QBank Quiz Domain 1

Test ID: 178834628

Question #1 of 54

Question ID: 1322855

Which of the following is true of privilege escalation?

A) vertical movement to a different level

B) granted freely

C) obtained without authorization

D) horizontal movement to the same level

Explanation

Privilege escalation occurs when someone obtains, without authorization, the rights and privileges of a different user. Privilege escalation usually occurs by logging in to a system using your valid user account and then finding a way to access files that you do not have permissions to access. This often involves invoking a program that can change your permissions, such as Set User ID (SUID) or Set Group ID (SGID), or invoking a program that runs in an administrative context.

There are several methods of dealing with privilege escalation, including using least privilege accounts, privilege separation, and so on. Privilege escalation can lead to denial-of-service (DoS) attacks. An example of privilege escalation is gaining access to a file you should not access by changing the permissions of your valid account.

Horizontal escalation is movement to an account on the same level, such as from a regular user to another regular user.

Vertical escalation is movement to an account on a different level, such as from a regular user to an administrator.

Privilege escalation is never granted freely. It is an attack.

Objective:
Security Concepts

Sub-Objective:
Describe security terms (Threat intelligence (TI); Threat hunting; Malware analysis; Threat actor; Run book automation (RBA); Reverse engineering; Sliding window anomaly detection; Principle of least privilege; Zero trust; Threat intelligence platform (TIP)

References:

NetSparker > What Is Privilege Escalation and Why Is It Important?

Question #2 of 54

Question ID: 1322852

Which of the following can be used to identify the details of a breach?

A) reverse engineering

B) chain of custody

C) decomposition

D) discovery

Explanation

Reverse engineering is the process of breaking down of an attack into its parts to understand how it happened. It may even involve reverse engineering the software involved in the attack to determine its purpose.

Chain of custody is a term that represents the chronological history of the possession of digital evidence. If it does not account for the security of the evidence at all times the evidence may be successfully challenged as corrupted.

Discovery is the exchange of evidence by both sides before a trial.

Decomposition is only one part of reverse engineering. Reverse engineering also includes analyzing the purpose of the attack.

Objective:
Security Concepts

Sub-Objective:
Describe security terms (Threat intelligence (TI); Threat hunting; Malware analysis; Threat actor; Run book automation (RBA); Reverse engineering; Sliding window anomaly detection; Principle of least privilege; Zero trust; Threat intelligence platform (TIP)

References:

Wiki > OWASP Reverse Engineering and Code Modification Prevention Project

---

Question #3 of 54

Question ID: 1322870

Which CVSS access vector metric value indicates the attacker must have access to the broadcast or collision domain of the vulnerable system for the attack to succeed?

A) High
B) Adjacent network
C) Local
D) Network

Explanation

The Adjacent Network (A) value indicates the attacker must have access to the broadcast or collision domain of the vulnerable system to perform the attack. The Common Vulnerability Scoring System (CVSS) access vector (AV) shows how a vulnerability may be exploited. The three vectors have the following meanings:

- Local (L) - The attacker must either have physical access to the vulnerable system or a local account
- Adjacent Network (A) -The attacker must have access to the broadcast or collision domain of the vulnerable system.
- Network (N) - These types of vulnerabilities are often described as remotely exploitable (from another network)

High is an attack complexity metric, not an access vector. The complexity metric assesses whether the attacker can perform the attack at will. It has two possible values:

- Low (L) - the attacker can perform the attack at will
- High (H) - the attack depends on conditions beyond the control of the attacker

The CVSS captures principal characteristics of a vulnerability and produces a numerical score that reflects its severity. This score can also be expressed as a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

Objective:
Security Concepts

Sub-Objective:
Describe terms as defined in CVSS (Attack vector; Attack complexity; Privileges required; User interaction; Scope)

References:

First > Common Vulnerability Scoring System SIG

Question #4 of 54

Question ID: 1322846

Which of the following is used to prevent malicious software on multiple systems?

A) network AV

B) HIDS

C) host AV

D) HIPS

Explanation

To protect multiple devices from malware, network antivirus (AV) should be used. These tools can protect an entire network of devices.

A host antivirus (AV) can only protect the device on which it is installed.

A host intrusion prevention system (HIPS) can prevent multiple attack types, but it can only protect the device on which it is installed.

A host intrusion detection system (HIDS) can detect multiple attack types, but it can only detect attacks against the device on which it is installed.

Intrusion prevention systems (IPS) and intrusion detection systems (IDS) work together to complement each other. IPS systems can block activities on certain Web sites. Users may be allowed to access the sites but may be prevented from accessing certain features within the site. In other cases, the entire site may be blocked, depending on the security requirements for the organization.

Objective:
Security Concepts

Sub-Objective:
Compare security deployments (Network, endpoint, and application security systems; Agentless and agent-based protections; Legacy antivirus and antimalware; SIEM, SOAR, and log management)

References:

TechRepublic > Pick an anti-virus solution that will grow with your network

---

Question #5 of 54

Question ID: 1325260

What is meant by the A in the CIA triad?

A) Accountability

B) Availability

C) Accessibility

D) Authorization

Explanation

The A in CIA stands for Availability. The CIA triad represents the three main goals of any security system. The letters stand for the following security goals:

- C - Confidentiality - means only authorized individuals can read the data
- I - Integrity - means only authorized individuals can change the data
- A - Availability- means data is always available when needed

Authorization and accountability (or accounting) are two of the three services provided by an AAA service. The third is authentication.

Accessibility is not a term normally used when discussing AAA or the CIA triad.

Objective:
Security Concepts

Sub-Objective:
Describe the CIA triad

References:

TechRepublic > The CIA Triad

Question #6 of 54

Question ID: 1322861

Which of these mitigation techniques applies the principle of defense in depth to help mitigate the attacks to which the device is susceptible?

A) Flood guard

B) Privileged user account

C) Signature management

D) Device hardening

Explanation

Device hardening is the application of defense in depth principles to help mitigate the attacks to which the device is susceptible. For a switch, device hardening could include shutting off unused ports. Another example could be blocking traffic on port 23 to prevent traffic on an unused port. Other enhanced security activities, such as password policies and establishing file permissions, are also examples of device hardening. Device hardening provides controls at all layers of the OSI model to provide the defense in depth.

Defense in depth is a multi-layered approach to security that establishes a robust defensive strategy against attackers. This strategy prevents a single attack from being sufficient to breach an environment, forcing attackers to use complex, multi-pronged, daisy-chain attacks that are more likely to fail or be detected during the attempt.

Signature management is the monitoring of digital signatures to ensure that file tampering has not occurred. This would only protect against data integrity attacks, not against any other kinds of attacks.

Flood guard establishes the maximum number of MAC addresses that can be seen by an interface. The switch monitors the traffic on the interface. If the network gets flooded with MAC addresses, the flood monitor can intervene by

disabling ports and filtering out traffic. This would only protect against a single type of attack, thereby not providing defense in depth.

A privileged user account is an account that has less-restrictive access to a system. Examples of privileged user accounts include domain administrator, local administrator, and application accounts. Users with privileged accounts can include systems admins, management personnel, network administrators, and database administrators, among others. This would not provide defense in depth because it only protects against certain account issues.

Objective:
Security Concepts

Sub-Objective:
Describe the principles of the defense-in-depth strategy

References:

Techopedia > Hardening

CompTIA Network+ N10-007 Cert Guide, Chapter 12: Network Security, Defense Against Attacks

---

Question #7 of 54

Question ID: 1322842

Which of the following tools is for email?

A) CWS
B) WSA
C) AMP
D) CES

Explanation

The Cloud Email Security tool is a Cisco tool for scenarios where cloud-based email is in use. It features Cisco Advanced Phishing Protection, domain protection (from using your domain as a spam source), and end user protection from bad actors.

The Web Security Appliance (WSA) is a Cisco tool that can as a web application firewall, protecting a web or HTTP server. Web Security can be run on an appliance, as a virtual machine, and even on a branch router. It is a form of web application firewall.

Cisco Advanced Malware Protection (AMP) is a malware avoidance tool. It prevents threats at point of entry, then continuously tracks every file it lets onto your endpoints. AMP can uncover even the most advanced threats, including fileless malware and ransomware.

Objective:
Security Concepts

Sub-Objective:
Compare security deployments (Network, endpoint, and application security systems; Agentless and agent-based protections; Legacy antivirus and antimalware; SIEM, SOAR, and log management)

References:

Cisco > Support > Product Support > Security > Configuring Office 365 (Microsoft) with Cisco Cloud Email Security (CES) > Document ID: 214812

Question #8 of 54

Question ID: 1322845

Which of the following is used to avoid malicious software?

A) WSA

B) CWS

C) AMP

D) CES

Explanation

Cisco Advanced Malware Protection (AMP) is a malware avoidance tool. It prevents threats at point of entry, then continuously tracks every file it lets onto your endpoints. AMP can uncover even the most advanced threats, including fileless malware and ransomware.

The Web Security Appliance (WSA) is a Cisco tool that can as a web application firewall, protecting a web or HTTP server. Web Security can be run on an appliance, as a virtual machine, and even on a branch router. It is a form of web application firewall.

The Cisco Cloud Web Security (CWS) tool for web servers when deployed in a cloud environment. The web-filtering service in Cisco CWS creates, enforces, and monitors web usage policies by applying real-time, rule-based filters and checking an up-to-date and accurate database for categorizing websites.

The Cloud Email Security tool is a Cisco tool for scenarios where cloud-based email is in use. It features Cisco Advanced Phishing Protection, domain protection (from using your domain as a spam source), and end user protection from bad actors.

Objective:
Security Concepts

Sub-Objective:
Compare security deployments (Network, endpoint, and application security systems; Agentless and agent-based protections; Legacy antivirus and antimalware; SIEM, SOAR, and log management)

References:

Cisco > Products > Security > Advanced Malware Protection (AMP)

Question #9 of 54

Question ID: 1322857

Which of the following represents an exploitable, unpatched, and unmitigated weakness in software?

A) exploit

B) vulnerability

C) breach

D) threat

Explanation

A vulnerability is a susceptibility to a threat that exists in a system that has not been mitigated. Patching would be a form of mitigation if it were used to address the vulnerability.

When a security weakness or vulnerability exists in a system and a threat actor takes advantage, the attack is considered an exploit. An example of a vulnerability is keeping ports open for nonessential services.

A threat is an external danger to which a system may or may not be vulnerable. It is a potential danger that could take advantage of a system if it is vulnerable. An attacker picking the lock of the back entrance to a facility is an example of a threat, not a vulnerability.

A breach is when an exploit is successful in providing unauthorized access to data.

Objective:
Security Concepts

Sub-Objective:
Compare security concepts (Risk (risk scoring/risk weighting, risk reduction, risk assessment); Threat; Vulnerability; Exploit)

References:

Threat Analysis > Threat, vulnerability, risk – commonly mixed up terms

---

Question #10 of 54

Question ID: 1322854

When you give users the minimum rights required to do their job, which security concept are you practicing?

A) job rotation
B) separation of duties
C) defense in depth
D) least privilege

Explanation

The principle of least privilege prescribes that users only be given the minimum rights required to do their job.

Separation of duties prescribes that any critical task should be broken into multiple tasks, with each given to a different person. Separation of duties ensures that no individual can compromise a system, and is considered valuable in deterring fraud.

A defense in depth strategy prescribes that multiple impediments be presented to a malicious individual. Multiple physical hurdles may be presented, but it can also use technical hurdles, such as multiple firewalls. Generally, defense-in-depth/layered security means that someone would have to breach multiple safeguards to have access to the entire network. For example, splitting your network into several subnets or VLANs based on departments would prevent a breach to the HR network from affecting the Accounting network.

Job rotation ensures that a particular role has more than one person trained to perform its duties. Personnel should be periodically rotated, particularly in important positions. Job rotation and separation of duties also help to prevent collusion.

Objective:
Security Concepts

Sub-Objective:
Describe security terms (Threat intelligence (TI); Threat hunting; Malware analysis; Threat actor; Run book automation (RBA); Reverse engineering; Sliding window anomaly detection; Principle of least privilege; Zero trust; Threat intelligence platform (TIP)

References:

Wiki > Principle of least privilege

Question #11 of 54

Question ID: 1322873

Which CVSS metric is described as the secrecy of an information resource managed by a software component due to an exploited vulnerability?

A) Integrity

B) Availability

C) Attack vector

D) Confidentiality

Explanation

Confidentiality is the secrecy of an information resource managed by a software component due to an exploited vulnerability. Confidentiality is an impact metric. The impact metric reflects the degree of impact, and can reflect the attack's impact on confidentiality, integrity, or availability. The scores can be:

- None (N)- no impact
- Low (L) - low impact
- High (H) - high impact

Integrity is an impact metric and is the extent to which the information resource can be changed due to an attack.

Availability measures the extent to which availability is at risk due to an attack. It is also an impact metric.

Attack vector is a base metric that describes the nature of the vulnerability. There are three CVSS base metrics as follows:

- Access Vector - The access vector (AV) shows how a vulnerability may be exploited.
- Attack Complexity - The attack complexity (AC) metric describes how easy or difficult it is to exploit the discovered vulnerability.
- Authentication - The authentication (Au) metric describes the number of times that an attacker must authenticate to a target to exploit it.

Objective:
Security Concepts

Sub-Objective:
Describe terms as defined in CVSS (Attack vector; Attack complexity; Privileges required; User interaction; Scope)

References:

HYPERLINK "https://www.first.org/cvss/"First > Common Vulnerability Scoring System SIG

Question #12 of 54

Question ID: 1322840

Which component is the hub in the pxGrid architecture?

A) FMC

B) ISE

C) WSA

D) ASA

Explanation

The ISE is the hub in a hub and spoke Cisco Platform Exchange Grid (pxGrid) architecture. Cisco Identity Services Engine (ISE) is used to share user and device context with your application. Communication occurs between the Cisco ISE session directory to other policy network systems, such as the ASA. Cisco Platform Exchange Grid (pxGrid) enables network system collaboration among parts of the IT infrastructure such as security monitoring and detection systems.

Cisco ISE receives context from the application for implementation of the ISE network policy. ISE enables quarantining users and devices in response to threating network events.

Cisco Web Security Appliance (WSA) can be a spoke in the pxGrid architecture, but not the hub. Web Security can be run on an appliance, as a virtual machine, and even on a branch router. It is a form of web application firewall.

Cisco Firepower Management Center (FMC) can be a spoke in the pxGrid architecture, but not the hub. It is an administrative nerve center for managing critical Cisco network security solutions. It provides complete and unified management over firewalls, application control, intrusion prevention, URL filtering, and advanced malware protection.

Objective:
Security Concepts

Sub-Objective:
Compare security deployments (Network, endpoint, and application security systems; Agentless and agent-based protections; Legacy antivirus and antimalware; SIEM, SOAR, and log management)

References:

Cisco Developer > Cisco Platform Exchange Grid (pxGrid)

Question #13 of 54

Question ID: 1322871

Which CVSS base metric shows how a vulnerability may be exploited?

A) attack complexity
B) authentication
C) access vector
D) confidentiality

Explanation

There are three base metrics used by CVSS:

- Access vector - The access vector (AV) shows how a vulnerability may be exploited.
- Attack complexity - The attack complexity (AC) metric describes how easy or difficult it is to exploit the discovered vulnerability.
- Authentication - The authentication (Au) metric describes the number of times that an attacker must authenticate to a target to exploit it.

Confidentiality is an impact metric, not a base metric. The impact metric reflects the degree of impact, and can reflect the attack's impact on confidentiality, integrity, or availability. The scores can have one of three values:

- None (N) - no impact
- Low (L) - low impact
- High (H) - high impact

The complexity metric assesses whether the attacker can perform the attack at will. It has two possible values:

- Low (L) - the attacker can perform the attack at will

- High (H) - the attack depends on conditions beyond the control of the attacker

The Common Vulnerability Scoring System (CVSS) captures principal characteristics of a vulnerability and produces a numerical score that reflects its severity. This score can also be expressed as a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

Objective:
Security Concepts

Sub-Objective:
Describe terms as defined in CVSS (Attack vector; Attack complexity; Privileges required; User interaction; Scope)

References:

First > Common Vulnerability Scoring System SIG

Question #14 of 54

Question ID: 1322844

Which of the following statements is NOT true of agentless antivirus?

A) exhaustive infrastructure scan

B) easier security management

C) higher overall cost than agent-based antivirus

D) centralized file scanning

Explanation

Agentless antivirus cost less to deploy than agent-based software.

The following are all advantages of agentless antivirus:

- Centralized file scanning
- Lower operational overhead
- Native integration
- Security policy consolidation
- Exhaustive infrastructure scan
- Reduction in computing resource demands, especially in mitigating or avoiding scan storms
- Considerably easier security management
- Always-on anti-virus/anti-malware protection

Objective:
Security Concepts

Sub-Objective:
Compare security deployments (Network, endpoint, and application security systems; Agentless and agent-based protections; Legacy antivirus and antimalware; SIEM, SOAR, and log management)

References:

WHOA > Advantages of Agentless Antivirus on Virtualized Cloud Infrastructure

---

Question #15 of 54

Question ID: 1322875

Which of the following CVSS scores measures the extent to which the information resource can be changed due to an attack?

A) Attack vector

B) Integrity

C) Confidentiality

D) Availability

Explanation

Integrity is the extent to which the information resource can be changed due to an attack.

Confidentiality is the secrecy of an information resource managed by a software component due to an exploited vulnerability.

Availability measures the extent to which availability is at risk due to an attack.

Attack vector describe the nature of the vulnerability. Version 3.0 of CVSS sets the possible values for the confidentiality, integrity, and availability metrics to none, low, and high. These are explained below for integrity:

- High (H) - There is a total loss of integrity, or a complete loss of protection. For example, the attacker is able to modify any/all files protected by the impacted component. Alternatively, only some files can be modified, but malicious modification would present a direct, serious consequence to the impacted component.
- Low (L) - Modification of data is possible, but the attacker does not have control over the consequence of a modification, or the amount of modification is constrained. The data modification does not have a direct, serious impact on the impacted component.
- None (N) - There is no loss of integrity within the impacted component.

Objective:
Security Concepts

Sub-Objective:
Describe terms as defined in CVSS (Attack vector; Attack complexity; Privileges required; User interaction; Scope)

References:

First > Common Vulnerability Scoring System SIG

Question #16 of 54

Question ID: 1322841

Which of the following is used to protect an HTTP server?

A) WSA

B) CES

C) ESA

D) AMP

Explanation

The Web Security Appliance (WSA) is a Cisco tool that can act as a web application firewall, protecting a web or HTTP server. Web Security can be run on an appliance, as a virtual machine, and even on a branch router. It is a form of web application firewall.

Cisco Advanced Malware Protection (AMP) is a malware avoidance tool. It prevents threats at point of entry, then continuously tracks every file it lets onto your endpoints. AMP can uncover even the most advanced threats, including fileless malware and ransomware.

The Cisco Email Security Appliance is an email security tool. It protects against phishing email attacks such as ransomware and analyzes emails for threats such as zero-day exploits and attacks hidden in attachments and malicious URLs.

The Cloud Email Security tool is a Cisco tool for scenarios where cloud-based email is in use. It features Cisco Advanced Phishing Protection, domain protection (from using your domain as a spam source), and end user protection from bad actors.

Objective:
Security Concepts

Sub-Objective:
Compare security deployments (Network, endpoint, and application security systems; Agentless and agent-based protections; Legacy antivirus and antimalware; SIEM, SOAR, and log management)

References:

Cisco > Products > Security > Cisco Web Security

Question #17 of 54

Question ID: 1322868

Joe created a Sales folder and placed three files in it. He then gave Sally read permission to the folder and gave James write permission to the folder. What type of access control system is in use?

A) ABAC
B) RBAC
C) DAC
D) MAC

Explanation

Discretionary access control (DAC) prescribes that the owner of an asset (data) decides the sensitively of the resource and who has access.

In attribute-based access control (ABAC), attributes and their combinations are used to control access. There are several classes of attributes that might be included.

- Environmental attributes - items such as location, time of day
- Object attributes - object type (medical record, bank account)
- Subject attributes - age, clearance, department, role, job title
- Action attribute - read, delete, view, approve

Role-based access control (RBAC) provides a specific set of rights and permission based on the job role assigned.

The mandatory access control (MAC) model (MAC) provides the strictest control over information access by classifying each asset’s sensitivity with a sensitivity label and controlling access according to the clearance level assigned to users.

Objective:
Security Concepts

Sub-Objective:
Compare access control models (Discretionary access control; Mandatory access control; Nondiscretionary access control; Role-based access control)

References:

Techopedia > Discretionary Access Control (DAC)

Question #18 of 54

Question ID: 1322887

Which of the following would be appropriate for detecting multiple logon failures?

A) rule-based detection
B) anomaly –based detection
C) behavioral-based detection
D) signature-based detection

Explanation

Rule-based detections look for narrowly defined activities such as multiple logon failures rather than looking for behaviors from a list that commonly accompany attacks.

Behavioral detection looks for behavior that typically accompanies an attack. For example, you might monitor the shell history for `unset HISTFILE`, a command that typically only attackers enter after compromising a machine. It is also sometimes called statistical-anomaly based detection.

Signature-based detection looks for something unique to a file (its signature) that can be used to determine if the file is present in the network.

Anomaly –based detection is a technique that creates a profile of normal network traffic and then alerts of any deviation from what it considers to be “normal”.

Objective:
Security Concepts

Sub-Objective:
Compare rule-based detection vs. behavioral and statistical detection

References:

Behavioral monitoring software

Question #19 of 54

Question ID: 1322858

Which of the following is the likelihood that a external security issue might affect an internal weakness?

A) exploit
B) risk
C) breach
D) threat

Explanation

Risk is the likelihood that an external threat will leverage an internal vulnerability.

When a security weakness or vulnerability exists in a system and a threat actor takes advantage of it, the attack is considered an exploit.

A threat is an external danger to which a system may or may not be vulnerable. It is a potential danger that could take advantage of a system if it is vulnerable. An attacker picking the lock of the back entrance to a facility is an example of a threat, not a vulnerability.

A breach is when an exploit is successful in providing unauthorized access to data.

Objective:
Security Concepts

Sub-Objective:
Compare security concepts (Risk (risk scoring/risk weighting, risk reduction, risk assessment); Threat; Vulnerability; Exploit)

References:

Cisco White Papers > The Risk Management Framework: Building a Secure and Regulatory Compliant Trading Architecture (PDF)

Question #20 of 54

Question ID: 1322880

NetFlow records make use of which concept?

A) referrer field
B) 5 tuple
C) urgent pointer
D) acknowledgment number

Explanation

NetFlow records contain five pieces of information called the 5-tuple. They are a unique combination of the following five elements:

- Source IP address
- Destination IP address
- Source port
- Destination port
- Protocol

All communications sharing this same combination are part of the same flow or conversation between two systems.

The urgent pointer is a filed in a TCP header that indicates the first urgent data byte in the packet.

An acknowledgment number is a field in a TCP header that is used to indicate the sequence number of the next byte of data that the sender will receive.

The referrer filed is a field in the HTTP header that t indicates the previous web page from which a request was routed. It is not part of a NetFlow v5 record

Objective:
Security Concepts

Sub-Objective:
Interpret the 5-tuple approach to isolate a compromised host in a grouped set of logs

References:

HYPERLINK "https://www.solarwinds.com/what-is-netflow" SolarWinds > How NetFlow Works

---

Question #21 of 54

Question ID: 1322885

Which of the following looks for evidence of compromise rather than the attack itself?

A) anomaly –based detection
B) signature-based detection
C) rule-based detection
D) behavioral-based detection

Explanation

Behavioral detection looks for behavior that typically accompanies an attack. For example, you might monitor the shell history for `unset HISTFILE`, a command that typically only attackers enter after compromising a machine. It is also sometimes called statistical-anomaly based detection.

Rule-based detections look for narrowly defined activities such as multiple logon failures rather than looking for behaviors from a list that commonly accompany attacks.

Signature-based detection looks for something unique to a file (its signature) that can be used to determine if the file is present in the network.

Anomaly –based detection is a technique that creates a profile of normal network traffic and then alerts of any deviation from what it considers to be “normal”.

Objective:
Security Concepts

Sub-Objective:
Compare rule-based detection vs. behavioral and statistical detection

References:

Behavioral monitoring software

Question #22 of 54

Question ID: 1322867

Which of the following models has as an advantage of stricter control over information access?

A) mandatory access control
B) identity-based access control
C) attribute-based access control
D) discretionary access control

Explanation

While representing the most inflexible model, the mandatory access control (MAC) model provides the strictest control over information access by classifying each asset's sensitivity with a sensitivity label and controlling access according to the clearance level assigned to users.

In attribute-based access control (ABAC), attributes and their combinations are used to control access. There are several classes of attributes that might be included.

- Environmental attributes - items such as location, time of day
- Object attributes - object type (medical record, bank account)
- Subject attributes - age, clearance, department, role, job title
- Action attribute - read, delete, view, approve

Discretionary access control (DAC) prescribes that the owner of an asset (data) decides the sensitively of the resource and who has access.

Identity-based access control is not a valid access control type.

Objective:
Security Concepts

Sub-Objective:
Compare access control models (Discretionary access control; Mandatory access control; Nondiscretionary access control; Role-based access control)

References:

Techopedia > Mandatory Access Control (MAC)

Question #23 of 54

Question ID: 1322882

Which of the following is part of the 5-tuple?

A) NetFlow record ID
B) device name
C) source IP address
D) operating system
E) web software

Explanation

The 5-tuple is a term used to describe the five significant parts of each TCP connection. The five elements that make each conversation unique are:

Source IP address

Destination IP address

Source port number

Destination port number

Protocol

By using the 5-tuple to uniquely identify each communication you can match up data from various sources that refer to the same communication.

Web software in use is not part of the 5-tuple.

In a TCP connection, the source device creates the connection, the TCP three-way handshake occurs, and the destination accepts the connection. This handshake involves three TCP packets. The first packet has the SYN flag set, indicating a desire to make a connection. The destination answers back with a TCP packet with the SYN and ACK flags set, indicating a willingness to create the connection. Finally, the source finalizes the connection with a TCP packet with only the ACK flag set.

Objective:
Security Concepts

Sub-Objective:
Interpret the 5-tuple approach to isolate a compromised host in a grouped set of logs

References:

Packet-Foo > TCP Analysis and the Five-Tuple

Question #24 of 54

Question ID: 1322863

When the facility has a fence, guards, a locked front door and locked interior doors, it called what?

A) defense in depth
B) separation of duties
C) AUP
D) piggybacking

Explanation

A defense in depth strategy prescribes that multiple impediments be presented to a malicious individual. In this case, multiple physical hurdles are presented, but they can also be technical hurdles such as multiple firewalls. Defense in-depth is a multi-layered approach to security that establishes a robust defensive strategy against attackers. This strategy prevents a single attack from being sufficient to breach an environment, forcing attackers to use complex, multi-pronged, daisy-chain attacks that are more likely to fail or be detected during the attempt.

Separation of duties prescribes that any operation susceptible to fraud should be broken into two tasks, with each task given to a different person.

Piggybacking is a social engineering attack in which an unauthorized individual enters a locked door after an authorized individual unlocks the door.

An acceptable use policy defines the manner in which employees are allowed to use a company's network equipment and resources, such as bandwidth, Internet access, and e-mail services.

Objective:
Security Concepts

Sub-Objective:
Describe the principles of the defense-in-depth strategy

References:

US Cert.gov > Defense in Depth

Question #25 of 54

Question ID: 1322878

Which of the following protocols is difficult to monitor due to encryption?

A) HTTPS

B) FTP

C) HTTP

D) Telnet

Explanation

The only protocol listed that is encrypted is HTTPS, the secure form of HTTP. A Web browser is an HTTP client that sends requests to server machines. The browser builds an HTTP request and sends it to the Internet Protocol address indicated by the URL. The HTTP daemon in the destination server machine receives the request and, after any necessary processing, it returns the requested file. HTTP is considered to be unsecure. If you need to protect an HTTP session, consider using HTTPS. HTTPS is a secure form of HTTP that uses Secure Socket Layer (SSL) to encrypt the HTTP messages, while HTTP transmits in clear text.

File Transfer Protocol (FTP) is a standard Internet protocol used to exchange files between computers on the Internet. Like HTTP, which transfers Web pages that can be displayed and related files, FTP is an application protocol that uses TCP/IP protocols. FTP is commonly used to transfer Web page files from a server to others via the Internet. It is also commonly used to download programs and other files to your computer from other servers. FTP works at the Application layer of the OSI model.

Telnet is a terminal emulation protocol. You can use Telnet to establish a remote session with a server and to issue commands on a server. Telnet client software provides you with a text-based interface and a command line from which you can issue commands on a server that supports the Telnet protocol. Telnet will not send notices when network devices have exceeded established performance thresholds. Telnet works at the Application layer of the OSI model.

Objective:
Security Concepts

Sub-Objective:
Identify the challenges of data visibility (network, host, and cloud) in detection

References:

Cloudflare > What Is HTTPS?

Question #26 of 54

Question ID: 1322869

Which vulnerability scoring system uses base, environmental, and temporal scores?

A) OWASP

B) CVSS

C) VERIS

D) NIST

Explanation

The Common Vulnerability Scoring System (CVSS) uses three score values: the base score, the environmental score, and the temporal score. The CVSS assessment measures three areas of concern:

- Base metrics for qualities intrinsic to a vulnerability
- Temporal metrics for characteristics that evolve over the lifetime of vulnerability

- Environmental metrics for vulnerabilities that depend on a particular implementation or environment

The Vocabulary for Event Recording and Incident Sharing (VERIS) is a set of metrics designed to provide a common language for describing security incidents in a structured and repeatable manner. It does not use base, environmental, and temporal metrics. It focuses on five major sections, each designed to capture a different aspect of the incident narrative. When viewed in aggregate, they give the business a tangible idea of cause and severity. The five sections are:

- Incident tracking
- Victim demographics
- Incident description
- Discovery & response
- Impact assessment

While the National Institute of Science and Technology (NIST) creates many security-related guidelines, they do not use base, environmental, and temporal metrics in a scoring system. NIST generates an entire series of Special Publications that are numbered, such as SP 80-200, which is the is FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION regarding Minimum Security Requirements for Federal Information and Information Systems.

The Open Web Application Security Project is nonprofit that provides web security information. It does not use base, environmental, and temporal metrics in a scoring system. One of their more well-known activities is creating a list of the top web vulnerabilities each year.

Objective:
Security Concepts

Sub-Objective:
Describe terms as defined in CVSS (Attack vector; Attack complexity; Privileges required; User interaction; Scope)

References:

First > Common Vulnerability Scoring System SIG

Question #27 of 54

Question ID: 1322888

Which of the following creates many false positives?

A) rule-based detection

B) signature-based detection

C) behavioral-based detection

D) anomaly –based detection

Explanation

Anomaly –based detection is a technique that creates a profile of normal network traffic and then alerts of any deviation from what it considers to be “normal”. This means anytime anything unusual (like a late night maintenance operation) will set off an alert.

Rule-based detections look for narrowly defined activities such as multiple logon failures rather than looking for behaviors from a list that commonly accompany attacks.

Behavioral detection looks for behavior that typically accompanies an attack. For example, you might monitor the shell history for `unset HISTFILE`, a command that typically only attackers enter after compromising a machine. It is also sometimes called statistical-anomaly based detection.

Signature-based detection looks for something unique to a file (its signature) that can be used to determine if the file is present in the network.

Objective:
Security Concepts

Sub-Objective:
Compare rule-based detection vs. behavioral and statistical detection

References:

Behavioral monitoring software

Question #28 of 54

Question ID: 1325261

Which of the following provides the C in CIA?

A) redundancy

B) multiple components

C) hashing

D) encryption

Explanation

CIA stands for Confidentiality, Integrity, and Availability. Confidentiality means preventing unauthorized access to data. One method of doing that is with encryption.

Integrity is a security service that ensures that digital files have not been changed. Digital signatures are an example of an integrity security method. A digital signature provides integrity and non-repudiation. Non-repudiation ensures that the data's origin is known. Availability is a security service that protects hardware and data from loss by ensuring that any needed data is available when necessary. Backups are an example of availability.

Redundancy, or the use of multiple components, increases availability, which is the A in CIA. Redundancy ensures that there are multiple ways to control the static environment. Redundancy occurs when you have additional systems in place that are ready to come online when one system fails.

Hashing algorithms generate hash values that can be compared to identify whether data has changed. Protecting data from unauthorized change provides integrity. Hashing algorithms include MD2, MD4, MD5, HAVAL, and all of the Secure Hash Algorithm (SHA) variants.

Using multiple components is a synonym for redundancy.

Objective:
Security Concepts

Sub-Objective:
Describe the CIA triad

References:

Techopedia > CIA Triad of Information Security

Question #29 of 54

Question ID: 1322851

Which of the following is a compilation of routine procedures and operations that the system administrator or operator carries out?

A) agenda
B) workflow
C) script
D) runbook

Explanation

A runbook is a compilation of routine procedures and operations that the system administrator or operator carries out. The runbook is typically divided into routine automated processes and routine manual processes. The effectiveness of a runbook can be measure by these metrics.

- Mean time to repair (MTTR)
- Mean time between failures (MTBF)
- Mean time to discover a security incident

Mean time between failures (MTBF) is an estimate of the amount of time a piece of equipment will last and is usually determined by the equipment vendor or a third party.

Mean time to repair (MTTR) is an estimate of the amount of time it will take to fix a piece of equipment and return it to production. The owner of the equipment usually determines this amount of time.

An agenda comprises items to be covered in a meeting.

A workflow describes the movement of a piece of work through a process from one operation to another.

While a script may a part of a runbook, not all runbook operations are automated. Some are manual.

Objective:
Security Concepts

Sub-Objective:
Describe security terms (Threat intelligence (TI); Threat hunting; Malware analysis; Threat actor; Run book automation (RBA); Reverse engineering; Sliding window anomaly detection; Principle of least privilege; Zero trust; Threat intelligence platform (TIP)

References:

Wiki > Runbook

Question #30 of 54

Question ID: 1322876

You have discovered a vulnerability to your web service that, if leveraged, would cause the service to be unable to serve up content to the users. Which CVSS metric will increase if this attack is realized?

A) availability
B) integrity
C) complexity
D) confidentiality

Explanation

When a service is rendered unable to do its job, its availability has been decreased, resulting in an increase in the availability metric.

The integrity metric increases when data is changed in the attack.

The confidentiality metric increases when there is a data disclosure or breach.

The complexity metric is a measure of the difficulty of succeeding in the attack.

Attack vector describe the nature of the vulnerability. The new version of CVSS (3.0) set the possible values for the confidentiality, integrity and availability metrics to none, low and high. These are explained below for integrity:

- High (H) - There is a total loss of integrity, or a complete loss of protection. For example, the attacker is able to modify any/all files protected by the impacted component. Alternatively, only some files can be modified, but malicious modification would present a direct, serious consequence to the impacted component.
- Low (L) - Modification of data is possible, but the attacker does not have control over the consequence of a modification, or the amount of modification is constrained. The data modification does not have a direct, serious impact on the impacted component.
- None (N) - There is no loss of integrity within the impacted component.

Objective:
Security Concepts

Sub-Objective:
Describe terms as defined in CVSS (Attack vector; Attack complexity; Privileges required; User interaction; Scope)

References:

First > Common Vulnerability Scoring System SIG

Question #31 of 54

Question ID: 1322856

What term represents the leveraging of a security weakness present in a system?

A) vulnerability

B) breach

C) threat

D) exploit

Explanation

When a security weakness or vulnerability exists in a system and a threat actor takes advantage of it, the attack is considered an exploit.

A vulnerability is a susceptibility to a threat that exists in a system. An example of a vulnerability is keeping ports open for nonessential services.

A threat is an external danger to which a system may or may not be vulnerable. It is a potential danger that could take advantage of a system if it is vulnerable. A hacker is a threat actor. An attacker picking the lock of the back entrance to a facility is an example of a threat, not a vulnerability.

A breach is when an exploit is successful in providing unauthorized access to data.

Objective:
Security Concepts

Sub-Objective:
Compare security concepts (Risk (risk scoring/risk weighting, risk reduction, risk assessment); Threat; Vulnerability; Exploit)

References:

Threat Analysis > Threat, vulnerability, risk – commonly mixed up terms

---

Question #32 of 54

Question ID: 1322864

In which access control model does the owner of the resource decide who has access to the resource?

A) MAC
B) DAC
C) NDAC
D) RBAC

Explanation

Discretionary access control is used when the data owner configures the appropriate permission for each user.

In the mandatory access control model (MAC), a central body assigns a sensitivity label to each document, such as secret, top secret, and so on. Users can access sensitivity levels to which they have been given access. The least privilege principle is most commonly associated with mandatory access control. Under MAC, only an administrator can change the category or classification of a subject or object.

In the non-discretionary access control (NDAC) model, a central body decides which users have access to which documents.

In role-based access control (RBAC), access is based on the job roles to which a user belongs.

Objective:
Security Concepts

Sub-Objective:
Compare access control models (Discretionary access control; Mandatory access control; Nondiscretionary access control; Role-based access control)

References:

Semantic Scholar > Analysis of DAC MAC RBAC Access Control based Models for Security

---

Question #33 of 54

Question ID: 1322849

Which of the following security principles states that any operation susceptible to fraud should be broken into two tasks that are assigned to different people?

A) AUP
B) defense in depth
C) separation of duties
D) piggybacking

Explanation

Separation of duties states that any operation susceptible to fraud should be broken into two or more tasks, with each given to a different person. This principle ensures that tasks are divided between users to ensure that one user cannot commit fraud.

A defense in depth strategy prescribes that multiple impediments be presented to a malicious individual. Multiple physical hurdles may be presented, but it can also use technical hurdles, such as multiple firewalls. Generally, defense-in-depth/layered security means that someone would have to breach multiple safeguards to have access to the entire network. For example, splitting your network into several subnets or VLANs based on departments would prevent a breach to the HR network from affecting the Accounting network.

Piggybacking is a social engineering attack in which an unauthorized individual enters a locked door after another an authorized individual unlocks the door.

An acceptable use policy defines the manner in which employees are allowed to use a company's network equipment and resources, such as bandwidth, Internet access, and e-mail services.

Objective:
Security Concepts

Sub-Objective:
Describe security terms (Threat intelligence (TI); Threat hunting; Malware analysis; Threat actor; Run book automation (RBA); Reverse engineering; Sliding window anomaly detection; Principle of least privilege; Zero trust; Threat intelligence platform (TIP)

References:

CSO > Separation of duties and IT security

Question #34 of 54

Question ID: 1322886

Which of the following is not an example of rule-based detection in Firesight ?

A) Detecting Portscans
B) Preventing Rate-Based Attacks
C) Locating a malicious file
D) Detecting Back Orifice

Explanation

Locating a malicious file is an example of signature-based detection. It operates by looking for something unique to a file (its signature) that can be used to determine if the file is present in the network.

All of the other options utilize rule-based detection using preprocessors. You can use several preprocessors in a network analysis policy to detect specific threats such as Back Orifice attacks, portscans, and rate-based attacks.

Objective:
Security Concepts

Sub-Objective:
Compare rule-based detection vs. behavioral and statistical detection

References:

FireSIGHT System User Guide Version 5.4.1

Question #35 of 54

Question ID: 1322860

What is the process of scoring risks by their likelihood and their impact?

A) quantitative risk analysis

B) qualitative risk analysis

C) disaster recovery plan

D) business impact analysis

Explanation

When scoring is used to rate risks by likelihood and impact, it is called qualitative risk analysis. Qualitative risk analysis does not assign monetary values. It is simply a subjective report that is compiled by the risk analysis team that describes the threats, countermeasures, and likelihood an event will occur.

Quantitative risk analysis attempts to attach dollar figures to potential risk outcomes. Quantitative risk analysis attempts to predict the likelihood a threat will occur and assigns a monetary value in the event a loss occurs. The likelihood of risk occurrence is usually based on subject matter expert opinion and rankings from statistical data.

A business impact analysis (BIA) focuses on critical business systems and the impact if they are lost to an outage. A BIA is created to identify the company's vital functions and prioritize them based on need. It identifies vulnerabilities and threats and calculates the associated risks.

A disaster recovery plan is a short term plan that is implemented when a large disaster event occurs. The plan is created to ensure that your company can resume operations in a timely manner. It mainly focuses on alternative procedures for processing transactions in the short term. It is carried out when the emergency occurs and immediately following the emergency.

Objective:
Security Concepts

Sub-Objective:
Compare security concepts (Risk (risk scoring/risk weighting, risk reduction, risk assessment); Threat; Vulnerability; Exploit)

References:

PMI > Qualitative risk assessment

Question #36 of 54

Question ID: 1322850

Which of the following is an individual behind an exploit?

A) threat source

B) threat actor

C) threat initiator

D) threat vector

Explanation

Threat actors are those who initiate attacks.

Threat vectors are the means used by a threat actor. For example, email might be one threat vector, while a DoS attack might be another.

Threat initiator and threat source are not terms used when discussing risk management.

Objective:
Security Concepts

Sub-Objective:
Describe security terms (Threat intelligence (TI); Threat hunting; Malware analysis; Threat actor; Run book automation (RBA); Reverse engineering; Sliding window anomaly detection; Principle of least privilege; Zero trust; Threat intelligence platform (TIP)

References:

Webopedia > threat actor

Question #37 of 54

Question ID: 1322859

When a threat actor takes advantage of a weakness, it is considered which of the following?

A) threat
B) breach
C) risk
D) exploit

Explanation

When a security weakness or vulnerability exists in a system and a threat actor takes advantage of it, the attack is considered an exploit. An example of a vulnerability is keeping ports open for nonessential services.

Risk is the likelihood that an external threat leverages an internal vulnerability.

A threat is an external danger to which a system may or may not be vulnerable. It is a potential danger that could take advantage of a system if it is vulnerable.

A breach occurs when an exploit is successful in providing unauthorized access to data.

Objective:
Security Concepts

Sub-Objective:
Compare security concepts (Risk (risk scoring/risk weighting, risk reduction, risk assessment); Threat; Vulnerability; Exploit)

References:

Threat Analysis > Threat, vulnerability, risk – commonly mixed up terms

---

Question #38 of 54

Question ID: 1322838

When encryption is not provided, which tenet of the CIA triad might be violated?

A) Confidentiality
B) Accountability
C) Availability

D) Authentication

Explanation

The confidentiality or the C in CIA might be violated. Unencrypted data may be caught and read by unauthorized persons.

CIA stands for Confidentiality, Integrity and Availability. Confidentiality means preventing unauthorized access to data. One method of doing that is with encryption. Integrity is a security service that ensures that digital files have not been changed. Digital signatures are an example of an integrity security method. A digital signature provides integrity and non-repudiation. Non-repudiation ensures that the data's origin is known. Availability is a security service that protects hardware and data from loss by ensuring that any needed data is available when necessary. Backups are an example of availability.

Authentication is not part of the CIA triad. It is part of an AAA service. Authentication, authorization, and accounting (AAA) is a term for controlling access to computer resources using authentication, enforcing policies using authorization, and auditing usage and providing the information necessary to bill for services using accounting.

Accountability is not part of the CIA triad. It is part of an AAA service.

Availability would not be violated because lack of encryption does not put the availability of the resource in danger.

Objective:
Security Concepts

Sub-Objective:
Describe the CIA triad

References:

TechRepublic > The CIA Triad

Question #39 of 54

Question ID: 1322848

Which of the following is a system that aggregates and analyzes security logs in real time for malicious activity?

A) NIDS
B) SIEM
C) antivirus
D) NIPS

Explanation

A security incident and event management system (SIEM) aggregates and analyzes security logs in real time for malicious activity. Aggregation is a SIEM feature that allows the collection of various events that are flagged by network hardware and software applications.

Correlation is a SIEM feature that looks for similarities in events that are collected from different devices. Correlation allows the analyst to examine seemingly unique events and determine the patterns between them.

Automated alerting and triggers are a SIEM feature that allow the system to react based on predetermined criteria. Alerts include one or more systems that notify an administrator when a predetermined event occurs. Triggers take it a step further, and respond to the event with a series of programmed actions. As an example, an NIPS can shut down port 80 when an unusually high amount of web traffic floods the network.

Antivirus programs detect and remove unwanted malicious software from a system.

A network intrusion detection system (NIDS) is a system that operated on the network and detects attacks on that network.

A network intrusion prevention system (NIPS) is a system that operated on the network and detects attacks on that network while also taking actions to stop the attack.

Intrusion prevention systems (IPS) and intrusion detection systems (IDS) work together to complement each other. IPS systems can block activities on certain Web sites. Users may be allowed to access the sites but may be prevented from accessing certain features within the site. In other cases, the entire site may be blocked, depending on the security requirements for the organization.

Objective:
Security Concepts

Sub-Objective:
Compare security deployments (Network, endpoint, and application security systems; Agentless and agent-based protections; Legacy antivirus and antimalware; SIEM, SOAR, and log management)

References:

TripWire > What Is a SIEM?

Question #40 of 54

Question ID: 1322874

Which of the following represents the metric values available for the integrity metric?

A) none, low, and high

B) none and required

C) low and high

D) none, partial, and complete

Explanation

The new version of CVSS (3.0) set the possible values for the confidentiality, integrity and availability metrics to none, low and high. These are explained below:

- High (H) - There is a total loss of integrity, or a complete loss of protection. For example, the attacker is able to modify any/all files protected by the impacted component. Alternatively, only some files can be modified, but malicious modification would present a direct, serious consequence to the impacted component.
- Low (L) - Modification of data is possible, but the attacker does not have control over the consequence of a modification, or the amount of modification is constrained. The data modification does not have a direct, serious impact on the impacted component.
- None (N) - There is no loss of integrity within the impacted component.

Prior to version 3.0 of CVSS, the possible values for these metrics were none, partial, and complete.

Low and high are values for attack complexity, which has replaced access complexity in version 3.0. Attack complexity measures the difficulty of the attack and has two possible values:

- Low (L) - the attacker can perform the attack at will
- High (H) - the attack depends on conditions beyond the control of the attacker.

None and required are values for user interaction, a new metric with version 3, which measures the extent to which the user must assist an attack. It has two possible values:

- None (N) - attack can be accomplished with no user interaction

- Required (R) - successful attack requires user interaction

None, partial, and complete are not a set of values used in the CVSS system.

Objective:
Security Concepts

Sub-Objective:
Describe terms as defined in CVSS (Attack vector; Attack complexity; Privileges required; User interaction; Scope)

References:

First > Common Vulnerability Scoring System SIG

Question #41 of 54

Question ID: 1322872

Which CVSS version 3.0 metric measures the extent to which the user must assist an attack?

A) attack complexity

B) user interaction

C) privileges required

D) attack vector

Explanation

User interaction, a new metric in version 3 of CVSS, measures the extent to which the user must assist an attack. It has two possible values:

- None (N) - attack can be accomplished with no user interaction
- Required (R) - successful attack requires user interaction

Privileges required is another new metric with version 3. Privileges required measures the access level required for the attack. It has three possible values:

- None (N) - attacker need not be authorized
- Low (L) - attacker needs user level access
- High (H) - attacker needs admin or system level access

Attack complexity has replaced access complexity in version 3.0, and measures the difficulty of the attack. It has two possible values:

- Low (L) - the attacker can perform the attack at will
- High (H) - the attack depends on conditions beyond the control of the attacker.

The Common Vulnerability Scoring System (CVSS) captures principal characteristics of a vulnerability and produces a numerical score that reflects its severity. This score can also be expressed as a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

Attack vector is a base metric that describes the nature of the vulnerability. There are three CVSS base metrics as follows:

- Access Vector - The access vector (AV) shows how a vulnerability may be exploited.
- Attack Complexity - The attack complexity (AC) metric describes how easy or difficult it is to exploit the discovered vulnerability.

- Authentication - The authentication (Au) metric describes the number of times that an attacker must authenticate to a target to exploit it.

Objective:
Security Concepts

Sub-Objective:
Describe terms as defined in CVSS (Attack vector; Attack complexity; Privileges required; User interaction; Scope)

References:

First > Common Vulnerability Scoring System SIG

Question #42 of 54

Question ID: 1322865

Your organization uses both the user's location and the time of day when assessing a connection request. What type of access control model is this?

A) DAC
B) MAC
C) ABAC
D) RBAC

Explanation

This is an example of attribute-based access control (ABAC). In this model, attributes and their combinations are used to control access. There are several classes of attributes that might be included:

- Environmental attributes - items such as location, time of day
- Object attributes - object type (medical record, bank account)
- Subject attributes - age, clearance, department, role, job title
- Action attribute - read, delete, view, approve

Role-based access control (RBAC) provides a specific set of rights and permission based on the job role assigned to the user.

Discretionary access control (DAC) prescribes that the owner of an asset (data) decides the sensitively of the resource and who has access.

Mandatory access control (MAC) creates clearance levels and assigns clearance levels to data assets and to users. Subjects (users) can only access levels to which they have been given clearance and those below.

Objective:
Security Concepts

Sub-Objective:
Compare access control models (Discretionary access control; Mandatory access control; Nondiscretionary access control; Role-based access control)

References:

CSRC > Attribute Based Access Control

Question #43 of 54

Question ID: 1322879

Which of the following represents a step in the second normal form in the process of normalization?

A) Create a separate table for each set of related data.

B) Eliminate fields that do not depend on the key.

C) Eliminate repeating groups in individual tables.

D) Create separate tables for sets of values that apply to multiple records.

Explanation

The process of data normalization can have up to five or more normal forms, but IPS systems typically only utilize the first three.

The first normal form (1NF) involves:

- Eliminating repeating groups in individual tables
- Creating a separate table for each set of related data
- Identifying each set of related data with a primary key

The second normal form (2NF) includes:

- Creating separate tables for sets of values that apply to multiple records
- Relating these tables with a foreign key

Eliminating repeating groups in individual tables is the only step in the third normal form (3NF).

Objective:
Security Concepts

Sub-Objective:
Identify potential data loss from provided traffic profiles

References:

HelpNet Security > The importance of data normalization in IPS

Microsoft Docs > Office > Access > Description of the database normalization basics

---

Question #44 of 54

Question ID: 1322847

Which of the following is a security product that collects, normalizes, and correlates event log data to provide a holistic view of the security posture?

A) Syslog

B) SIEM

C) IPS

D) IDS

Explanation

A security information and events management (SIEM) solution is a product that collects normalizes and correlates event log data to provide a holistic view of the security posture.

An intrusion prevention system (IPS) is one that can not only detect malicious activity but also take actions to stop it.

An intrusion detection system (IPS) is one that can detect malicious activity and alert technicians.

A syslog system can centralize logs, but not normalize and correlate event log data to provide a holistic view of the security posture. A syslog server receives and stores log messages sent from syslog clients. A syslog client sends logging information to a syslog server. A syslog server ensures that a network administrator can review device error information from a central location.

Objective:
Security Concepts

Sub-Objective:
Compare security deployments (Network, endpoint, and application security systems; Agentless and agent-based protections; Legacy antivirus and antimalware; SIEM, SOAR, and log management)

References:

TripWire > What Is a SIEM?

Question #45 of 54

Question ID: 1322877

OpenDNS is a Cisco security solution designed to protect which component?

A) Cloud

B) WAN

C) DMZ

D) LAN

Explanation

OpenDNS is a company and service that hosts a cloud computing security product suite, Umbrella. OpenDNS's business services were renamed as Cisco Umbrella; home products retained the OpenDNS name. It also offers DNS resolution as an alternative to using Internet service providers' DNS servers or locally installed DNS servers.

Other services offered for cloud protection by Cisco include Cloud lock.

While other products exist for LAN, WAN and DMZ, the Umbrella feature is not one of them.

A local area network (LAN) covers a small geographic area. Typically, a LAN is confined to a campus, a single building, a floor of a building, or an area with in a building.

A wide area network (WAN) uses routers (or a collection of routers) to connect LANs that are dispersed over a large geographic area. An example would be a company with office locations in Boston, Miami, Chicago, Dallas, Denver, and San Francisco. Each office has its own LAN, and routers are used to provide connections between the offices. By building the WAN, the offices can share resources and data.

Objective:
Security Concepts

Sub-Objective:
Identify the challenges of data visibility (network, host, and cloud) in detection

References:

Cisco > OpenDNS

Question #46 of 54

Question ID: 1322881

Which of the following is NOT one of the five tuples?

A) source IP address

B) destination IP address

C) source port number

D) device name

Explanation

The 5-tuple is a term used to describe the five significant parts of each TCP connection. The five elements which make each conversation unique are:

- Source IP address
- Destination IP address
- Source port number
- Destination port number
- Protocol

By using the 5-tuple to uniquely identify each communication, you can map data from various sources that refer to the same communication.

In a TCP connection, the source device creates the connection, the TCP three-way handshake occurs, and the destination accepts the connection. This handshake involves three TCP packets. The first packet has the SYN flag set, indicating a desire to make a connection. The destination answers back with a TCP packet with the SYN and ACK flags set, indicating a willingness to create the connection. Finally, the source finalizes the connection with a TCP packet with only the ACK flag set.

Device name is not one of the five tuples.

Objective:
Security Concepts

Sub-Objective:
Interpret the 5-tuple approach to isolate a compromised host in a grouped set of logs

References:

Packet-Foo > TCP Analysis and the Five-Tuple

Question #47 of 54

Question ID: 1322866

A newly hired help desk technician is placed in the Help Desk security group. The user thereby inherits five permissions. What type of access control model is this?

A) MAC

B) ABAC

C) DAC

D) RBAC

Explanation

Role-based access control (RBAC) provide a specific set of rights and permission based on the job role assigned to a user.

In attribute-based access control (ABAC), attributes and their combinations are used to control access. There are several classes of attributes that might be included.

- Environmental attributes - items such as location, time of day
- Object attributes - object type (medical record, bank account)
- Subject attributes - age, clearance, department, role, job title
- Action attribute - read, delete, view, approve

Discretionary access control (DAC) prescribes that the owner of an asset (data) decides the sensitively of the resource and who has access.

Mandatory access control (MAC) creates clearance levels and assigns clearance levels to data assets and to users. Subjects (users) can only access levels to which they have been given clearance and those below.

Objective:
Security Concepts

Sub-Objective:
Compare access control models (Discretionary access control; Mandatory access control; Nondiscretionary access control; Role-based access control)

References:

Digital Guardian > What is Role-Based Access Control (RBAC)? Examples, Benefits, and More

---

Question #48 of 54

Question ID: 1322853

Which of the following is based on a well-known technique for approximated queries that update their results continuously as new fresh data arrives from the stream?

A) heuristics

B) reverse engineering

C) signature based recognition

D) sliding window anomaly detection

Explanation

Sliding window anomaly detection uses a process called sliding windows semantics to update their results continuously as new fresh data arrive from the stream, thus making attack or anomaly detection more accurate.

Heuristics is an approach that identifies malware based on the behavior it exhibits rather than a signature. A heuristic IDS uses artificial intelligence (AI) to detect intrusions. Analytics are performed on the actions taken, and the IDS takes action based on the logic in the AI.

Signature based recognition is a malware detection method based on the detection tool possessing the identifying signature of the malware. Signature-based monitoring relies upon a database that contains the identities of possible attacks. This database is known as the signature database. Signature-based monitoring watches for intrusions that match a known identity or signature. Signature-based monitoring requires that updates be regularly obtained to ensure effectiveness.

Reverse engineering is the breaking down of an attack into its parts to understand how it happened. It may even involve reverse engineering the software involved in the attack to determine its purpose.

Objective:
Security Concepts

Sub-Objective:
Describe security terms (Threat intelligence (TI); Threat hunting; Malware analysis; Threat actor; Run book automation (RBA); Reverse engineering; Sliding window anomaly detection; Principle of least privilege; Zero trust; Threat intelligence platform (TIP)

References:

Research Gate > Network traffic anomaly detection based on sliding window

---

Question #49 of 54

Question ID: 1322843

Which tool can be used to detect data loss?

A) CTD
B) ESA
C) ASA
D) WSA

Explanation

Cisco Cyber Threats Dashboard (CTD) can capture and analyze historical data about network flows, and use the data to create a baseline for the network. It continually monitors flows and compares them to baseline parameters to determine whether data loss event has occurred.

Adaptive Security Appliance (ASA) is a firewall product. It does not capture and analyze historical data about network flows, and use the data to create a baseline for the network. It is used to control the flow of traffic from one network to another.

Cisco Web Security Appliance (WSA), powered by Cisco Talos, protects you by automatically blocking risky sites and testing unknown sites before allowing users to link to them. Web Security can be run on an appliance, as a virtual machine, and even on a branch router. It is a form of web application firewall.

The Cisco Email Security Appliance is an email security tool. It protects against phishing email attacks such as ransomware and analyzes emails for threats such as zero-day exploits and attacks hidden in attachments and malicious URLs.

Objective:
Security Concepts

Sub-Objective:
Compare security deployments (Network, endpoint, and application security systems; Agentless and agent-based protections; Legacy antivirus and antimalware; SIEM, SOAR, and log management)

References:

Cisco > td > docs > solutions > Enterprise > Data_Center > VMDC > Cloud_Security > 1-0 > DG > Cisco Cloud Security 1.0, Design Guide > Chapter: End-To-End Visibility

---

Question #50 of 54

Question ID: 1322883

Which of the following is NOT one of the 5 tuple?

A) source IP address

B) source port number

C) netflow record ID

D) destination IP address

Explanation

The NetFlow ID appears in the NetFlow header when using NetFlow to capture what is called a flow. This comprises all packets that are part of the same conversation as defined by the 5-tuple that all packets share. However, the NetFlow ID is not one of the five tuples.

By using the 5-tuple to uniquely identify each communication you can match up data from various sources that refer to the same communication.

The 5 tuple is a term used to describe the 5 significant parts of each TCP connection. These 5 elements which make each conversation unique are:

- Source IP address
- Destination IP address
- Source port number
- Destination port number
- Protocol

The source device creates the connection and the destination accepts the connection following the TCP three-way handshake. This handshake involves three TCP packets. The first packet has the SYN flag set, indicating a desire to make a connection. The destination answers back with a TCP packet with the SYN and ACK flags set, indicating a willingness to create the connection. Finally, the source finalizes the connection with a TCP packet with only the ACK flag set.

Objective:
Security Concepts

Sub-Objective:
Interpret the 5-tuple approach to isolate a compromised host in a grouped set of logs

References:

Packet-Foo > TCP Analysis and the Five-Tuple

Question #51 of 54

Question ID: 1322862

Which of the following concepts is illustrated by network segmentation, air-gaps, multiple firewalls, and virtualization?

A) Vendor diversity

B) Defense-in-depth

C) Control diversity

D) None of the above

Explanation

Network segmentation, air gaps, multiple firewalls, and virtualization are all examples of defense-in-depth, also referred to as layered security. Generally, defense-in-depth/layered security means that someone would have to breach multiple

safeguards to have access to the entire network. For example, splitting your network into several subnets or VLANs based on departments would prevent a breach to the HR network from affecting the Accounting network. Air gapping refers to completely isolating a vulnerable device from the rest of the network. Vendor diversity means that you are using several suppliers, primarily to isolate vulnerabilities or minimize errors. No single security system is all-encompassing. What is missed by Vendor X is often caught by Vendor Y. Vendor diversity does not ensure air-gapping or network segmentation are implemented in your network.

Control diversity means that you are not relying on one single security mechanism. Control diversity can be further classified as administrative controls, physical controls, and technical controls. Administrative controls are policies and procedures, such as not opening ZIP files attached to emails. Physical controls include locks and fencing and provide physical protection for your facilities and assets. Technical controls include such things as IDS/IPS, firewalls and antimalware. Typically, administrative and technical controls work best when they work together, rather than independently. Control diversity is one aspect of defense-in-depth but does not cover all layers of a defense-in-depth strategy.

In any organization, user training is a paramount concern. The best administrative and technical controls are useless if a user is not trained on how to identify user-targeted attacks, such as phishing emails and suspicious attachments.

Objective:
Security Concepts

Sub-Objective:
Describe the principles of the defense-in-depth strategy

References:

CompTIA Security+ Deluxe Study Guide: SY0-501. Chapter 2: Monitoring and Diagnosing Networks

---

Question #52 of 54

Question ID: 1325262

Which of the following is NOT a reason why it is difficult to obtain visibility on security in the cloud?

A) Cloud-based assets tend to be more short-lived than on-premises IT assets.

B) Traditional security controls reflect the security needs of the static data center, not cloud data centers.

C) Security solutions for the cloud are more costly than for on-premises IT assets.

D) Cloud environments are inherently complex.

Explanation

Security solutions for cloud are not more costly than for on-premises IT assets, and in many cases are included as part of the cloud service. The issue becomes what is visible to your tools in the cloud environment.

The other statements reflect reasons why it might be more difficult to obtain visibility into cloud security.

Cloud environments are inherently complex. What with public, private, hybrid, and other types of clouds, understanding your environment is more difficult than with an on-premises based network.

Traditional, familiar security controls that might be applied to the cloud reflect the security needs of the static data center, not the cloud data center. For example, not all hypervisors may be compatible with all monitoring tools, and as a result, the network security professional might require multiple overlapping tools to achieve a clear picture.

Finally, cloud-based assets tend to be more short-lived than traditional IT assets. An example of a short-lived cloud asset includes an AWS Lambda function invoked by a trigger to execute a specific task. Services and virtual machines are dynamically added and removed as the cloud workload scales up and down. As a result of such constant change, it

is difficult to keep track of everything that's connected to the network over a period of time and achieve complete network visibility.

Objective:
Security Concepts

Sub-Objective:
Identify the challenges of data visibility (network, host, and cloud) in detection

References:

Network visibility challenges in modern networks

Question #53 of 54

Question ID: 1322839

What type of tool or system is typically required to accept data in multiple semantics and convert it to a common format?

A) SIEM
B) VERIS
C) SYSLOG
D) NAC

Explanation

Security Incident and Event Management (SIEM) tools, such as Splunk, can interpret common data values into a universal format. They accept input from IPS devices, firewalls, NetFlow generating devices, servers, endpoints, and syslogs from infrastructure devices.

Network Access Control (NAC) systems validate the health of remote system before allowing them access to the network. It does not accept data streams from multiple sources and convert them to a common format.

Syslog is a service that centralizes log files. However, it does not aggregate them or interpret common data values into a universal format

Vocabulary for Event Recording and Incident Sharing (VERIS) is a common language for describing security incidents in a structured and repeatable manner. While VERIS provides vital specifications for describing data events in a common format, it is a schema and not a tool or system.

Objective:
Security Concepts

Sub-Objective:
Compare security deployments (Network, endpoint, and application security systems; Agentless and agent-based protections; Legacy antivirus and antimalware; SIEM, SOAR, and log management)

References:

Imperva > Security information and event management (SIEM)

Question #54 of 54

Question ID: 1322884

How are connections differentiated in a traditional stateful firewall?

A) by source and destination IP address, source and destination MAC address, and transport protocol

B) by source and destination IP address and source and destination MAC address

C) by source IP address

D) by source IP address and source MAC address

Explanation

A traditional stateful firewall differentiates connections based on the TCP 5 tuple, which consists of:

- source IP address
- destination IP address
- source MAC address
- destination MAC address
- transport protocol

Stateful firewalls monitor the state of each TCP connection. When traffic is encountered, a stateful firewall first examines a packet to see if it is the result of a previous connection. Information about previous connections is maintained in the state table. A packet is allowed if it is a response to a previous connection. If the state table holds no information about the packet, the packet is compared to the access control list (ACL). Depending on the ACL, the packet will be forwarded to the appropriate host or dropped completely.

Stateful firewalls can be used to track connectionless protocols, such as the User Datagram Protocol (UDP), because they examine more than the packet header.

Among the tasks that can be performed by analyzing the logs of a traditional stateful firewall are:

- Confirming the timing of network connections
- Auditing the applications used with a social networking web site

Objective:
Security Concepts

Sub-Objective:
Interpret the 5-tuple approach to isolate a compromised host in a grouped set of logs

References:

CiscoExpert > Stateful Inspection