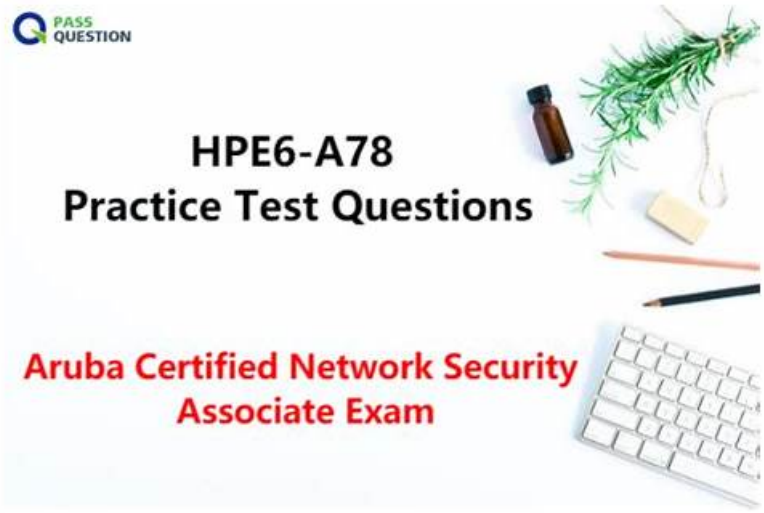
HPE6-A78試験の準備方法｜100％合格率のHPE6-A78関連資格試験対応試験｜有難いAruba Certified Network Security Associate Exam無料サンプル



ちなみに、ShikenPASS HPE6-A78の一部をクラウドストレージからダウンロードできます：https://drive.google.com/open?id=1ngtsR4VJ6gFc4nxr8d5GNz-Z_Nl0-quD

HPのHPE6-A78認定試験に受かるのはあなたの技能を検証することだけでなく、あなたの専門知識を証明できて、上司は無駄にあなたを雇うことはしないことの証明書です。当面、IT業界でHPのHPE6-A78認定試験の信頼できるソースが必要です。ShikenPASSはとても良い選択で、HPE6-A78の試験を最も短い時間に縮められますから、あなたの費用とエネルギーを節約することができます。それに、あなたに美しい未来を作ることに助けを差し上げられます。

HPE6-A78試験は、60の多肢選択問題から構成される90分間の試験です。この試験は、候補者のネットワークセキュリティ領域での知識、スキル、能力をテストするよう設計されています。候補者は、最低70％のスコアで試験に合格する必要があります。試験は、世界中のPearson VUEテストセンターを通じて実施され、候補者はPearson VUEのウェブサイトから試験に登録することができます。HPE6-A78試験は、ネットワークセキュリティにおける専門知識を証明し、この分野でキャリアを進めたいITプロフェッショナルにとって有益な認定です。

>> HPE6-A78関連資格試験対応 <<

実用的-検証するHPE6-A78関連資格試験対応試験-試験の準備方法HPE6-A78無料サンプル

現在でHPのHPE6-A78試験を受かることができます。ShikenPASSにHPのHPE6-A78試験のフルバージョンがありますから、最新のHPのHPE6-A78のトレーニング資料をあちこち探す必要がないです。ShikenPASSを利用したら、あなたはもう最も良いHPのHPE6-A78のトレーニング資料を見つけたのです。弊社の質問と解答を安心にご利用ください。あなたはきっとHPのHPE6-A78試験に合格できますから。

HPE6-A78試験は、ネットワークセキュリティソリューションの設計、実装、および管理を担当する専門家に最適です。この試験では、さまざまなサイバー脅威に対してエンタープライズネットワークを保護するために必要なスキルと知識を検証します。 HPE6-A78試験は、セキュリティの脆弱性を特定し、セキュリティソリューションを実装し、セキュリティイベントを監視する候補者の能力を評価するように設計されています。

HPのHPE6-A78試験は、Aruba製品を使用してネットワークセキュリティの知識とスキルを証明したい個人向けの認定試験です。この試験は、候補者がネットワークセキュリティインフラストラクチャを構成および管理し、ネットワークセキュリティの脅威を特定および軽減し、ネットワークのセキュリティを確保するためのベストプラクティスを実装する能力をテストするように設計されています。この試験に合格することは、ネットワークセキュリティにおける専門知識を証明し、Aruba認定ネットワークセキュリティアソシエイトとして認められる素晴らしい方法です。

HP Aruba Certified Network Security Associate Exam 認定 HPE6-A78 試験問題 (Q115-Q120):

質問 # 115
How can hackers implement a man-in-the-middle (MITM) attack against a wireless client?

- A. The hacker runs an NMap scan on the wireless client to find its MAC and IP address. The hacker then connects to another network and spoofs those addresses.
- B. The hacker uses spear-phishing to probe for the IP addresses that the client is attempting to reach. The hacker device then spoofs those IP addresses.
- C. The hacker uses a combination of software and hardware to jam the RF band and prevent the client from connecting to any wireless networks.
- D. The hacker connects a device to the same wireless network as the client and responds to the client's ARP requests with the hacker device's MAC address.

正解：D

解説：
A common method for hackers to perform a man-in-the-middle (MITM) attack on a wireless network is by ARP poisoning. The attacker connects to the same network as the victim and sends false ARP messages over the network. This causes the victim's device to send traffic to the attacker's machine instead of the legitimate destination, allowing the attacker to intercept the traffic.

質問 # 116
A company has an Aruba solution with a Mobility Master (MM) Mobility Controllers (MCs) and campus Aps. What is one benefit of adding Aruba Airwave from the perspective of forensics?

- A. Airwave is required to activate Wireless Intrusion Prevention (WIP) services on the ArubaOS solution
- B. Airwave retains information about the network for much longer periods than ArubaOS solution
- C. Airwave can provide more advanced authentication and access control services for the AmbaOS solution
- D. AirWave enables low level debugging on the devices across the ArubaOS solution

正解：B

解説：
Adding Aruba Airwave to an Aruba solution that includes a Mobility Master (MM), Mobility Controllers (MCs), and campus APs offers several benefits, notably in the realm of network forensics. One of the significant advantages is that Airwave can retain detailed information about the network for much longer periods than what is typically possible with just ArubaOS solutions. This extensive data retention is crucial for forensic analysis, allowing network administrators and security professionals to conduct thorough investigations of past incidents. With access to historical data, professionals can identify trends, pinpoint security breaches, and understand the impact of specific changes or events within the network over time.
:
Aruba's official product documentation and user guides for Airwave and ArubaOS, which outline features, benefits, and use cases related to network management and forensic capabilities.
Industry case studies and whitepapers that discuss the implementation and advantages of integrating Airwave into existing network infrastructure for enhanced monitoring and security.

質問 # 117
A company has an AOS controller-based solution with a WPA3-Enterprise WLAN, which authenticates wireless clients to HPE Aruba Networking ClearPass Policy Manager (CPPM). The company has decided to use digital certificates for authentication. A user's Windows domain computer has had certificates installed on it. However, the Networks and Connections window shows that authentication has failed for the user. The Mobility Controller's (MC's) RADIUS events show that it is receiving Access-Rejects for the authentication attempt.
What is one place that you can look for deeper insight into why this authentication attempt is failing?

- A. The RADIUS events within the CPPM Event Viewer
- B. The Alerts tab in the authentication record in CPPM Access Tracker
- C. The reports generated by HPE Aruba Networking ClearPass Insight
- D. The packets captured on the MC control plane destined to UDP 1812

正解：B

解説：
The scenario involves an AOS-8 controller-based solution with a WPA3-Enterprise WLAN using HPE Aruba Networking ClearPass Policy Manager (CPPM) for authentication. The company is using digital certificates for authentication (likely EAP-TLS, as it's the most common certificate-based method for WPA3-Enterprise). A user's Windows domain computer has certificates installed, but authentication fails. The Mobility Controller (MC) logs show Access-Rejects from CPPM, indicating that CPPM rejected the authentication attempt.
Access-Reject: An Access-Reject message from CPPM means that the authentication failed due to a policy violation, certificate issue, or other configuration mismatch. To troubleshoot, we need to find detailed information about why CPPM rejected the request.
Option C, "The Alerts tab in the authentication record in CPPM Access Tracker," is correct. Access Tracker in CPPM logs all authentication attempts, including successful and failed ones. For a failed attempt (Access-Reject), the authentication record in Access Tracker will include an Alerts tab that provides detailed reasons for the failure. For example, if the client's certificate is invalid (e.g., expired, not trusted, or missing a required attribute), or if the user does not match a policy in CPPM, the Alerts tab will specify the exact issue (e.g., "Certificate not trusted," "User not found in directory").
Option A, "The reports generated by HPE Aruba Networking ClearPass Insight," is incorrect. ClearPass Insight is used for generating reports and analytics (e.g., trends, usage patterns), not for real-time troubleshooting of specific authentication failures.
Option B, "The RADIUS events within the CPPM Event Viewer," is incorrect. The Event Viewer logs system-level events (e.g., service crashes, NAD mismatches), not detailed authentication failure reasons. While it might log that an Access-Reject was sent, it won't provide the specific reason for the rejection.
Option D, "The packets captured on the MC control plane destined to UDP 1812," is incorrect. Capturing packets on the MC control plane for UDP 1812 (RADIUS authentication port) can show the RADIUS exchange, but it won't provide the detailed reason for the Access-Reject. The MC logs already show the Access-Reject, so the issue lies on the CPPM side, and Access Tracker provides more insight.
The HPE Aruba Networking ClearPass Policy Manager 6.11 User Guide states:
"Access Tracker (Monitoring > Live Monitoring > Access Tracker) logs all authentication attempts, including failed ones. For an Access-Reject, the authentication record in Access Tracker includes an Alerts tab that provides detailed reasons for the failure. For example, in a certificate-based authentication (e.g., EAP-TLS), the Alerts tab might show 'Certificate not trusted' if the client's certificate is not trusted by ClearPass, or 'User not found' if the user does not match a policy. This is the primary place to look for deeper insight into authentication failures." (Page 299, Access Tracker Troubleshooting Section) Additionally, the HPE Aruba Networking AOS-8 8.11 User Guide notes:
"If the Mobility Controller logs show an Access-Reject from the RADIUS server (e.g., ClearPass), check the RADIUS server's authentication logs for details. In ClearPass, the Access Tracker provides detailed failure reasons in the Alerts tab of the authentication record, such as certificate issues or policy mismatches." (Page 500, Troubleshooting 802.1X Authentication Section)
:
HPE Aruba Networking ClearPass Policy Manager 6.11 User Guide, Access Tracker Troubleshooting Section, Page 299.
HPE Aruba Networking AOS-8 8.11 User Guide, Troubleshooting 802.1X Authentication Section, Page 500.

質問 # 118
A company has an Aruba solution with a Mobility Master (MM) Mobility Controllers (MCs) and campus Aps.
What is one benefit of adding Aruba Airwave from the perspective of forensics?

- A. Airwave is required to activate Wireless Intrusion Prevention (WIP) services on the ArubaOS solution
- B. Airwave can provide more advanced authentication and access control services for the AmbaOS solution
- C. AirWave enables low level debugging on the devices across the ArubaOS solution
- D. Airwave retains information about the network for much longer periods than ArubaOS solution

正解：A

質問 # 119
You have been asked to send RADIUS debug messages from an ArubaOS-CX switch to a central SIEM server at 10.5.15.6. The server is already defined on the switch with this command: logging 10.5.6.12 You enter this command: debug radius all What is the correct debug destination?

- A. buffer
- B. syslog
- C. console
- D. file

正解：B

解説：
When configuring an ArubaOS-CX switch to send RADIUS debug messages to a central SIEM server, it is important to correctly direct these debug outputs. The command debug radius all activates debugging for all RADIUS processes, capturing detailed logs about RADIUS operations. If the SIEM server is already defined on the switch for logging purposes (as indicated by the command logging 10.5.6.12), the correct destination for these debug messages to be sent to the SIEM server would be through the syslog. This ensures that all generated logs are forwarded to the centralized server specified for logging, enabling consistent log management and analysis. Using syslog as the destination leverages the existing logging setup and integrates seamlessly with the network's centralized monitoring systems.

質問 # 120
.....