実務に役立つ
サイバーセキュリティの基礎

CompTIA
CySA+
問題集

CS0-001対応

TAC

はじめに

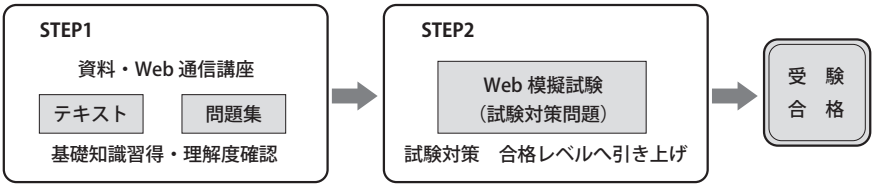
■ 本書について

本書は、TAC CySA+テキスト（CS0-001対応）で学習し、CompTIA CySA+（CS0-001）試験の受験を目標とする方向けの問題集です。
TAC CySA+テキスト（CS0-001対応）で、サイバーセキュリティに関連する知識を学習する際、この問題集を併用することで、より高い学習効果を得ることができるよう作成されています。理解度の確認にご利用ください。
またCySA+（CS0-001）試験の合格を目標とし、TAC CySA+テキスト（CS0-001対応）とこの問題集で基礎知識を習得された方には、試験対策に最適な、TAC Web通信講座「CySA+Web模擬試験」をおすすめしております（http://web.tac-school.co.jp/it/comptia/index.html）。
こちらの模擬試験で理解が不足している部分を確認し、弱点を補強するためにもぜひご活用ください。

■ TAC CompTIA関連教材ラインアップ

TACではCompTIA認定資格取得をサポートするために、以下のCompTIA関連教材を販売しております。試験範囲の知識習得のためのテキスト、理解度確認のための問題集、試験対策のためのWeb模擬試験のほか、通信講座も開講しております。学習教材として幅広くご利用ください。

基本的な学習の流れ



ラインアップ一覧

	IT Fundamentals	Cloud Essentials	A+	Network+	Server+	Security+	CySA+	Project+	Cloud+
テキスト	●	●	●	●	●	●	●	●	●
問題集			●	●	●	●	●	●	●
資料通信	●	●	●	●	●	●	●	●	●
Web通信		●	●	●		●			
Web模擬試験	●	●	●	●	●	●	●	●	●

※資料通信・Web通信にはテキスト・問題集・Web模擬試験が含まれます。
※Web通信には講義動画が含まれます。
※Project+（試験番号:PK0-004）テキスト・問題集は2018年春発売予定です。資料通信は2018年夏発売予定です。
※試験番号および試験配信時期により、教材ラインアップが変更となる場合がございます。最新情報は、下記TAC CompTIA講座ホームページをご確認ください。

TAC　CompTIA講座ホームページ　　http://web.tac-school.co.jp/it/comptia/
お問い合わせ　its@tac-school.co.jp

TAC e受付（コースお申し込み総合サイト）　　http://ec.tac-school.co.jp/
TACサイバーブックストア（書籍販売サイト）　　https://bookstore.tac-school.co.jp/

■ 各種トレーニングのご案内

企業研修においては、上記コンテンツのほかに、各種アセスメントテスト、オリジナルレジュメ、出題傾向予想資料等をご提供しております。CompTIAをベースとした顧客起点でのIT実務能力育成にご活用ください。
企業向け研修サービス、カリキュラム提案、教材コンテンツの販売に関しては、以下までお問い合わせください。

TAC法人事業部　http://www.tac.biz/
東日本エリア：法人営業2部　　TEL：03-5276-9802
東海、北陸エリア：東海法人グループ　　TEL：052-586-5239
西日本エリア：西日本法人営業部　　TEL：06-6371-1075
受付時間：平日9：30 ～ 17：30（土日祝祭日は定休日）

Contents

第1章

サイバーセキュリティ

Q 001

脅威インテリジェンスアナリストより社内の複数のサーバーに該当する脆弱性が報告されました。セキュリティアナリストとして、脆弱性のあるサーバーを特定するために何をしますか。

- a. OSフィンガープリントの確認
- b. トポロジーディスカバリー
- c. フィッシング
- d. ファイアウォールのログ分析

A

正解は「OSフィンガープリントの確認」です。

a

OSフィンガープリントにより、機器のOSとそのバージョンを特定することができ、これらの情報から脆弱性に該当するサーバーを特定することができます。
トポロジーディスカバリーは、ネットワーク上の機器とその接続形態を自動検出することです。
フィッシングは、金融機関などを装ったメールで偽のWebサイトに誘導して個人情報を窃取する攻撃ですが、社内ユーザーへの訓練として攻撃に適切に対応できるかを確認することもできます。
ファイアウォールのログでは、セグメント間での送受信を許可・拒否される通信ポリシーおよびポリシー違反パケットを確認することができます。

Q 002

公開されている会社の情報やブランドイメージを確認するために使用するのはどれですか。

- a. ソーシャルメディア
- b. パケットキャプチャ
- c. ファイアウォールのログ
- d. イントラネット

A

正解は「ソーシャルメディア」です。

a

インターネット上で利用できるFacebookやTwitterなどのソーシャルネットワーキングサービス（SNS）において、ユーザーは日常の出来事を投稿し、興味のある製品やイベント情報を検索します。SNS上の投稿などを収集･分析すること（ソーシャルメディアプロファイリング）により自社製品やサービスの評価を確認し、市場調査を行うことができます。

パケットキャプチャはパケットを解析することができますが、設問のような用途には使用しません。

ファイアウォールのログでは、インターネットと自社の間でのアクセスが適切であったかどうかを確認することができます。

Q

003

社内に設置したサーバーのほうがクラウドと比較した場合に、セキュリティレベルが高いと考えられる理由はどれですか。

- a. どこからでも接続できる
- b. セキュアOSが利用できる
- c. 無線通信を利用できる
- d. 物理的セキュリティを確保できる

A

正解は「物理的セキュリティを確保できる」です。

d

クラウドはインターネット上のデータセンターに保存されたデータにさまざまな場所からアクセスできるサービスです。インターネット利用を前提とし、物理デバイスやオペレーターにはデータセンターの共用リソースを利用します。
一方、社内に設置したサーバー（オンプレミス）は、自社内の物理的に閉じた環境に設置されるため物理的セキュリティが確保しやすくなります。
OSはクラウドも社内に設置したサーバーも複数から選択できます。OSの選択の自由度は、自社に設置するほうが高くなりますが、セキュリティレベルは同程度です。

Q

004

仮想環境と物理環境を識別できる情報はどれですか。

- a. IPアドレス
- b. ドメイン名
- c. ファイアウォールルール
- d. MACアドレス

A

正解は「MACアドレス」です。

d

物理環境は、各物理NICに割り当てられた一意なMACアドレスを使用します。一方、仮想環境のMACアドレスは、仮想マシンの作成時に、仮想化ソフトごとに用意された任意のアドレスプールから割り当てられます。
IPアドレス、ドメイン名は、仮想環境も物理環境も同じルールで割り当てられます。また、ファイアウォールルールも同じルールが適用されます。

Q

005

デスクトップPCとサーバーを比較した場合、サーバーのほうがセキュリティ上、優れているところはどこですか。（2つ選択してください）

- ☐ a. 物理セキュリティ
- ☐ b. パケットアナライザー
- ☐ c. OS
- ☐ d. syslog

A

正解は「物理セキュリティ」、「OS」です。

ⓐ
ⓒ

デスクトップPCと比較すると、サーバーのほうがOSの機能が高く、シャーシやサーバー室の利用などの物理セキュリティの面でも優れています。
パケットアナライザーやsyslogはサーバー / クライアントOSのいずれでも利用可能です。

Q

006

組織内のネットワーク接続形態を確認するのに使用するツールはどれですか。

- a. OSフィンガープリント
- b. トポロジーディスカバリー
- c. フィッシング
- d. パケットキャプチャ

A

正解は「トポロジーディスカバリー」です。

b

トポロジーディスカバリーは、ネットワーク上の機器とその接続形態を自動検出することができ、ネットワーク構成を確認することができます。
OSフィンガープリントにより、機器のOSとそのバージョンを特定することができ、これらの情報から脆弱性に該当するサーバーを特定することができます。
フィッシングは、金融機関などを装ったメールで偽のWebサイトに誘導して個人情報を窃取する攻撃です。
パケットキャプチャは、ネットワーク上のパケットを捕捉し、解析や集計をすることができます。

Q

007

攻撃者が組織内の人間になりすまして情報を収集するのはどれですか。

- a. DNSハーベスティング
- b. フィッシング
- c. メールハーベスティング
- d. ソーシャルエンジニアリング

A

正解は「ソーシャルエンジニアリング」です。

d

ソーシャルエンジニアリングは、話術や会話の盗み聞きなど、人間の心理や行動の隙をつくことで情報を収集するものです。攻撃者が組織内の人間になりすまして情報を収集することもソーシャルエンジニアリングに該当します。
DNSハーベスティングは、ドメイン内のIPアドレスを収集するものです。
フィッシングは、金融機関などを装ったメールで偽のWebサイトに誘導して個人情報を窃取する攻撃です。
メールハーベスティングは、メールアドレスを収集するもので、自動生成したメールアドレスあてにメールを送り、エラーにならないものは有効として収集します。