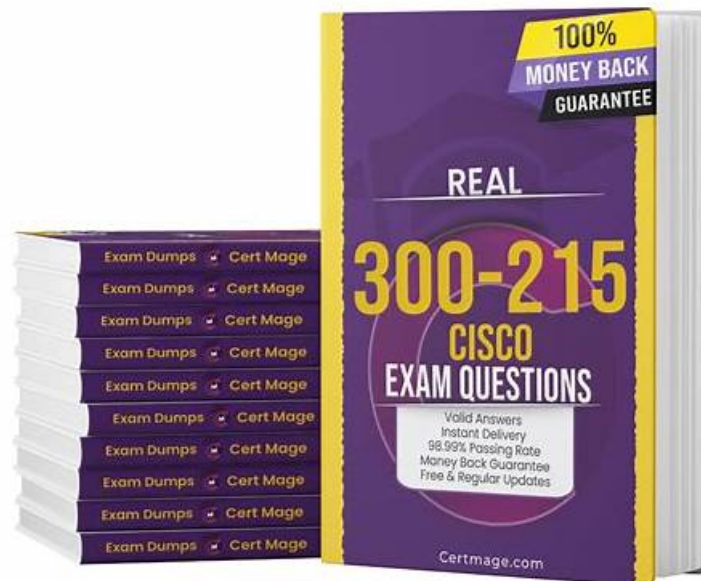


Cisco 300-215専門トレーニング、300-215練習問題集



BONUS!!! Xhs1991 300-215ダンプの一部を無料でダウンロード: <https://drive.google.com/open?id=1R8VVHFskGQYH3VWwE8NkhM0k12rFWVCa>

当社Ciscoの300-215学習ツールでは、選択できる3つのバージョンがあり、PDFバージョン、PCバージョン、APPオンラインバージョンが含まれます。各バージョンはさまざまな状況や機器に対応しており、最も便利な方法を選択して300-215テストトレントを学習できます。たとえば、APPオンラインバージョンは印刷可能で、ダウンロードへの即時アクセスを促進します。300-215ガイドトレントはいつでもどこでも学習できます。300-215学習ツールのPCバージョンは、実際の試験のシナリオを刺激できます。365日間の無料アップデートと無料デモを提供しています。

Cisco 300-215認定資格は、IT業界で高く評価され、多くの雇用者にとってセキュリティ専門家としての貴重な資格と認識されています。この認定資格は、保持者がCisco CyberOpsのテクノロジーを使用してセキュリティインシデントを検出、調査、対応するために必要な知識とスキルを持っていることを示しており、新しい仕事の機会を開拓し、収入を増やすためのキャリアアップにも役立ちます。

Cisco 300-215認定試験は、Cisco Technologiesを使用したインシデント対応、法医学分析、およびセキュリティ運用の専門知識を開発したい専門家向けに設計されています。この認定は、セキュリティインシデントと違反を検出、調査、および対応するために使用されるさまざまなシスコツールと技術に関する候補者の知識を検証します。この試験では、ネットワークインフラストラクチャのセキュリティ、エンドポイント保護、脅威インテリジェンス、サイバーセキュリティポリシーと手順など、さまざまなトピックをカバーしています。

>> Cisco 300-215専門トレーニング <<

300-215練習問題集、300-215専門知識

現在のネットワークの全盛期で、Ciscoの300-215の認証試験を準備するのにいろいろな方法があります。Xhs1991が提供した最も依頼できるトレーニングの問題と解答はあなたが気楽にCiscoの300-215の認証試験を受けることに助けを差し上げます。Xhs1991にCiscoの300-215の試験に関する問題はいくつかの種類がありますから、すべてのIT認証試験の要求を満たすことができます。

Cisco 300-215試験は、Cisco Technologiesを使用して法医学分析とインシデント対応を実施する際にサイバーセキュリティの専門家のスキルと知識をテストするように設計されています。この試験では、シスコが提供する

さまざまなツールとテクニックを使用したセキュリティインシデントの識別、封じ込め、および修復に焦点を当てています。

Cisco Conducting Forensic Analysis & Incident Response Using Cisco Technologies for CyberOps 認定 300-215 試験問題 (Q86-Q91):

質問 #86

A network host is infected with malware by an attacker who uses the host to make calls for files and shuttle traffic to bots. This attack went undetected and resulted in a significant loss. The organization wants to ensure this does not happen in the future and needs a security solution that will generate alerts when command and control communication from an infected device is detected. Which network security solution should be recommended?

- A. Cisco Secure Email Gateway (ESA)
- B. Cisco Secure Firewall ASA
- C. Cisco Secure Firewall Threat Defense (Firepower)
- D. Cisco Secure Web Appliance (WSA)

正解: C

質問 #87

Drag and drop the steps from the left into the order to perform forensics analysis of infrastructure networks on the right.

Obtain	step 1
Strategize	step 2
Collect	step 3
Analyze	step 4
Report	step 5

正解:

解説:

Obtain	Obtain
Strategize	Strategize
Collect	Collect
Analyze	Analyze
Report	Report



Reference: https://subscription.packtpub.com/book/networking_and_servers/9781789344523/1/ch01lvl1sec12/network-forensics-investigation-methodology

質問 # 88

A malware outbreak revealed that a firewall was misconfigured, allowing external access to the SharePoint server. What should the security team do next?

- A. Review and update all firewall rules and the network security policy
- B. Disable external IP communications on all firewalls
- C. Scan for and fix vulnerabilities on the firewall and server
- D. Harden the SharePoint server

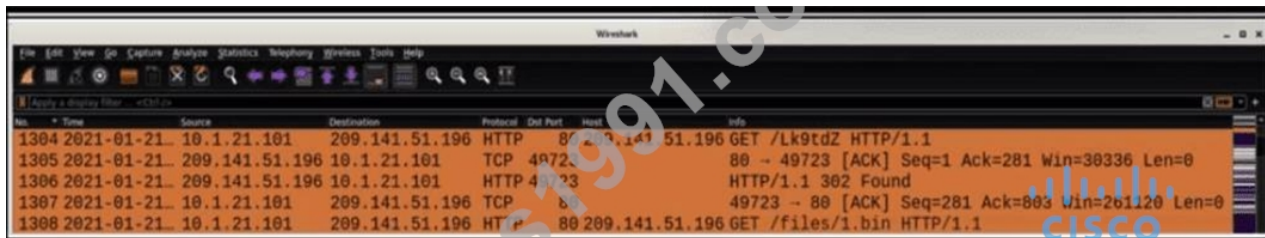
正解: A

解説:

The incident stems from a policy-level issue rather than a technical vulnerability. According to incident response best practices, the priority should be to review and update firewall rules and ensure that the network security policy aligns with the principle of least privilege and correct access segmentation.

質問 # 89

Refer to the exhibit.



What is occurring within the exhibit?

- A. Source 10.1.21.101 is communicating with 209.141.51.196 over an encrypted channel.
- B. Source 10.1.21.101 sends HTTP requests with the size of 302 kb.
- C. Host 209.141.51.196 redirects the client request from /Lk9tdZ to /files/1.bin.
- D. Host 209.141.51.196 redirects the client request to port 49723.

正解: C

解説:

The Wireshark capture shows a series of HTTP requests and responses:

- * The client (10.1.21.101) sends a GET request for /Lk9tdZ.
 - * The server (209.141.51.196) responds with HTTP/1.1 302 Found, which is a standard HTTP status code indicating a redirection.
 - * The subsequent GET request from the client is for /files/1.bin, which indicates it followed the redirect.
- This behavior confirms that the server is issuing an HTTP 302 redirect from the initial request path /Lk9tdZ to /files/1.bin. This is often observed in malware command-and-control behavior or file download staging.
- * Option A is incorrect: 302 is a status code, not a data size.
 - * Option C is incorrect: port 49723 is a source/destination ephemeral port, not a redirect target.
 - * Option D is incorrect: communication is over HTTP, not HTTPS (which would indicate encryption).

Reference: CyberOps Technologies (CBRFIR) 300-215 study guide, Chapter on Network Traffic Analysis and HTTP Status Code

Interpretation.

質問 #90

Refer to the exhibit.



```
Dec 28 11:27:10 CyberOps sshd[8423]: Failed password for invalid user admin from Cyber port 44216 ssh2
Dec 28 11:27:13 CyberOps sshd[8425]: Failed password for invalid user phoenix from Cyber port 20532 ssh2
Dec 28 11:27:17 CyberOps sshd[8428]: Failed password for invalid user test from Cyber port 24492 ssh2
Dec 28 11:27:22 CyberOps sshd[8430]: Failed password for invalid user rainbow from Cyber port 46591 ssh2
Dec 28 11:27:25 CyberOps sshd[8432]: Failed password for invalid user runner from Cyber port 57129 ssh2
Dec 28 11:27:34 CyberOps sshd[8434]: Failed password for invalid user user from Cyber port 11960 ssh2
Dec 28 11:27:37 CyberOps sshd[8437]: Failed password for invalid user abc123 from Cyber port 5921 ssh2
Dec 28 11:27:48 CyberOps sshd[8439]: Failed password for invalid user passwd from Cyber port 21298 ssh2
```

A web hosting company analyst is analyzing the latest traffic because there was a 20% spike in server CPU usage recently. After correlating the logs, the problem seems to be related to the bad actor activities. Which attack vector is used and what mitigation can the analyst suggest?

- A. Phishing attack; conduct regular user training and use email filtering solutions.
- B. Distributed denial of service; use rate limiting and DDoS protection services.
- C. SQL Injection; implement input validation and use parameterized queries.
- **D. Brute-force attack; implement account lockout policies and roll out MFA.**

正解: D

解説:

Comprehensive and Detailed Explanation:

The log entries show repeated SSH login attempts for various invalid usernames (e.g., admin, phoenix, rainbow, test, user, etc.) from different source ports. These are clear signs of a brute-force attack—an automated process trying multiple usernames and passwords in hopes of gaining access.

Mitigating such attacks includes:

- * Implementing account lockout policies (e.g., locking an account after several failed login attempts).
- * Enabling Multi-Factor Authentication (MFA) to ensure that password guessing alone is insufficient for account access.

Therefore, the correct answer is:

D). Brute-force attack; implement account lockout policies and roll out MFA.

質問 #91

.....

300-215練習問題集: <https://www.xhs1991.com/300-215.html>

- 300-215試験合格攻略 ※ 300-215日本語的中対策 □ 300-215対応問題集 □ 【 www.shikenpass.com 】 に移動し、✓ 300-215 □ ✓ □ を検索して無料でダウンロードしてください300-215必殺問題集
- 300-215日本語版問題解説 □ 300-215試験関連赤本 □ 300-215対応受験 ♥ ➡ www.goshiken.com □ □ □ には無料の【 300-215 】問題集があります300-215模擬モード
- 実際の300-215専門トレーニング試験・試験の準備方法・効率的な300-215練習問題集 □ ▶ www.jpshiken.com ◀ の無料ダウンロード ➡ 300-215 □ □ □ ページが開きます300-215試験概要
- 300-215日本語版トレーニング □ 300-215対応問題集 □ 300-215日本語版問題解説 □ Open Webサイト □ www.goshiken.com □ 検索 ➡ 300-215 □ □ □ 無料ダウンロード300-215必殺問題集
- 300-215対応問題集 □ 300-215認定資格 □ 300-215試験関連赤本 □ 時間限定無料で使える《 300-215 》の試験問題は【 www.passtest.jp 】サイトで検索300-215日本語版トレーニング
- 300-215日本語的中対策 □ 300-215再テスト □ 300-215復習テキスト ☺ ➡ www.goshiken.com □ を開き、▶ 300-215 ◀ を入力して、無料でダウンロードしてください300-215試験関連赤本
- 300-215対応資料 □ 300-215試験過去問 □ 300-215必殺問題集 □ [www.goshiken.com] サイトにて [300-215] 問題集を無料で使おう300-215赤本勉強
- 100% 合格率300-215 | 有効的な300-215専門トレーニング試験 | 試験の準備方法Conducting Forensic Analysis & Incident Response Using Cisco Technologies for CyberOps練習問題集 □ 最新▶ 300-215 ◀ 問題集ファイルは【 www.goshiken.com 】にて検索300-215認定資格
- 300-215関連受験参考書 □ 300-215必殺問題集 □ 300-215試験合格攻略 □ 今すぐ※ www.jpctestking.com □ ※ □ で“300-215”を検索して、無料でダウンロードしてください300-215復習テキスト
- 100% 合格率300-215 | 有効的な300-215専門トレーニング試験 | 試験の準備方法Conducting Forensic Analysis & Incident Response Using Cisco Technologies for CyberOps練習問題集 ☒ 今すぐ (www.goshiken.com) で (300-215) を検索し、無料でダウンロードしてください300-215必殺問題集

- 300-215赤本勉強 □ 300-215認定資格 □ 300-215認定資格 □ 「 www.jpexam.com 」の無料ダウンロード▶
300-215 ◀ページが開きます300-215対応問題集
- www.stes.tyc.edu.tw, estar.jp, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.4shared.com, www.stes.tyc.edu.tw,
lms.ait.edu.za, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt,
myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw,
stackblitz.com, Disposable vapes

P.S.Xhs1991がGoogle Driveで共有している無料の2026 Cisco 300-215ダンプ: <https://drive.google.com/open?id=1R8VVHFskGQYH3VWwE8NkhM0k12rFWVCa>