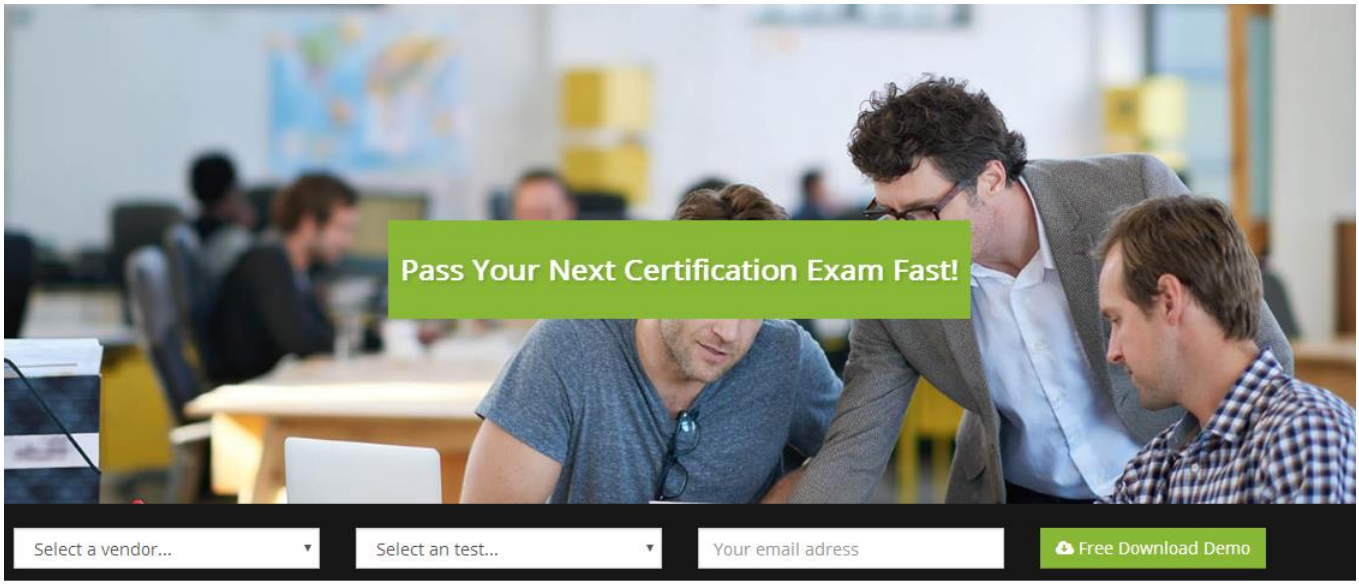
ITPassLeader



Instant Download | 365 Days Free Updates | Money Back Guarantee | Security & Privacy

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.	✓	✓	✓

http://www.itpassleader.com

High-praise Exam Dumps Questions grant you success by high pass rate - ITPassLeader

Exam : **312-49v10-JPN**

Title : Computer Hacking Forensic Investigator (CHFI-v10) (312-49v10日本語版)

Vendor : EC-COUNCIL

Version : DEMO

QUESTION NO: 1
専門家として証言を求められる前に、弁護士はまず何をしなければなりませんか?
A. 専門家証人としての資格
B. 陪審員に履歴書を読み上げる
C. ダメージコントロールを行う
D. 検査を実施するために使用したツールが完璧であることを証明してください
Answer: A

QUESTION NO: 2
次のツールのうち、ユーザーが Windows
システムで紛失した管理者パスワードをリセットできるのはどれですか?
A. 高度なOfficeパスワード回復
B. Active@ パスワードチェンジャー
C. Smartkey パスワード回復バンドル標準
D. パスワードキットフォレンジック
Answer: B

QUESTION NO: 3
警告バナーの使用は、従業員が想定する_____を克服し、企業が訴訟を回避するのに役立ちます。企業のイントラネット、ネットワーク、または仮想プライベートネットワーク(VPN)に接続する際に、企業の調査担当者がネットワーク内に保存されている情報を監視、検索、取得できるようになります。
A. 労働権
B. 言論の自由の権利
C. インターネットアクセス権
D. プライバシーの権利
Answer: D

QUESTION NO: 4
Web サーバーの IIS ログ ファイルを調べていると、次のエントリが見つかります。

```
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Development/index.asp
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /login.asp?username=if ((select user)='sa' OR (select user)='dbo')
select 1 else select 1/0
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Developments/index_02.jpg
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Development/index_04.jpg
```

このログファイルから何がわかりますか?
A. Webバグ
B. クロスサイトスクリプティング
C. 隠しフィールド
D. SQLインジェクションの可能性があります
Answer: D

QUESTION NO: 5
既知のエクスプロイトをネットワークに実行し、潜在的な脆弱性をテストしています。ウイルス対策ソフトの強度をテストするため、本番ネットワークを模倣したテストネットワーク

を構築しました。このソフトは、単純なマクロウイルスや暗号化ウイルスをブロックすることに成功しました。そこで、コード全体が書き換えられ、シグネチャは子ウイルスごとに異なりますが、機能は同じままであるウイルスコードを使用して、ソフトウェアの真の性能をテストすることにしました。テストしているウイルスの種類は何ですか？
A. 多態的
B. 変態
C. 寡形態
D. 変身
Answer: B

QUESTION NO: 6
Netstat を -ano スイッチとともに使用した場合、次のどの情報が表示されますか?
A. イーサネット統計
B. IPルーティングテーブルの内容
C. ルーティングテーブルの詳細
D. TCPおよびUDP接続の詳細
Answer: D

QUESTION NO: 7
あなたは、顧客データを保存する 4 つの 30 TB ストレージ エリア
ネットワークを持つ地方銀行のコンピューター
フォレンジック調査員として契約しています。
このネットワークからデジタル証拠を取得するには、どのような方法が最も効率的でしょうか?
A. DoubleSpaceでファイルの圧縮コピーを作成します
B. フォルダまたはファイルのスパースデータコピーを作成します
C. ビットストリームディスクイメージファイルを作成する
D. ビットストリームのディスクツーディスクファイルを作成する
Answer: C

QUESTION NO: 8
調査員ができるだけ早くパスワードを解読できるようにする Decryption Collection
のどの機能ですか?
A. 10分であらゆるパスワードを解読します
B. 16台以下のコンピュータに処理を分散する
C. 暗号化ファイルシステムのサポート
D. MD5ハッシュ検証のサポート
Answer: B

QUESTION NO: 9
FAT ファイル
システムは、ファイルを削除済みとしてマークするためにどのコードを使用しますか?
A. ESH
B.5EH

C. H5E
D. E5H
Answer: D

QUESTION NO: 10
次のコマンドは、ウェブサイトのログインページに何を表示しますか？ SELECT email, passwd, login_id, full_name FROM members WHERE email = 'someone@somehwere.com'; DROP TABLE members; --'
A. メンバーテーブル全体を削除します
B. エラー! 参照元が見つかりません。メールアドレスをメンバーテーブルに挿入します。
C. メンバーテーブルの最初のユーザーのパスワードを取得します。
D. このコマンドは構文が正しくないため、何も生成しません。
Answer: A

QUESTION NO: 11
Windows OS ファイル
システムからファイルが削除されると、ファイルのヘッダーに何が起こりますか?
A. OSは削除されたファイル名の最初の文字を16進バイトコードE5hに置き換えます。
B. OS はファイルの 16 進バイト コーディング全体を置き換えます。
C. ファイルの16進バイトコードは同じですが、ファイルの場所は異なります。
D. OSは削除されたファイル名の2番目の文字を16進バイトコードEh5に置き換えます。
Answer: A

QUESTION NO: 12
CAN-SPAM 法では、次のことが義務付けられています。
A. 誤解を招くような件名を使用しないでください
B. 受信者にあなたの居場所を教えないでください
C. メッセージを広告として識別しない
D. 実際のヘッダー情報を使用しない
Answer: A

QUESTION NO: 13
カイルは経理部門用に開発したアプリケーションの最終テストを行っています。
最後のテストは、プログラムの安全性を最大限に高めることです。カイルは次のコマンドを実行します。この時点で何をテストしているのでしょうか？
#include #include int main(int argc, char
*argv[]) { char buffer[10]; if (argc < 2) { fprintf (stderr, "USAGE: %s string\n", argv[0]); return 1; } strcpy(buffer, argv[1]); return 0; }
A. バッファオーバーフロー
B. SQLインジェクション
C. フォーマット文字列のバグ
D. カーネル注入
Answer: A

QUESTION NO: 14
文書、証言、宣誓のもとで書かれた質問と回答、事実の認諾を求める書面による要請、現場の検証などを要求することにより、裁判前に情報を得ようとする努力は、どのような法律用語で説明されていますか?
A. 検出
B. 伝聞
C. 略奪
D. 発見
Answer: D

QUESTION NO: 15
Web ログを確認すると、HTTP ステータス コード
フィールドにリソースが見つからないというエントリが表示されます。
リソースが見つからない場合にログに表示される実際のエラー コードは何ですか?
A.202
B. 404
C.606
D.999
Answer: B

QUESTION NO: 16
次のレジストリ
ハイブのうち、システム上のさまざまなファイルを開くために使用されたアプリケーションに関する構成情報を提供するものはどれですか。
A. HKEY_CLASSES_ROOT
B. HKEY_CURRENT_CONFIG
C.HKEY_LOCAL_MACHINE
D. HKEY_USERS
Answer: A

QUESTION NO: 17
Mac OS X で使用されるファイル システムは次のどれですか?
A. EFS
B. HFS+
C. EXT2
D. NFS
Answer: B

QUESTION NO: 18
Windows 管理者パスワードをリセットするためのツールは次のどれですか?
A. R-スタジオ
B. Windows パスワード回復ブートディスク
C. Windows データ復旧ソフトウェア

D. Windows用TestDisk
Answer: B

QUESTION NO: 19
ジェフは政府機関のサイバーセキュリティ部門に所属するフォレンジック調査員です。ジェフは、政府機関のウェブアプリケーションへのDDoS攻撃に関与したWindows 10コンピューターのメモリダンプを取得する任務を負っています。ジェフはメモリを収集するために現場にいます。ジェフが使用できるツールは何でしょうか？
A. ボラティリティ
B. 剖検
C. RAMマッパー
D. メモリチェック
Answer: A

QUESTION NO: 20
被害者、目撃者、または容疑者の電子デバイス上のデジタル証拠にアクセスする前に、捜査官は法的プライバシー要件を尊重するためにまず何をすべきでしょうか?
A.地方自治体または雇用主に事実を通知する
B. バッテリーを取り外すか、デバイスの電源をオフにします
C. 外部通信からデバイスを保護する
D. 捜索の正式な書面による同意を得る
Answer: A

QUESTION NO: 21
ビット ストリーム イメージの作成に使用できる、Windows アプリケーションとしても使用できる標準 Linux コマンドの名前は何ですか?
A. mコピー
B. 画像
C. MD5
D. dd
Answer: D

QUESTION NO: 22
次の捜索令状のうち、最初の対応者が被害者のコンピューターのコンポーネント(ハードウェア、ソフトウェア、ストレージ デバイス、ドキュメントなど)を捜索して押収することを許可しているのはどれですか。
A. ジョン・ドゥ捜索令状
B. 市民情報提供者捜索令状
C. 電子記憶装置捜索令状
D. サービスプロバイダー捜索令状
Answer: C

QUESTION NO: 23
次のレジストリ コンポーネントのうち、キーの LastWrite

時間だけでなく他のセルへのオフセットも含まれるのはどれですか。
A. 値リストセル
B. 値セル
C. キーセル
D. セキュリティ記述子セル
Answer: C

QUESTION NO: 24
新しいウェブサイトを公開する前に、最後のテストを実施しています。ウェブサイトには多くの動的ページがあり、データベース内の商品在庫にアクセスするSQLバックエンドに接続しています。あるウェブセキュリティサイトで、脆弱性をチェックするためにウェブページの検索フィールドに次のコードを入力することを推奨していました。このコードを入力して検索をクリックすると、「これはテストです」というポップアップウィンドウが表示されます。このテストの結果はどうでしょうか？
A. あなたのウェブサイトはCSSに対して脆弱です
B. あなたのウェブサイトは脆弱ではありません
C. あなたのウェブサイトはSQLインジェクションに対して脆弱です
D. あなたのウェブサイトはウェブバグに対して脆弱です
Answer: A

QUESTION NO: 25
ネットワーク管理者のアンディは、Windowsシステム上で異常なネットワークサービスが稼働しているのではないかと疑っています。Windowsシステム上で異常なネットワークサービスが起動しているかどうかを確認するには、以下のどのコマンドを使用すればよいでしょうか？
A. ネットサーバー
B. ネットマネージャー
C. lusrmgr
D. ネットスタート
Answer: D

QUESTION NO: 26
XYZ社から、境界メールゲートウェイのセキュリティ評価を依頼されました。ニューヨークのオフィスから、特別な形式のメールを作成し、インターネット経由でXYZ社の従業員に送信しました。XYZ社の従業員は、このセキュリティについて認識しています。
A. ソースコードレビュー
B. ファイアウォールの設定を確認する
C. データ項目と脆弱性スキャン
D. 従業員とネットワークエンジニアへのインタビュー
Answer: A

QUESTION NO: 27
次の米国法のうち、金融機関(融資、金融または投資に関するアドバイス、保険などの金融商品やサービスを消費者に提供する企業)に顧客の情報をセキュリティの脅威から保護する

ことを義務付けているのはどれですか。
A. ソックス
B. HIPAA
C. GLBA
D. FISMA
Answer: C

QUESTION NO: 28
ジョージはフロリダ州の州機関に勤務する上級セキュリティアナリストです。彼の州議会は、すべての州機関に毎年セキュリティ監査を受けることを義務付ける法案を可決しました。必要な要件を把握したジョージは、最初の監査が行われる前に、できるだけ早くIDS(侵入検知システム)を導入する必要があります。この州法案では、「時間ベース誘導装置」を備えたIDSの使用が義務付けられています。
この要件を満たすために、George はどのような IDS 機能を実装する必要がありますか?
A. シグネチャベースの異常検出
B. パターンマッチング
C. リアルタイム異常検出
D. 統計に基づく異常検出
Answer: C

QUESTION NO: 29
クラウドフォレンジック調査は、複数の管轄区域およびマルチテナントに関する課題を伴います。クラウドサービスプロバイダー(CSP)とクライアント間の役割と責任をより深く理解するために、フォレンジック調査員はどの文書を確認すべきでしょうか？
A. サービスレベル契約
B. サービスレベル管理
C. 国および地方の規制
D. 主要業績評価指標
Answer: A

QUESTION NO: 30
ユーザーのスタートアップ フォルダー
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\
のレジストリ設定に関して、正しい記述はどれですか。
A.
このサブキーのすべての値は、ユーザー固有の設定であるため、特定のユーザーがログオンしたときに実行されます。
B. 値runで指定された文字列は、ユーザーがログオンしたときに実行されます。
C. このキーのすべての値はシステム起動時に実行されます
D.
このサブキーのすべての値は、特定のユーザーがログオンすると実行され、その後削除されます。
Answer: D

QUESTION NO: 31
商業目的で電子メールを送信するための規則を設定し、商業メッセージの最低要件を確立し、電子メールの受信者に送信者に電子メールの送信を停止するように要求する権利を与え、上記の規則に違反した場合の罰則を規定している米国の法律はどれですか。
A. スパム禁止法
B. アメリカン: NAVSO P-5239-26 (RLL)
C. CAN-SPAM法
D. アメリカ: DoD 5220.22-M
Answer: C

QUESTION NO: 32
メールアーカイブとは、メールに含まれるデータを保存· 保護し、後日迅速にアクセスできるようにする体系的なアプローチです。アーカイブには主にローカルアーカイブとサーバーストレージアーカイブの2種類があります。ローカルアーカイブに関する記述のうち、正しいものはどれですか？
A.
サーバーストレージアーカイブは、ローカルシステムに保存されているサーバー情報と設定であり、ローカルアーカイブは、メールサーバーに保存されているローカル電子メールクライアント情報です。
B.
ウェブメールは、ほとんどの場合オフラインアーカイブがないため、対処が困難です。サーバー上の必要なデータにアクセスするための最善の方法については、担当弁護士にご相談ください。
C.
ローカルアーカイブは、法廷で証拠として認められるためには、サーバーストレージアーカイブと一緒に保存する必要がある。
D.
ローカルアーカイブは、電子メールクライアントがメッセージデータを変更する可能性があるため、証拠としての価値がありません。
Answer: B

QUESTION NO: 33
研究室の法医学スタッフが調査を行う際に最初に行うステップは何ですか?
A. 電子証拠のパッケージ化
B. 電子犯罪現場の安全確保と評価
C. 予備面接の実施
D. 電子証拠の輸送
Answer: B

QUESTION NO: 34
次の ISO
標準のうち、光ディスク間でデータを交換するためのファイルシステムとプロトコルを定義するものはどれですか?
A.ISO 9660

B.ISO/IEC 13940
C.ISO 9060
D.IEC 3490
Answer: A

QUESTION NO: 35
ユーザーから外部から脅迫メールを受け取ったという報告を受け、調査を依頼されました。メッセージの発信元を追跡する際に、最も関心のある項目は次のどれですか？
A. X509アドレス
B. SMTP応答アドレス
C. 電子メールヘッダー
D. ホストドメイン名
Answer: C