PDFVCE

Choose the version that fits your needs	PDF Version	Desktop Test Engine	Online Test Engine
Latest and Up-to-Date exam dumps with real exam questions answers.	✓	✓	✓
Get 12-Months free updates without any extra charges.	✓	✓	✓
Experience same exam environment before appearing in the certification exam.	✗	✓	✓
100% exam passing guarante in the first attempt.	✓	✓	✓
20% discount on more than one license and 30% discount on 5+ license purchases.	✗	✓	✓
100% secure purchase on SSL.	✓	✓	✓
Completely private purchase without sharing your personal info with anyone.	✓	✓	✓

Exam : **212-82-JPN**

Title : Certified Cybersecurity Technician (212-82日本語版)

Vendor : ECCouncil

Version : DEMO

QUESTION NO: 1
セキュリティ専門家の Malachi
氏は、受信トラフィックと送信トラフィックを追跡するために組織内にファイアウォールを実装しました。彼は、OSI モデルのセッション層で動作し、ホスト間の TCP
ハンドシェイクを監視して、要求されたセッションが正当かどうかを判断するファイアウォールを導入しました。
上記のシナリオで Malachi によって実装されたファイアウォール テクノロジを特定します。
A. 次世代ファイアウォール (NGFW)
B. 回線レベルゲートウェイ
C. ネットワークアドレス変換 (NAT)
D. パケットフィルタリング
Answer: B
Explanation:
A circuit-level gateway is a type of firewall that works at the session layer of the OSI model and monitors the TCP handshake between hosts to determine whether a requested session is legitimate. It does not inspect the contents of each packet, but rather relies on the session information to filter traffic

QUESTION NO: 2
次のどれが物理的なセキュリティ管理の例ですか?
(該当するものをすべて選択してください)
A. 警備員
B. ファイアウォール
C. 生体認証アクセス制御
D. 暗号化アルゴリズム
Answer: AC

QUESTION NO: 3
攻撃者のマシン I のダウンロード フォルダーにある実行可能ファイル ShadowByte.exe を分析し、ファイルのリンカー情報の値を特定します。(実践的な質問)
A. 04.25
B. 2.25
C. 3.5
D. 6.2
Answer: B

QUESTION NO: 4
ネットワークに接続されたマシンの 1 つに RAT
が設定されており、サーバーのデスクトップにある重要な機密企業文書を盗みます。さらに調査すると、サーバーの IP アドレスが 20.20.10.26 であることが判明しました。Thief
クライアントを使用してリモート接続を開始し、フォルダー内に存在するファイルの数を確認します。
ヒント: Thief フォルダーは次の場所にあります: Z:\CCT-Tools\CCT Module 01 Information

Security Threats and Vulnerabilities\Remote Access Trojans (RAT)\Thief of Attacker Machine-1。

A. 2

B. 4

C. 3

D. 5

Answer: C

Explanation:

3 is the number of files present in the folder in the above scenario. A RAT (Remote Access Trojan) is a type of malware that allows an attacker to remotely access and control a compromised system or network. A RAT can be used to steal sensitive data, spy on user activity, execute commands, install other malware, etc. To initiate a remote connection using thief client, one has to follow these steps:

Navigate to the thief folder located at Z:\CCT-Tools\CCT Module 01 Information Security Threats and Vulnerabilities\Remote Access Trojans (RAT)\Thief of Attacker Machine-1.

Double-click on thief.exe file to launch thief client.

Enter 20.20.10.26 as IP address of server.

Enter 1234 as port number.

Click on Connect button.

After establishing connection with server, click on Browse button.

Navigate to Desktop folder on server.

Count number of files present in folder.

The number of files present in folder is 3, which are:

Sensitive corporate docs.docx

Sensitive corporate docs.pdf

Sensitive corporate docs.txt

QUESTION NO: 5

ライリーはルイに秘密のメッセージを送信しました。メッセージを送信する前に、ライリーは自分の秘密鍵を使用してメッセージにデジタル署名しました。ルイはメッセージを受信し、対応する鍵を使用してデジタル署名を検証し、メッセージが送信中に改ざんされていないことを確認しました。

上記のシナリオでルイがデジタル署名を検証するために使用したキーは次のどれですか?

A. ライリーの公開鍵

B. ルイの公開鍵

C. ライリーの秘密鍵

D. ルイの秘密鍵

Answer: A

Explanation:

Riley's public key is the key that Louis used to verify the digital signature in the above scenario. A digital signature is a cryptographic technique that verifies the authenticity and integrity of a message or document. A digital signature is created by applying a hash function to the message or document and then encrypting the hash value with the sender's private key. A digital signature can be verified by decrypting the hash value with the sender's public

key and comparing it with the hash value of the original message or document.Riley's public key is the key that corresponds to Riley's private key, which he used to sign the message.
Louis's public key is the key that corresponds to Louis's private key, which he may use to encrypt or decrypt messages with Riley.
Louis's private key is the key that only Louis knows and can use to sign or decrypt messages.
Riley's private key is the key that only Riley knows and can use to sign or encrypt messages.

QUESTION NO: 6
組織のネットワーク管理者である Jordan
は、ネットワーク関連の問題を特定し、ネットワーク
パフォーマンスを改善するように指示されました。ネットワークのトラブルシューティング中に、ターゲット ホストで IP 関連サービス (FTP や Web サービスなど)
が利用できないためにデータグラムを転送できないことを示すメッセージを受け取りました。このシナリオで Jordan が見つけたネットワークの問題は次のどれですか。
A. 時間超過メッセージ
B. 宛先に到達できないメッセージ
C. 到達不可能なネットワーク
D. ネットワークケーブルが接続されていません
Answer: B
Explanation:
Destination unreachable message is the network issue that Jordan found in this scenario.
Destination unreachable message is a type of ICMP message that indicates that the datagram could not be forwarded owing to the unavailability of IP-related services (such as FTP or web services) on the target host. Destination unreachable message can be caused by various reasons, such as incorrect routing, firewall blocking, or host configuration problems.

QUESTION NO: 7
犯罪捜査官のルーベンは、元のファイルに影響を与えずに、疑わしいメディア内の削除されたファイルとフォルダーをすべて取得したいと考えています。この目的のために、彼はメディア全体のクローン コピーを作成し、元のメディアの汚染を防ぐ方法を使用します。
上記のシナリオで Ruben が使用した方法を特定します。
A. スパース獲得
B. ビットストリームイメージング
C. ドライブの復号化
D. 論理的獲得
Answer: B
Explanation:
Bit-stream imaging is the method utilized by Ruben in the above scenario. Bit-stream imaging is a method that involves creating a cloned copy of the entire media and prevents the contamination of the original media. Bit-stream imaging copies all the data on the media, including deleted files and folders, hidden partitions, slack space, etc., at a bit level. Bit-stream imaging preserves the integrity and authenticity of the digital evidence and allows further analysis without affecting the original media. Sparse acquisition is a method that involves creating a partial copy of the media by skipping empty sectors or blocks. Drive

decryption is a method that involves decrypting an encrypted drive or partition using a password or a key. Logical acquisition is a method that involves creating a copy of the logical files and folders on the media using file system commands.

QUESTION NO: 8
攻撃者は、ping-of-death (PoD) 技術を使用して、対象の Android
デバイスをクラッシュさせました。ネットワーク トラフィックは SOC
チームによってキャプチャされ、詳細な分析を実行するために提供されました。攻撃者のマシン 2 のドキュメント フォルダーにある android.pcapng ファイルを分析し、PoD
パケットの長さ (バイト単位) を特定します。(実践的な質問)
A. 52
B. 056
C. 58
D. 54
Answer: D

QUESTION NO: 9
あるソフトウェア会社は、従業員の出勤と退勤の時間を記録して勤怠を追跡するワイヤレス技術を導入しました。同社の各従業員は、タグが埋め込まれた入場カードを所持しています。従業員がオフィスの敷地内に入るときはいつでも、入り口でカードをスワイプする必要があります。ワイヤレス技術は、自動識別と物体に取り付けられたタグの追跡のために、無線周波数の電磁波を使用してデータを転送します。
上記のシナリオでソフトウェア会社が実装したテクノロジは次のどれですか?
A. WiMAX
B. RFID
C. ブルートゥース
D. Wi-Fi
Answer: B
Explanation:
RFID (Radio Frequency Identification) is the wireless technology that the software company has implemented in the above scenario. RFID uses radio-frequency electromagnetic waves to transfer data for automatic identification and for tracking tags attached to objects. WiMAX (Worldwide Interoperability for Microwave Access) is a wireless technology that provides high- speed broadband access over long distances. Bluetooth is a wireless technology that enables short-range data communication between devices, such as phones, laptops, printers, etc. Wi-Fi (Wireless Fidelity) is a wireless technology that allows devices to connect to a local area network or the internet using radio waves.

QUESTION NO: 10
ソフトウェア会社は、安全なアプリケーション開発のベスト
プラクティスに従って、新しいソフトウェア製品を開発しています。ソフトウェア
アナリストの Dawson
は、クライアントのネットワーク内のアプリケーションのパフォーマンスをチェックし、エンド
ユーザーがアプリケーションにアクセスする際に直面する問題を特定する責任を負っていま

す。
安全なアプリケーション開発ライフサイクルの次のどの層でアプリケーションのパフォーマンスのチェックが必要ですか?
A. 開発
B. ステージング
C. テスト
D. 品質保証 (QA)
Answer: C
Explanation:
Testing is the tier of the secure application development lifecycle that involves checking the application performance in the above scenario. Secure application development is a process that involves designing, developing, deploying, and maintaining software applications that are secure and resilient to threats and attacks. Secure application development can be based on various models or frameworks, such as SDLC (Software Development Life Cycle), OWASP (Open Web Application Security Project), etc. Secure application development consists of various tiers or stages that perform different tasks or roles. Testing is a tier of the secure application development lifecycle that involves verifying and validating the functionality and security of software applications before releasing them to end users. Testing can include various types of tests, such as unit testing, integration testing, system testing, performance testing, security testing, etc.
Testing can be used to check the application performance and identify any errors, bugs, or vulnerabilities in the software applications. In the scenario, a software company develops new software products by following the best practices for secure application development. Dawson, a software analyst, is responsible for checking the performance of applications in the client's network to determine any issue faced by end users while accessing the application. This means that he performs testing for this purpose. Development is a tier of the secure application development lifecycle that involves creating and coding software applications according to the design and specifications. Staging is a tier of the secure application development lifecycle that involves deploying software applications to a simulated or pre-production environment for testing or evaluation purposes. Quality assurance (QA) is a tier of the secure application development lifecycle that involves ensuring that software applications meet the quality standards and expectations of end users and stakeholders

QUESTION NO: 11
病院の安全対策として設置されたIoTデバイスがサーバーにアラートを送信しました。ネットワークトラフィックがキャプチャされ、「攻撃者マシン」のドキュメントフォルダに保存されました。
1. IoTdeviceTraffic.pcapng ファイルを分析し、IoT
デバイスがネットワーク経由で送信したコマンドを特定します。
A. Tempe_Low
B. Low_Tem p e
C. High_Tcmpe
D. Temp_High
Answer: D

Explanation:
The IoT device sent the command Temp_High over the network, which indicates that the temperature in the hospital was above the threshold level. This can be verified by analyzing the IoTdeviceTraffic.pcapng file using a network protocol analyzer tool such as Wireshark. The command Temp_High can be seen in the data field of the UDP packet sent from the IoT device (192.168.0.10) to the server (192.168.0.1) at 12:00:03.

QUESTION NO: 12
大手銀行機関である Alpha Finance は、新しいモバイル バンキング
アプリを立ち上げています。機密性の高い金融データが扱われることから、アプリケーションが最善のセキュリティ
プラクティスに準拠していることを保証したいと考えています。主な推奨事項として、Alpha Finance が優先すべきガイドラインは何ですか。
A. アプリ内にウイルス対策を埋め込む
B. ユーザーログインに多要素認証 (MFA) を採用する
C. 安全な取引のためにアプリ内VPNを提供する
D. ユーザーにOSの最新バージョンへのアップデートを促す
Answer: B

QUESTION NO: 13
ステルス性と高度な技術で知られる APT (Advanced Persistent Threat)
グループが、大手ソフトウェア開発会社を標的にしました。この攻撃は、数か月にわたって綿密に計画され、実行されました。アプリケーション レベルとオペレーティング システム レベルの両方で脆弱性が悪用されました。この攻撃により、機密ソース
コードが抽出され、開発業務が中断されました。事後分析により、フィッシング、ソフトウェア/ハードウェアの未知/未修正の脆弱性の悪用、ネットワーク内での横方向の移動など、複数の攻撃ベクトルが明らかになりました。この攻撃の性質と実行方法を考慮すると、攻撃者がこの APT を開始するために使用した主な方法は何ですか?
A. デフォルトのパスワードを悪用してネットワークへの初期アクセスを取得します。
B. 開発者が使用するアプリケーションのゼロデイ脆弱性を悪用します。
C. ファイアウォールの既知の脆弱性を悪用してネットワーク防御を回避します。
D. 会社の開発環境へのアクセス権を持つサードパーティベンダーを侵害する。
Answer: B

QUESTION NO: 14
ターゲットウェブサーバーでホストされているウェブアプリケーション（www.moviescope.com）は、SQLインジェクション攻撃に対して脆弱です。このウェブアプリケーションを悪用し、moviescopeデータベースからユーザー認証情報を抽出してください。データベース内のユーザー「John」のUID（ユーザーID）を特定してください。注：あなたはこのウェブアプリケーションにアカウントを持っており、認証情報も一致しています。
A. 3
B. 4
C. 2
D. 5

Answer: B
Explanation:
4 is the UID (user ID) of a user, John, in the database in the above scenario. A web application is a software application that runs on a web server and can be accessed by users through a web browser. A web application can be vulnerable to SQL injection attacks, which are a type of web application attack that exploit a vulnerability in a web application that allows an attacker to inject malicious SQL statements into an input field, such as a username or password field, and execute them on the database server. SQL injection can be used to bypass authentication, access or modify sensitive data, execute commands, etc. To exploit the web application and extract the user credentials from the moviescope database, one has to follow these steps:
Open a web browser and type www.moviescope.com
Press Enter key to access the web application.
Enter sam as username and test as password.
Click on Login button.
Observe that a welcome message with username sam is displayed.
Click on Logout button.
Enter sam' or `1'='1 as username and test as password.
Click on Login button.
Observe that a welcome message with username admin is displayed, indicating that SQL injection was successful.
Click on Logout button.
Enter sam'; SELECT * FROM users; ?as username and test as password.
Click on Login button.
Observe that an error message with user credentials from users table is displayed.
The user credentials from users table are:

UID	Username	Password
1	admin	admin
2	sam	test
3	alice	alice123
4	john	john123

The UID that is mapped to user john is 4

QUESTION NO: 15
法医学者のカソン氏は、脅迫者がインターネット上で特定の子供をいじめた事件の捜査を任された。事件を法的に進める前に、カソン氏は証拠の出所や事件との関連性など、裏付けとなるすべての文書を文書化し、陪審員の前に提出した。
上記のシナリオでは、次の証拠規則のうちどれが議論されましたか?
A. 本物
B. 理解できる
C. 信頼できる
D. 許容される

Answer: D
Explanation:
Admissible is the rule of evidence discussed in the above scenario. A rule of evidence is a criterion or principle that determines whether a piece of evidence can be used in a legal proceeding or investigation. Admissible is a rule of evidence that states that the evidence must be relevant, reliable, authentic, and understandable to be accepted by a court or a jury.Admissible also means that the evidence must be obtained legally and ethically, without violating any laws or rights. In the scenario, Kason has documented all the supporting documents, including source of the evidence and its relevance to the case, before presenting it in front of the jury, which means that he has followed the admissible rule of evidence.
Authentic is a rule of evidence that states that the evidence must be original or verifiable as genuine and not altered or tampered with.
Understandable is a rule of evidence that states that the evidence must be clear and comprehensible to the court or jury and not ambiguous or confusing. Reliable is a rule of evidence that states that the evidence must be consistent and trustworthy and not based on hearsay or speculation.

QUESTION NO: 16
セキュリティ専門家のアンドレは、データベースをクライアントと共有する前に、従業員の名前、電話番号、クレジットカード番号を分離する任務を負っていました。この目的のために、彼はデータベース フィールド内の重要な情報をアスタリスク (*) やハッシュ (#) などの特殊文字に置き換えることができる匿名化技術を実装しました。
上記のシナリオでアンドレが使用したテクニックは次のどれですか?
A. トークン化
B. マスキング
C. ハッシュ
D. バケット化
Answer: B
Explanation:
Masking is the technique that Andre employed in the above scenario. Masking is a deidentification technique that can replace the critical information in database fields with special characters such as asterisks (*) and hashes (#). Masking can help protect sensitive data from unauthorized access or disclosure, while preserving the format and structure of the original data.Tokenization is a deidentification technique that can replace the critical information in database fields with random tokens that have no meaning or relation to the original data. Hashing is a deidentification technique that can transform the critical information in database fields into fixed-length strings using a mathematical function. Bucketing is a deidentification technique that can group the critical information in database fields into ranges or categories based on certain criteria.

QUESTION NO: 17
ネットワークで SSH が有効になっているマシンへの SSH
接続を開始します。マシンに接続したら、flag.txt
ファイルを見つけて、ファイルに隠されたコンテンツを選択します。SSH
ログインの資格情報は以下に記載されています。

ヒント：
ユーザー名: sam
パスワード: admin@l23

A. sam@bob

B. bob2@sam

C. bob@sam

D. sam2@bob

Answer: C

Explanation:

Quid pro quo is the social engineering technique that Johnson employed in the above scenario.

Social engineering is a technique that involves manipulating or deceiving people into performing actions or revealing information that can be used for malicious purposes. Social engineering can be performed through various methods, such as phone calls, emails, websites, etc. Quid pro quo is a social engineering method that involves offering a service or a benefit in exchange for information or access. Quid pro quo can be used to trick victims into believing that they are receiving help or assistance from a legitimate source, while in fact they are compromising their security or privacy.In the scenario, Johnson performed quid pro quo by claiming himself to represent a technical support team from a vendor and offering to help sibertech.org with a server issue, while in fact he prompted the victim to execute unusual commands and install malicious files, which were then used to collect and pass critical information to Johnson's machine.

Diversion theft is a social engineering method that involves diverting the delivery or shipment of goods or assets to a different location or destination. Elicitation is a social engineering method that involves extracting information from a target by engaging them in a conversation or an interaction. Phishing is a social engineering method that involves sending fraudulent emails or messages that appear to come from a trusted source, such as a bank, a company, or a person, and asking the recipient to click on a link, open an attachment, or provide personal or financial information.