Vendor: Oracle

Exam Code:1Z0-881

Exam Name: Oracle Solaris 10 Security Administrator Certified Expert Exam

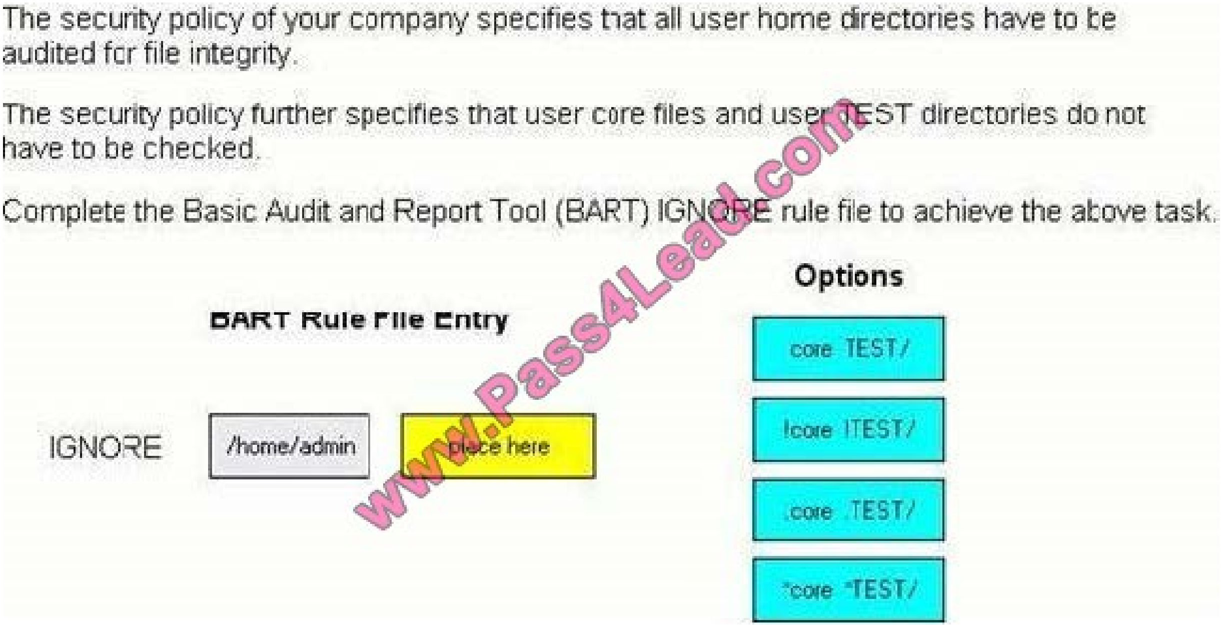
Version: Demo

QUESTION 1

Click the Task button.

Drag and drop question. Drag the items to the proper locations.

Select and Place:

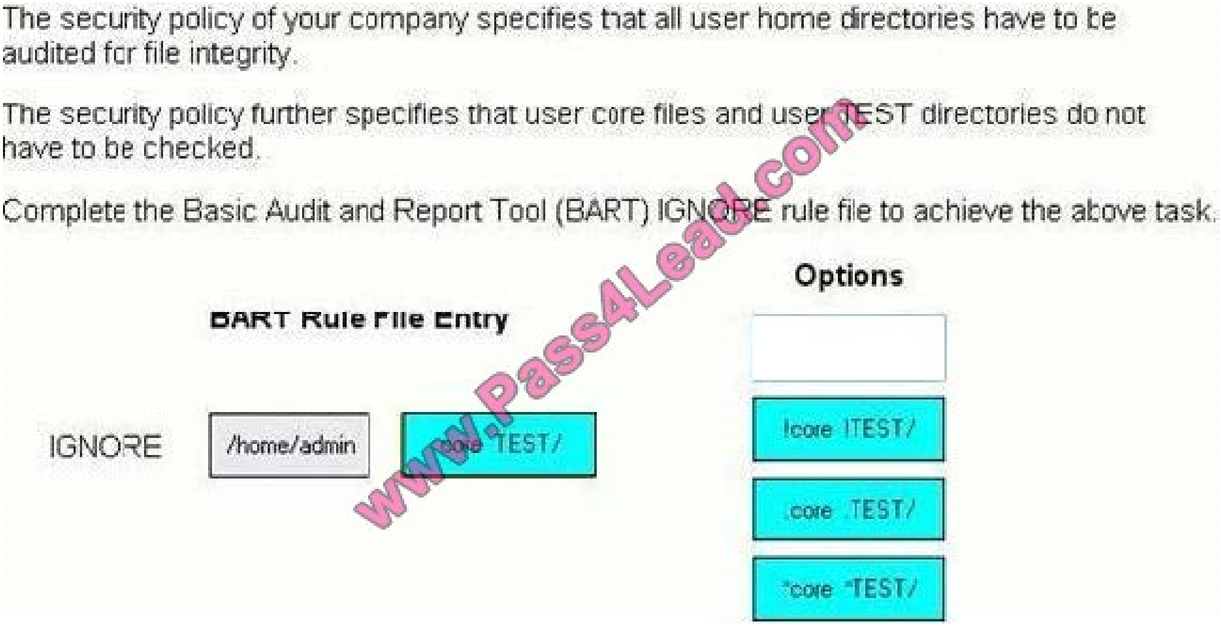


The security policy of your company specifies that all user home directories have to be audited for file integrity.

The security policy further specifies that user core files and user TEST directories do not have to be checked.

Complete the Basic Audit and Report Tool (BART) IGNORE rule file to achieve the above task.

Correct Answer:



The security policy of your company specifies that all user home directories have to be audited for file integrity.

The security policy further specifies that user core files and user TEST directories do not have to be checked.

Complete the Basic Audit and Report Tool (BART) IGNORE rule file to achieve the above task.

QUESTION 2

Which two tasks can you perform using the Audit facility? (Choose two.)

A. generate an overview of CPU usage by users

B. generate an overview of disk space occupied by a particular user

C. generate an overview of which users recently changed their password

D. generate an overview of the network bandwith in use by a particular user

E. generate an overview of all the applications executed by a particular user

Correct Answer: CE

QUESTION 3

Before a security administrator modifies the default privilege list used for a SMF start or stop method, it is important to first determine which privileges are actually needed by that service. Which three utilities determine what privileges are used by a program or service? (Choose three.)

A. ppriv

B. truss

C. pfexec

D. dtrace

E. svcadm

Correct Answer: ABD

QUESTION 4

A system administrator suspects that /etc/passwd or /etc/shadow has been modified without proper authorization. Which two methods or programs can be used to find out whether that happened? (Choose two.)

A. bart

B. pkgchk

C. pwdsign

D. file system backups

E. the Solaris Fingerprint Database

Correct Answer: AD

QUESTION 5

The svcs output of a system lists this service: legacy_run Jan_30 lrc:/etc/rc3_d/S52imq If the system administrator wants this service to be disabled permanently, which action needs to be taken?

A. /etc/init.d/imq stop

B. /etc/init.d/imq disable

C. svcadm disable lrc:/etc/rc3_d/S52imq

D. The system administrator can NOT disable any services which are started through legacy /etc/init.d scripts.

E. The system administrator needs to inspect the start script and check for a service-specific way to disable the service.

Correct Answer: E

QUESTION 6

A user needs to be able to mount the file system located on a USB memory stick on a workstation. How can you allow the user to mount and unmount this file system when required?

A. Give the user write access to /etc/vfstab.

B. Give the user write access to /etc/mnttab.

C. Assign the user the sys_mount privilege for the file system.

D. Enable and configure the automount daemon (automountd).

E. Enable and configure the volume management daemon (vold).

Correct Answer: E

QUESTION 7

Which two commands are part of Sun Update Connection? (Choose two.)

A. /usr/bin/pkgadm

B. /usr/bin/keytool

C. /usr/sbin/smpatch

D. /usr/sbin/patchadd

E. /usr/bin/updatemanager

Correct Answer: CE

QUESTION 8

A security administrator has a requirement to help configure and deploy a new server. What are two security tasks that the security administrator should perform? (Choose two.)

A. Configure the server to use LDAP for authentication.

B. Configure network interfaces and routing information.

C. Install a DTrace probe to capture the use of privileges.

D. Disable any network services that are NOT being used.

E. Apply software patches to correct security vulnerabilities.

Correct Answer: DE

QUESTION 9

You are administering a consolidated system with many zones, and have been asked to enable auditing. What must you do, after auditing has been enabled, to be able to distinguish between the audit events from different zones in the global zone\\'s audit trail?

A. Start auditd in each local zone.

B. Use the +perzone audit policy in the global zone.

C. Use the +zonename audit policy in the global zone.

D. Update audit_control in each local zone to include the zone name.

Correct Answer: C

QUESTION 10

How would you configure auditing to identify when an attacker has removed audit records?

A. Execute the command bsmconv +cnt and reboot.

B. Audit records already have sequence numbers by default.

C. auditconfig -setpolicy +cnt should be added to /etc/security/audit_startup.

D. auditconfig -setpolicy +seq should be added to /etc/security/audit_startup.

Correct Answer: D

QUESTION 11

Your employer has acquired a number of systems as a part of an acquisition of another company. You suspect that a number of the systems might have been hacked, so you want to remove any malicious software that might have been installed by the hacker. The systems have not previously had the Solaris Security Toolkit software used on them. Which would remove any software installed by the hacker?

A. Run Solaris Security Toolkit in audit mode, and remove anything it detects.

B. Reinstall Solaris on the system, and run Solaris Security Toolkit after installation.

C. Run Solaris Security Toolkit with the undo option, and then re-run it in normal mode.

D. Boot the system from CD-ROM and run Solaris Security Toolkit in standalone mode.

Correct Answer: B

QUESTION 12

A user started the ssh-agent followed by the ssh-add command. Afterwards the user connects to a remote system by using the ssh command. What will this ssh command do?

A. It requires the user to enter their pass-phrase.

B. It generates new keys from the user\\'s pass-phrase.

C. It allows the user to authenticate through the GSS-API.

D. It authenticates without asking for the user\\'s pass-phrase.

Correct Answer: D

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

100% Guaranteed Success

100% Money Back Guarantee

365 Days Free Update

Instant Download After Purchase

24x7 Customer Support

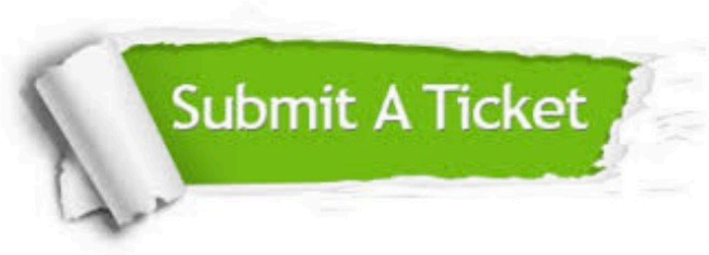
Average 99.9% Success Rate

More than 800,000 Satisfied Customers Worldwide

Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



One Year Free Update

Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.

Money Back Guarantee

To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.

Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.