement Patch management servers

d. Implement live

Video Source Skills Tested: Implement and support patch and vulnerability management

28. A technician reports that he read in a recent tech magazine that the brand of computers on your production network have a documented issue with their original BIOS instruction set. The article recommends that the BIOS be flashed (updated) to correct this issue. What should you do?

a. Test the proposed changes in the lab and if successful flash the BIOS of the production systems.

b. Test the proposed changes in the lab and if successful meet with department heads and schedule the implementation of the change on a department-by-department basis.

c. Make the change immediately.

d. Refer the change to your Change Control Board and wait for approval.

29. As a member of the server administration team, you receive a call at 2 am explaining that the database server has failed and has rendered several business units unable to continue their work. When you arrive at the office, you determine that the server has been infected with malicious code. After researching the issue, you determine that once you remove the malicious software, several registry keys will also need to be changed. Your company has a change control policy in place. What should you do?

a. Wait until the morning and begin the process of change control.

b. Make the change to limit the disruption to the business, as per your emergency change control process.

c. Remove the malicious code, but do not modify the registry of the system.

d. Call the head of the departments affected and determine how critical it is to restore services to those departments. Base your decisions on his reply.

30. The Change Control Board has approved a modification to the systems settings of the computers in the finance department. The proposed changes are tested in the lab and found to have no negative impact. The changes are scheduled and rolled out to the finance computers. Shortly thereafter the systems begin to fail with random error messages. What is most likely the problem?

a. The lab environment does not accurately reflect the systems in the Finance Department.

b. The Finance Department computers have been infected with a virus.

c. The settings were improperly configured.

d. The Finance department systems have had additional software installed which conflicts with the configuration changes.

Source Video

Skills Tested: Participate in and understand the change control process

Domain 7 Security Operations PART 2

Redundancy and Business Continuity

1. You have been tasked with developing a strategy to provide redundancy for hard drives. You need to determine the average amount of time a hard drive should last. Which of the following metrics would provide the best indication of the life expectancy of a device?

a. MTTR

b. MTBF

c. SLA

d. SLE

2. A file server operates on your organizational network. In the past, RAID 0 was used to enhance the performance of both “read” and “write” operations. Now, you’ve been asked to update the RAID array to include redundancy without losing the performance boost. Which is the best choice?

a. Disk Striping

b. RAID 1

c. Disk Duplexing

d. RAID 5

3. When using a mirrored set of drives (A RAID 1 array) how much disk space can be used for storage if two 4 TB drives are purchased?

a. 1 TB

b. 2 TB

c. 3 TB

d. 4TB

Source Video

Skills Tested Hardware Redundancy

4. In order to provide high availability for your company's website, a technician suggests that you implement clustering. Which of the following is the best definition of a cluster?

a. Multiple servers which, in turn, handle incoming requests to increase performance

b. Multiple servers that replicate information on a regular basis so that all servers contain current information

c. Multiple physical servers acting as a single logical unit

d. Multiple servers configured with "Round Robin" load balancing through DNS

5. You work in a small store that sells auto parts. The company's computer systems are used to access inventory and other minor activities as needed. There is very little money in the budget for IT systems. However, redundancy for the server is necessary as a failure in service would equate to lost sales. What is the cheapest way to provide server redundancy from the choices below?

a. Implement an Active-Passive cluster

b. Implement a web farm

c. Migrate your services to the cloud

d. Implement RAID 10

6. What is the difference between redundant servers and a server cluster?

a. Redundant servers don't provide load balancing while all clusters provide that service by default.

b. Usually, redundant servers are individual and discrete devices on the network while a cluster may contain many nodes but will still appear as a single system.

c. Redundant servers can span geographic locations, but a server cluster must be local.

d. Redundant servers have a quicker failover and fail-back process than a server cluster.

Video Source

Skills Tested: Understand redundancy provided by server clustering

7. At 4:00 in the afternoon you receive a request to install an operating system patch on a production server. Before applying the patch, you want to ensure that you're able to recover the server in the event that the patch does not work properly. What type of backup should you perform?

a. Full

b. Incremental

c. Differential

d. Copy

8. Your organization always performs a nightly backup at 9:00pm. Each morning, the tape is ejected, and the backup report indicates the backup was successful. However, malware has infected the data on the current drive, and when you attempt to restore from the backup, you get an error message which reads "File not found." How should backups be tested and verified?

a. Backups should be hashed and the hash compared with the hash on the logs.

b. Backup reports are accurate and a good indication of a successful backup. In this case, he problem is caused by something else.

c. The only way to have true confidence in backups is to restore them periodically.

d. Backups should be verified as part of the backup procedure.

9. Your organization runs a full backup each Sunday night. Then, each day of the week an incremental backup is performed. On Thursday morning the server suffers a failure requiring a full restoration of data. How many tapes must be restored?

a. 1

b. 2

c. 3

d. 4

Video Source

Skills Tested: Understand Backup and Restore Operations

10. You work for an organization that has a very low tolerance for loss of data. Nightly backups, though conducted, do not provide enough protection against data loss. What type of technology would allow you to transfer batches of transactions to an offsite facility numerous times per day?

a. Clustering

b. Data Shadowing

c. Electronic Vaulting

d. Remote Journaling

11. After a disaster, critical systems are migrated to an offsite facility. A user calls with a complaint that the restored data is too old to be of any use. You check the restored data to ensure it was restored from the most current backup available. What is the most likely cause of this problem?

a. The user is likely looking at a cached copy.

b. The data was restored to the incorrect directory.

c. There is a network replication issue.

d. Recovery point objectives are very short, and the backups are not frequent enough to meet those needs.

12. How best would database shadowing be defined?

a. The database is copied to an alternative location periodically for fault tolerance.

b. The data transactions are simultaneously written to two different databases.

c. The database transactions are written to a striped set for performance.

d. The database uses RAID 1.

Video Source

Skills Tested: Additional backup strategies

13. The Disaster Recovery Plan provides instruction on the actions necessary to be taken during the immediacy of the disaster, with a focus on protecting life, above all, and then property. Which of the following provides the next steps of the DRP?

a. Return services to order, starting with least critical working towards most critical.

b. Return services to order starting with most critical working towards least critical.

c. Restoring operations to full capacity as quickly as possible.

d. Restoring the original facility so that business processes can return.

14. A small organization has a RAID array that can be restored in one hour to provide redundancy for hard drives. In addition, they have a backup policy in which data is backed up every night at midnight; the backups are stored onsite for one month and then off-site for one year. The strategies were decided in writing the BIA. In the above situation, what are the organizations RPO for data?

a. One Day

b. One Hour

c. One Week

d. One Month

15. Your organization leases a cold site from a vendor in the area. What information may not be guaranteed in your contract? a. Size of the facility b. Services available at the facility c. Availability of the facility d. General location of the facility

Video Source

Skills Tested: Implement disaster recovery processes

16. You would like to conduct a test of your organization's Disaster Recovery Plan, but are concerned about the potential harm to your production environment. You would like to use the most realistic test, without out the risk of running processes out of the offsite location. What type of test would be best in this situation?

a. Checklist

b. Structured Walkthrough

c. Simulation

d. Parallel

17. Which of the following would not be determined in a test of the disaster recovery plan?

a. Does the plan include practical instructions that can be carried out?

b. How well do employees carry out the plan?

c. Does the plan contain accurate information?

d. Are all the necessary steps addressed in the plan?

18. On Friday afternoon your organization shuts down all business processes. Over the weekend the team works on enabling services at an offsite facility. On Monday morning, all business functions are performed at the offsite location. What type of testing was performed?

a. Structured walk-through

b. Parallel

c. Simulation

d. Full interruption

Video Source

Skills Tested: Test disaster recovery plans

19. You are the project manager for the Business Continuity Planning project. After getting a written policy from senior management, you're ready to proceed with the following steps. As you begin conducting the BIA (Business Impact Analysis) one of your team members asks the difference between Business Impact Analysis and Risk Analysis. How should you respond to the question?

a. The BIA and risk analyses are the same things and both address the potential threats and their potential harm.

b. The BIA addresses the impact that various threats could have on your organization, while risk analysis determines how likely the threats are to materialize.

c. The BIA identifies and prioritizes business processes based on criticality while risk analysis focuses on threats and their likelihood and impact.

d. The BIA identifies the risks while Risk Analysis addresses how we respond to risks.

20. The first step of creating a Business Continuity Plan is to obtain a BCP policy from senior management. In addition to setting the direction and goals of the plan, why else is the policy so important?

a. The BCP policy is a commitment from senior management to support and fund the project.

b. The BCP policy indicates how important the BCP is to the organization and will help encourage involvement from all the employees in the organization.

c. The BCP policy is necessary to be in compliance with regulations that require a BCP.

d. The BCP policy authorizes the project manager of the project.

21. Often senior management assigns members to the BCP team. Which employees should be members of the BCP team?

a. IT managers

b. A cross-functional representation of the business units

c. All employees

d. Senior management

Video Source

Skills Tested: Participate in business continuity planning and exercises

22. One morning, as you swipe your access card and enter the building, an unknown individual attempts to enter behind you. How should you proceed?

a. Ask the visitor if he or she has an access card. If not, ask him or her to leave.

b. Ask the visitor if he or she has an access card. If not, escort him or her to security immediately.

c. Ask him or her which department her works for and call that department.

d. Ask him to show you some form of identification before letting him in.

23. In assessing the environment of the server room, the following information was collected: Humidity 70% and temperature 70 degrees. What should be done to protect the devices in the server room?

a. Increase the temperature.

b. Decrease the temperature.

c. Increase the humidity.

d. Decrease the humidity.

24. Your organization is considering adding fencing to your perimeter to increase the physical safety of employees and provide a physical barrier against attackers. What is the least height fence that will deter an intruder?

a. 8 feet

b. 6 feet

c. 10 feet

d. 12 feet

Video Source

Skills Tested: Implement and manage physical security

25. Your data center is populated with numerous electronic devices and has a staff of roughly two hundred people. Your organization requires that a water-based sprinkler system is used to limit the loss of life and property in the event of a fire. What type of sprinkler system is best-suited for this environment?

a. Wet pipe

b. Dry pipe

c. Deluge

d. Pre-action

26. The BCP is made of several sub-plans. Which of the following sub-plans would include information on how to help employees with physical challenges to evacuate a building in the event of an emergency?

a. Crisis Communication Plan

b. Occupant Emergency Plan

c. Reconstitution Plan

d. Recovery Plan

27. In a data center, the greatest risk of fire comes from electrical distribution systems. How close to these systems should fire extinguishers be placed?

a. 25 feet

b. 50 feet

c. 100 feet

d. 1000 feet

Video Source

Skills Tested: Participate in addressing personnel safety concerns

Domain 8 Software Development Security

1. When allowing users to input information to a form, you want to ensure that data which does not meet your requirements is blocked from entry, but not modified. You would also like to ensure that no data control language is used as well. What should happen before form entries are accepted?

a. Validation

b. Sanitization

c. Extraction

d. Elevation

2. Which of the following is a software testing technique used to discover coding errors and security loopholes in software, particularly lack of input validation

a. Validating

b. Sanitizing

c. Fuzzing

d. White box testing

3. Your organization has determined a need to be more aggressive with its security testing of software before implementation. Senior management has asked whether white box testing is currently used. What is white box testing?

a. A type of code review

b. A type of user acceptance testing

c. A type of fuzzing

d. A type of input validation

Source Video

Skills Tested: Assess the security of software

4. You have been hired to assess the security for a small training company. This company offers an introductory class to computer hacking. The classroom is not segmented from the rest of the training company's network. The admin explains that the students in the class are only script kiddies and could never do any real harm. What is your response?

a. Agree, as the skills necessary to truly damage a network or system are much higher than what a user of that level of knowledge would possess.

b. Agree, as the cost of segmenting the classroom from the rest of the network would be greater than the potential for loss.

c. Disagree, as script kiddies can be just as dangerous as any other hacker, and sometimes more so, as they don't realize the power of the code they are executing.

d. Assume the admin has assessed the risk, and support his decision.

5. An Advanced Persistent Threat is a type of attack directly targeting a specific system or organization. These attacks are often sophisticated and occur over a period of time until ultimately accomplishing their goal. What attack type would an APT be classified as?

a. Unstructured

b. Structured

c. Restructured

d. Highly Structured

6. An organization has asked that you provide penetration testing for a critical database server. Authorized pen-testing is sometimes referred to as ____________.

a. White-hat testing

b. White-box Testing

c. Grey-hat Testing

d. Grey-box Testing

Video Source

Skills tested: Assess effectiveness of security controls

7. When scanning a system, which of the following information would be LEAST helpful to an attacker?

a. Network services running

b. IP Address and Subnet Mask

c. Operating system

d. Installed software

8. The first step of many attacks is reconnaissance. In reconnaissance, an attacker looks to find information about the organization from publically available sources. Which of the following is LEAST likely to help an attacker?

a. Job postings for technical positions in your organization

b. The WhoIs database

c. Company Policy and Mission Statement from the company's web page

d. List of branch offices, locations, and phone numbers

9. Senior management has recently become concerned with reducing their liability in relation to the protection of company assets. They want to ensure that the meet legal requirements and industry standards in relation to information security. By authorizing a vulnerability test of the corporate network, what legal responsibility are they demonstrating?

a. Due Care

b. Due Diligence

c. Proximate Causation

d. Adherence to policy

Video Source

Skills Tested: Understand the essentials of vulnerability scans and penetration testing

10. An attack in which unvalidated data is sent to an interpreter as part of a query or command, tricking the interpreter into executing hostile commands or processing data without proper authentication is called _____________

a. XSRF Attack

b. Code injection

c. Reverse query

d. DDoS

11. In configuring a web server for your intranet, you've been advised to use SSL/TLS instead of HTTP. You've heard that HTTP is insecure and does not often privacy for data. What is another concern of HTTP?

a. HTTP is slower than HTTPS due to the extended handshake process.

b. HTTP key distribution is complex.

c. HTTP authenticates but does not encrypt

d. HTTP is stateless.

12. A web page displays comments by customers in relation to their new test product. They hope that the positive feedback from customers will encourage other customers to buy their product. However an attacker enters, "<script>MaliciousCommand();</script>" into the comment section. When the page is displayed in users' browser, the script will run. What type of attack is this?

a. XSRF

b. XSS

c. LDAP Injection

d. Session hijacking

Video Source

Skills Tested: Understand common threats directed at web applications

13. While you are logged into your online bank account at MyBank.com, a malicious user, “Mallory” send an email with the link: <imgsrc="https://www.MyBank.com/transfer?amount=1000&amp;destination=mallory"> When you click, the link is processed by your browser and sends 1000 to Mallory. The attack appears as if it originates from you, as your session ID and other cookies are sent as part of the request. What type of attack is this?

a. XSRF

b. XSS

c. LDAP Injection

d. Session hijacking

14. When John provides his username and password to a banking server, he is granted access to his own confidential banking information. John then notices the URL reads “https://bank/balance?acc=123” John modifies the URL to read, “https://bank/balance?acc=124” and is able to access another user’s account. What is exploited in this attack?

a. Missing input validation

b. Directory Traversal

c. Indirect Object Access

d. Missing Function level

15. A user logs on to a company site with his username, JSmith and sees the following reference in the URL: Http://company.com/app/standarduserpage. He then types : http://company.com/app/administratorpage and gains administrative privileges to the site. What is exploited in this attack?

a. Missing input validation

b. Directory traversal

c. Indirect object access

d. Missing function level access control

Video Source

Skills Tested: Skills Tested: Understand common threats directed at web applications

16. Java applets are small applications that run in users' browser that provide additional functionality. However, if that applet is allowed unlimited access to operating system resources or hardware such as memory it can be used to modify the system maliciously, it can do harm in the hands of someone with the intent of causing damage or harm. What defensive mechanism is used to limit the scope of Java applets?

a. Input validation

b. Client-side scripting

c. Sandboxing

d. Indirect object access

17. You, as a database administrator, want to control user access to your database. Users need the ability to manipulate items in the database, while still being forced to create well-formed transactions. What should you provide to give the users the access they need while still protecting your database?

a. Privileged access

b. Anonymous access

c. Front-end application

d. Client-side script

18. You work for a vendor that frequently processes credit card payments for customers. To be in compliance with PCI-DSS (Payment Card Industry Data Security Standards) as well as to follow best practices, you want to ensure that no credit card numbers are stored on your Point of Sale terminals nor in your company database. What is recommended in this situation?

a. Tokenization

b. Principle of least privilege

c. Front-end applications

d. Anonymization

Video Source

Skills Tested: Understand defensive coding techniques to mitigate application vulnerabilities

19. Distributed databases are those which house portions of the database in multiple locations. This may be for load-balancing, redundancy, security, or efficiency. Which of the following services is offered through a distributed database?

a. LDAP

b. DNS

c. Office 365

d. PaaS

20. Active Directory and other directory services based on the LDAP structure are hierarchical in nature. DNS is also a hierarchical database, which is hierarchical as well. Which of the following is true about these database models?

a. In relational databases, parents can have only one child

b. In relational databases, a child can have only one parent

c. In hierarchical databases, a parent can have only one child

d. In hierarchical databases, a child can have only one parent

21. Database models that store information in tables and rows and use primary and foreign keys to organize data are referred to as ____________

a. Distributed

b. Hierarchical

c. Segregated

d. Relational

Video Source

Skills tested: Understand the different type of database models.

22. In each table of a relational database, there must be a field that uniquely identifies every record as being unique. What is this field called?

a. Primary key

b. Foreign key

c. Degree

d. Attribute

23. You Database administrator mentioned that a relationship link was based on a one-to-many relationship. What database term describes the type of relationship and how the records are related?

a. Cardinality

b. Schema

c. Tuple

d. Attribute

24. Which of the following is the best definition of a database's schema?

a. The relationship between keys

b. Centrally located repository to store database functions, metadata and other elements that are available universally within the database

c. The defining description of all elements in a database including tables, relations, relationships, etc.

d. The rules of a database that are used to enforce principals such as entity and referential integrity

Video Source

Skills Tested: Understand components of a relational database