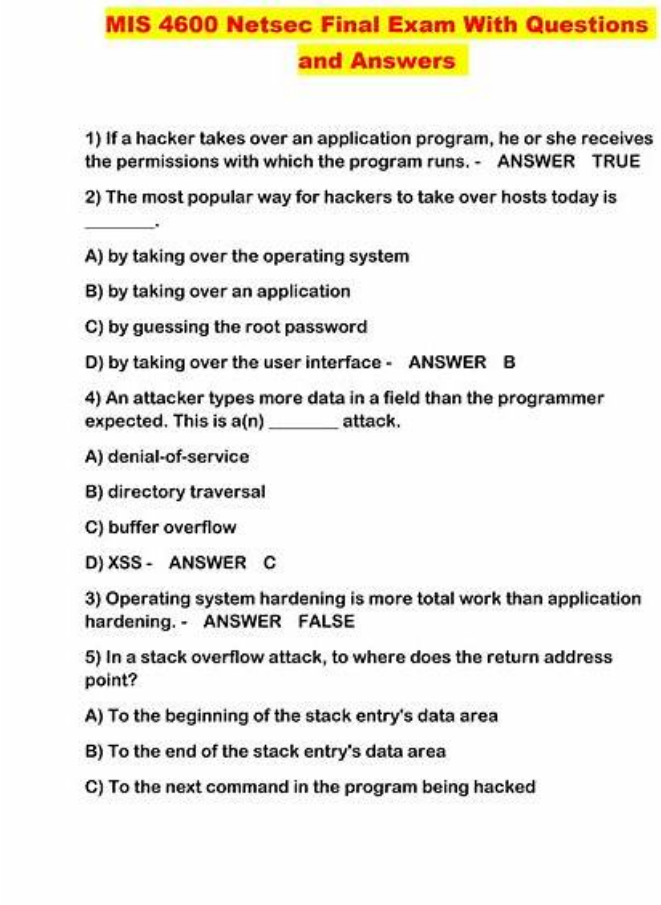
NetSec-Analyst Valid Exam Forum - NetSec-Analyst Valid Exam Sample



MIS 4600 Netsec Final Exam With Questions and Answers

1) If a hacker takes over an application program, he or she receives the permissions with which the program runs. - ANSWER TRUE

2) The most popular way for hackers to take over hosts today is _____.

A) by taking over the operating system

B) by taking over an application

C) by guessing the root password

D) by taking over the user interface - ANSWER B

4) An attacker types more data in a field than the programmer expected. This is a(n) _____ attack.

A) denial-of-service

B) directory traversal

C) buffer overflow

D) XSS - ANSWER C

3) Operating system hardening is more total work than application hardening. - ANSWER FALSE

5) In a stack overflow attack, to where does the return address point?

A) To the beginning of the stack entry's data area

B) To the end of the stack entry's data area

C) To the next command in the program being hacked

DOWNLOAD the newest PassTorrent NetSec-Analyst PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=13iB9Ze_mGnXCuKl13fctB-yU9muyIPj8

In this information-dominated society, boosting plenty stocks of knowledge and being competent in some certain area can establish yourself in society and help you get a high social status. Passing NetSec-Analyst certification can help you realize these goals and find a good job with high income. If you buy our NetSec-Analyst Practice Test you can pass the NetSec-Analyst exam successfully and easily. And if you study with our NetSec-Analyst exam questions for only 20 to 30 hours, you will pass the NetSec-Analyst exam easily.

Palo Alto Networks NetSec-Analyst Exam Syllabus Topics:

Topic	Details
Topic 1	• Policy Creation and Application: This section of the exam measures the abilities of Firewall Administrators and focuses on creating and applying different types of policies essential to secure and manage traffic. The domain includes security policies incorporating App-ID, User-ID, and Content-ID, as well as NAT, decryption, application override, and policy-based forwarding policies. It also covers SD-WAN routing and SLA policies that influence how traffic flows across distributed environments. The section ensures professionals can design and implement policy structures that support secure, efficient network operations.

Topic 2	• Management and Operations: This section of the exam measures the skills of Security Operations Professionals and covers the use of centralized management tools to maintain and monitor firewall environments. It focuses on Strata Cloud Manager, folders, snippets, automations, variables, and logging services. Candidates are also tested on using Command Center, Activity Insights, Policy Optimizer, Log Viewer, and incident-handling tools to analyze security data and improve the organization overall security posture. The goal is to validate competence in managing day-to-day firewall operations and responding to alerts effectively.
Topic 3	• Troubleshooting: This section of the exam measures the skills of Technical Support Analysts and covers the identification and resolution of configuration and operational issues. It includes troubleshooting misconfigurations, runtime errors, commit and push issues, device health concerns, and resource usage problems. This domain ensures candidates can analyze failures across management systems and on-device functions, enabling them to maintain a stable and reliable security infrastructure.
Topic 4	• Object Configuration Creation and Application: This section of the exam measures the skills of Network Security Analysts and covers the creation, configuration, and application of objects used across security environments. It focuses on building and applying various security profiles, decryption profiles, custom objects, external dynamic lists, and log forwarding profiles. Candidates are expected to understand how data security, IoT security, DoS protection, and SD-WAN profiles integrate into firewall operations. The objective of this domain is to ensure analysts can configure the foundational elements required to protect and optimize network security using Strata Cloud Manager.

NetSec-Analyst Valid Exam Sample & NetSec-Analyst Practice Test Fee

PassTorrent exam study material is essential for candidates who want to appear for the Palo Alto Networks NetSec-Analyst certification exams and clear it to validate their skill set. This preparation material comes with Up To 1 year OF Free Updates And Free Demos. Place your order now and get Real NetSec-Analyst Exam Questions with these offers.

Palo Alto Networks Network Security Analyst Sample Questions (Q228-Q233):

NEW QUESTION # 228
An organization relies heavily on cloud applications. Due to compliance requirements, they must log all successful and unsuccessful login attempts to sensitive cloud applications, including the user, application, and source IP. Additionally, they need to generate real-time alerts for any failed login attempts exceeding a threshold (e.g., 3 failed attempts within 5 minutes) from a single source IP to a sensitive application. How would you configure Palo Alto Networks firewall logs and profiles to meet these requirements?

- A. Enable 'Log at Session End' on the security policy for the sensitive applications. Configure an 'Alert Log' setting in the 'Monitor' tab for 'authentication-failed' messages with a threshold.
- B. Set the security policy 'Action' to 'Deny' for sensitive applications, which will automatically log failed attempts. Use an 'External Dynamic List' for sensitive application URLs and link it to a 'URL Filtering' profile that generates alerts on block actions.
- C. For the security policy governing sensitive cloud applications, set 'Log at Session End'. Create a 'Log Forwarding Profile' to forward 'Authentication' logs to the Panorama management server. On Panorama, configure a 'Managed Log Forwarding Profile' with an 'Email' alert for 'authentication-failed' events, and enable 'Alerting on Repeated Failures' with the specified threshold and timeframe.
- D. Enable 'SSL Decryption' for all cloud application traffic. Configure a 'Vulnerability Protection' profile with a custom signature to detect failed login attempts and set the action to 'alert'.
- E. Enable 'Log at Session Start' for the security policy. Create a custom 'Log Forwarding Profile' to send all traffic logs to an external SIEM. Configure the SIEM to generate alerts based on failed authentication events and thresholds.

Answer: C

Explanation:
Option C is the most comprehensive and correct approach. 1. Logging All Login Attempts: 'Log at Session End' on the security

policy ensures that the full session details, including application and user (if User-ID is enabled, which is crucial for this scenario), are logged. Successful and unsuccessful authentication attempts are part of these logs, especially if App-ID properly identifies the login process. 2. Real-time Alerts for Failed Attempts with Threshold: The key here is using the 'Authentication' logs, which are distinct from generic 'Traffic' logs and specifically contain authentication events. Forwarding these to Panorama (or a Syslog server, but Panorama provides built-in alerting). Panorama's 'Managed Log Forwarding Profile' allows for granular alerting on specific log types ('Authentication' logs in this case) and, critically, offers 'Alerting on Repeated Failures' with configurable thresholds for time and count from a source. This directly addresses the requirement for failed login attempt alerting with a threshold from a single source IP. Other options are less precise: A lacks the specific 'Authentication' log forwarding and thresholding mechanism. B offloads everything to the SIEM, which is valid but doesn't leverage the firewall's built-in advanced alerting. D (Vulnerability Protection) is for exploits, not authentication logging/alerting. E (Deny action and URL Filtering) is incorrect as it focuses on blocking and URL categorization rather than granular authentication logging and repeated failure alerting.

NEW QUESTION # 229
What two authentication methods on the Palo Alto Networks firewalls support authentication and authorization for role-based access control? (Choose two.)

- A. Kerberos
- B. LDAP
- C. TACACS+
- D. SAML

Answer: C,D

Explanation:
Reference:
The administrative accounts are defined on an external SAML, TACACS+, or RADIUS server. The server performs both authentication and authorization. For authorization, you define Vendor-Specific Attributes (VSAs) on the TACACS+ or RADIUS server, or SAML attributes on the SAML server. PAN-OS maps the attributes to administrator roles, access domains, user groups, and virtual systems that you define on the firewall.

NEW QUESTION # 230
Recently changes were made to the firewall to optimize the policies and the security team wants to see if those changes are helping. What is the quickest way to reset the hit counter to zero in all the security policy rules?

- A. Highlight a rule and use the Reset Rule Hit Counter > Selected Rules for each rule
- B. At the CLI enter the command reset rules and press Enter
- C. Reboot the firewall
- D. Use the Reset Rule Hit Counter > All Rules option

Answer: D

Explanation:
References:

NEW QUESTION # 231
What is considered best practice with regards to committing configuration changes?

- A. Validate configuration changes prior to committing
- B. Export configuration after each single configuration change performed
- C. Disable the automatic commit feature that prioritizes content database installations before committing
- D. Wait until all running and pending jobs are finished before committing

Answer: C

NEW QUESTION # 232
A large financial institution uses Panorama to manage their firewall estate. They are implementing a strict change management

process where all policy modifications, object creations, or deletions must be reviewed and approved before being committed and pushed. They want to ensure that only approved changes are present in the 'candidate config' before a commit, and that deviations are easily identifiable. Which Panorama feature, when combined with a robust operational process, helps enforce this requirement and identify discrepancies?

- A. Leverage the 'Validate' function before committing to check for syntax errors, combined with regular 'Config Audits' and comparing the running configuration with a golden configuration stored externally.
- B. Implement 'Config Locks' before making changes, ensuring only one administrator can modify the configuration at a time.
- C. Utilize 'Admin Roles' to restrict non-approved users from making any changes to the candidate configuration.
- D. Use 'Shared Policy' and 'Device Group Policy' hierarchies effectively, combined with the 'Revert' option for the candidate configuration if unapproved changes are found.
- E. Regularly export the candidate configuration (XML) and compare it against a baseline configuration using an external diff tool, then use 'Load Named Configuration' if a rollback is needed.

Answer: A,E

Explanation:
Both C and E contribute significantly to enforcing strict change management and identifying discrepancies, though in different ways. Option C suggests using Panorama's built-in 'Validate' function, which is essential for ensuring syntactical correctness and policy coherence. More importantly, it highlights 'Config Audits' (which can be done via Panorama's operational commands or API to compare running configs against desired states) and the comparison against a 'golden configuration' (often stored externally and managed by a version control system). This comparison is key to identifying unapproved deviations. Option E describes a more manual, but highly effective, programmatic approach. Regularly exporting the candidate configuration and using an external 'diff tool allows for precise identification of every change, approved or not. 'Load Named Configuration' provides a mechanism for rollback to a known good state. While Admin Roles (A) and Config Locks (B) are important for controlling access and concurrent edits, they don't directly identify unapproved changes already present in the candidate config. Option D is about configuration organization and rollback, but doesn't inherently identify unapproved changes before commit/push, only allows reverting them.

NEW QUESTION # 233
.....

□NetSec-Analyst Reliable Test Notes

- Authoritative NetSec-Analyst Valid Exam Forum - Pass NetSec-Analyst in One Time - Complete NetSec-Analyst Valid Exam Sample □ The page for free download of ▹ NetSec-Analyst ◃ on ✔ www.examcollectionpass.com □✔□ will open immediately □NetSec-Analyst Current Exam Content
- NetSec-Analyst Valid Guide Files □ NetSec-Analyst Valid Study Questions □ VCE NetSec-Analyst Dumps □ Download ▶ NetSec-Analyst ◀ for free by simply searching on 《 www.pdfvce.com 》 □VCE NetSec-Analyst Dumps
- Vce NetSec-Analyst Torrent □ Valid Braindumps NetSec-Analyst Questions □ New NetSec-Analyst Test Papers □ Open 《 www.troytecdumps.com 》 enter " NetSec-Analyst " and obtain a free download □VCE NetSec-Analyst Dumps
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, felbar.net, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.growwithiren.com, motionentrance.edu.np, www.stes.tyc.edu.tw, Disposable vapes

What's more, part of that PassTorrent NetSec-Analyst dumps now are free: https://drive.google.com/open?id=13iB9Ze_mGnXCuKl13fctB-yU9muyIPj8