Exam : **SYO-501-JPN**

Title : CompTIA Security+ Certification Exam (SY0-501日本語版)

Vendor : CompTIA

Version : DEMO

QUESTION NO: 1
ペネトレーションテスターは、企業のネットワークの脆弱性を受動的にテストしています。ペネトレーションテスターは次のどのツールを使用する必要がありますか？
（2つ選択してください。）
A. tcpdump
B. Zenmap
C. Wireshark
D. Nmap
E. Snort
F. 日東
Answer: D,F

QUESTION NO: 2
組織の研究部門は、エアギャップネットワークでワークステーションを使用しています。競合他社が、研究部門で作成されたファイルに基づいて製品をリリースしました。研究ファイルのセキュリティと機密性を向上させるために、管理者は次のうちどれを行うべきですか？
A. 研究部門にWebアプリケーションファイアウォールをインストールします。
B. ワークステーションでリムーバブルメディアコントロールを構成します。
C. ワークステーションに多要素認証を実装します。
D. 各研究用ワークステーションにHIDSをインストールします。
Answer: B

QUESTION NO: 3
セキュリティエンジニアは、EAP-
TLSワイヤレスネットワークで使用するために、商用CAからRADIUSサーバーに証明書を展開します。認証が失敗しているため、エンジニアは証明書のプロパティを調べます。

```
Issuer: (A commercial CA)
Valid from: (yesterday's date)
Valid to: (one year from yesterday's date)
Subject: CN=smithco.com
Public key: RSA (2048 bits)
Enhanced key usage: Client authentication (1.3.6.1.5.5.7.3.2)
Key usage: Digital signature, key encipherment (a0)
```

次のうちどれが失敗の最も可能性の高い原因ですか？
A. 証明書に適切なOIDがありません。
B. キーの使用において、証明書にワイヤレス認証がありません。
C. 証明書の有効期限が切れています。
D. 証明書は自己署名されています。
Answer: B

QUESTION NO: 4
監査中、監査者は、特定されたミッションクリティカルなアプリケーションのコピーとその災害復旧計画を確認するように要求します。監査対象の会社には、ホストするアプリケーションに関するSLAがあります。MOSTが懸念する可能性が高いのは次のうちどれですか？

A. リスク評価
B. ARO / ALE
C. MTTR / MTBF
D. RTO / RPO
Answer: D

QUESTION NO: 5
不適切な入力処理が原因である可能性が最も高いのは、次のうちどれですか。
A. データベーステーブルの損失
B. ファイアウォールACLの違反
C. 信頼できない証明書の警告
D. 再起動ループの電源をオフにします
Answer: A

QUESTION NO: 6
ユーザーが外部ドメインに電子メールを送信しようとすると、すぐにバウンスバックメッセージが受信されます。次に、ユーザーはヘルプデスクに連絡して、メッセージが重要であり、すぐに配信する必要があることを伝えます。電子メールログを調べているときに、システム管理者は電子メールとバウンスバックの詳細を見つけます。
SSN情報が含まれているようであるため、メールは拒否されました。電子メールの外部受信者を介してSSN情報を送信すると、会社のポリシーに違反します。
次のテクノロジーのうち、メールの送信を正常に停止したのはどれですか？
A. UTM
B. DEP
C. WAF
D. DLP
Answer: B

QUESTION NO: 7
最高情報セキュリティ責任者（CISO）は、プロジェクトの範囲を超えてシステムへのアクセスを許可することなく、請負業者が会社の内部ネットワークに安全にアクセスする方法を設計するようセキュリティアーキテクトに依頼します。
CISOのニーズに最適な方法は次のうちどれですか？
A. PaaS
B. IaaS
C. VPN
D. VDI
Answer: C

QUESTION NO: 8
SOCは、最近の事件後のプロセスと手順を見直しています。レビューでは、感染したホストの隔離が最善の行動方針であると判断するのに30分以上かかったことが示されています。これにより、マルウェアは封じ込められる前に追加のホストに拡散することができました。インシデント対応プロセスを改善するには、次のうちどれが最善でしょうか。

A. ネットワークを信頼ゾーンと非信頼ゾーンに分割する
B. 感染したホストの手動検疫の実装
C. 許容できる使用法に関する追加のエンドユーザートレーニングを提供する
D. より良い意思決定ポイントでプレイブックを更新する
Answer: C

QUESTION NO: 9
次の環境のうち、通常、現在のバージョンの構成とコードをホストし、ユーザーストーリーの応答とワークフローを比較し、テストのために実際のデータの変更されたバージョンを使用する環境はどれですか。
A. 開発
B. 生産
C. ステージング
D. テスト
Answer: A

QUESTION NO: 10
システムレベルで実行するためのアクセス権がなくても、アプリケーションが機能するために必要なリソースのみにアクセスするための安全な環境を提供するものは次のうちどれですか。
A. Sandbox
B. DMZ
C. GPO
D. Honeypot
Answer: A

QUESTION NO: 11
セキュリティアナリストは、ワイヤレスネットワークの要件を指定しています。アナリストは、さまざまなアーキテクチャの選択肢によって提供されるセキュリティ機能について説明する必要があります。
次のどれがPEAP、EAP-TLS、およびEAP-TTLSによって提供されますか？
A. 安全なハッシュ
B. 証明書のピン留め
C. 相互認証
D. キーの回転
Answer: C

QUESTION NO: 12
次の出力が与えられます：

```
NMAP -P 80 ==script hostmap=bfk.nse company.com
starting NMAP 6.46
NMAP scan report for company.com (172.255.240.169)

Port State Service
80/TCP open http

Host script results
hostmap-bfk
hosts:
172.255.240.169
web1.company.com
swebdb1.company.com
web3.company.com
swebdb2.company.com

NMAP done: scanned in 2.10 seconds
```

次のうち、スキャンされた環境を最もよく表しているのはどれですか？
A. ホストがスキャンされ、Webベースの脆弱性が見つかりました
B. ドメインへの接続が確立され、いくつかのリダイレクト接続が識別されました
C. company.comのコンテンツ管理システムにWebシェルが植えられました
D. ホストが複数のドメインをホストしているWebサーバーとして識別されました
Answer: A

QUESTION NO: 13
ユーザーが企業のDHCPサーバーからIPアドレスを取得できません。次のうちどれが原因である可能性が最も高いですか？
A. リソースの枯渇
B. メモリオーバーフロー
C. 不適切な入力処理
D. デフォルト設定
Answer: A

QUESTION NO: 14
ある会社は最近、セキュリティポリシーを変更して、事前に承認されたWebサイトにのみアクセスできるようにし、エンドユーザーの構成なしでセットアップを実行できるようにしました。新しいセキュリティポリシーを実装するための最適な構成は次のうちどれですか？
A. 自動トリガーとヒューリスティックNIDSを備えたSIEMをインストールします。
B.

ループ防止機能とMACフィルタリングアクセスポイントを備えたレイヤ3スイッチをインストールします。
C. ACLルーターとエージェントレスNACをインストールします。
D. 透過プロキシをインストールして構成します。
Answer: D

QUESTION NO: 15
攻撃者はインターネット上のいくつかのシステムを制御し、それらを使用してWebサイトを攻撃し、正当なトラフィックへの応答を停止させています。次のうち、攻撃を最もよく表しているのはどれですか？
A. DDoS
B. MITM
C. バッファオーバーフロー
D. DNSポイズニング
Answer: A

QUESTION NO: 16
暗号技術者は、企業向けに新しい独自のハッシュ関数を開発し、その実装を推奨する前に従業員に関数のテストを依頼しました。従業員は、文書の平文バージョンを取得してハッシュし、元の平文文書を少し変更してハッシュします。
2つの異なるドキュメントから2つの同一のハッシュ値が生成されるまで、このプロセスを繰り返します。次のBESTのどれがこの暗号攻撃を説明していますか？
A. ブルートフォース
B. リプレイ
C. 既知の平文
D. 衝突
Answer: D

QUESTION NO: 17
システムがワークロードの変化に自動的に適応できるようにする回復力戦略は次のうちどれですか？
A. フォールトトレランス
B. 冗長性
C. 高可用性
D. 弾力性
Answer: D
Section: (none)
Explanation

QUESTION NO: 18
セキュリティ管理者は、すべてのVPNユーザーにNAC要件を追加して、共同要件を確保していますか？
A. 永続的なエージェントを実装します。
B. エージェントレス実装を使用します。

C. PKIを実装します。
D. ウイルス対策ソフトウェアをインストールします。
Answer: A

QUESTION NO: 19
ネットワークのサイバー衛生スキャンを毎週実行する前に、更新する必要があるのは次のうちどれですか？
A. アンチウイルスの定義
B. 脆弱性シグネチャ
C. WIDS設定
D. レインボーテーブル
Answer: B

QUESTION NO: 20
新しいPKIが会社で構築されていますが、ネットワーク管理者は、クライアントが証明書のステータスをチェックするために1日に2回発生するトラフィックの急増を懸念しています。トラフィックの急増を減らすために実装する必要があるのは次のうちどれですか？
A. OCSP
B. SAN
C. OID
D. CRL
Answer: A

QUESTION NO: 21
悪意のある攻撃者がデータを盗もうとするリスクが高い高度に安全な環境で、ファラデーケージを展開する最も良い理由は次のうちどれですか。
A. 悪意のある変更から監査ログの整合性を保護するため
B. 信号強度を最大化するために、距離による信号減衰を最小化する
C. 組み込みプロセッサとの外部RF干渉を最小限に抑えるため
D. クレデンシャルの取得を防ぐための発散制御を提供する
Answer: C

QUESTION NO: 22
ある会社は、本社の場所での外部メディアの使用を禁止しています。セキュリティアナリストは、システム上で実行されている奇妙なプロセスに気付いたときに、環境内のサーバーにリポジトリを追加する作業を行っています。アナリストはコマンドを実行し、次のことを確認します。

```
$ history
      ifconfig -a
      netstat -n
      pskill 1788
      pskill 914
      mkdir /tmp/1
      mount -u sda101 /tmp/1
      cp /tmp/1/* ~/1/
      umount /tmp/1
      ls -al 1/1/
      apt-get update
      apt-get upgrade
      clear
```

この出力を前提として、次のセキュリティ問題のどれが発見されましたか？

A. トロイの木馬のアクティベーション

B. マルウェアのインストール

C. ポリシー違反

D. 誤って構成されたHIDS

Answer: C

QUESTION NO: 23

コンピュータフォレンジックアナリストは、500ページのテキストを含む単一のファイルを含むサムドライブを収集しました。ファイルの機密性を維持するために、アナリストは次のうちどれを使用する必要がありますか？

A. SHA

B. NOA

C. SLA

D. AES

Answer: D

QUESTION NO: 24

セキュリティ情報を読んだ後、ネットワークセキュリティマネージャーは、悪意のある人物が同じソフトウェアの欠陥を使用してネットワークに侵入したのではないかと心配しています。エクスプロイトコードは公開されており、同じ業種の他の業界に対して使用されていると報告されています。フォレンジックレビューの優先リストを決定するために、ネットワークセキュリティマネージャーが最初に相談する必要があるのは次のどれですか？

A. The full packet capture data

B. The vulnerability scan output

C. The IDS logs

D. The SIEM alerts

Answer: B

QUESTION NO: 25

会社には、侵入テストのチームがあります。このチームは、会社のファイルサーバー上に、クリアテキストのユーザー名とそれに続くハッシュが含まれていると思われるファイルを見

つけました。このファイルの内容について詳しく知るために、侵入テスト担当者は次のどのツールを使用する必要がありますか？
A. Vulnerability scanner
B. Exploitation framework
C. Netcat
D. Password cracker
Answer: D

QUESTION NO: 26
サードパーティのソフトウェアをダウンロードした後、ユーザーはWindowsアンチウイルスが古くなったことを示すポップアップメッセージを継続的に受信し始めます。サブスクリプションがビットコインで更新されるまで、ユーザーはファイルやプログラムにアクセスできません。次のタイプの攻撃のどれが実行されていますか？
A. 暗号マルウェア
B. スパイウェア
C. ランサムウェア
D. アドウェア
Answer: C

QUESTION NO: 27
システムに問題が発生した場合にサーバーデータのバックアップが提供する制御タイプは次のうちどれですか？
A. 予防
B. 探偵
C. 抑止力
D. コレクター
Answer: D

QUESTION NO: 28
次のタイプのセキュリティテストのうち、パッチ適用が必要な既存のコードとID領域を分析するために最も費用効果の高いアプローチはどれですか。
A. White box
B. Gray box
C. Red team
D. Blue team
E. Black box
Answer: A

QUESTION NO: 29
最近、ある組織がISO
27001認証を取得しました。次のうちどれがこの認証の利点と最も考えられるでしょうか？
A. 組織がセキュリティ基準を満たしていることを顧客に保証します。
B. データ侵害の場合に保険を提供します。

C. 組織全体でデジタルフォレンジックデータを共有できます。
D.
組織がセキュリティクリアランスを必要とする外国のエンティティと連携できることを証明します。
E. ITセキュリティスタッフに無料のトレーニングと認定リソースを提供します。
Answer: A

QUESTION NO: 30
次のベストのどれが「発生の可能性」を説明しますか？
A. どの程度のダメージを与えてもイベントが発生する可能性
B. すべての要素が考慮された後の組織への全体的な影響
C. 脅威アクターが組織のシステムを標的にして悪用を試みる確率
D. システムに悪用される可能性のある弱点または欠陥がある可能性
Answer: C