



Oracle

Exam 1z0-881

Oracle Solaris 10 Security Administrator Certified Expert Exam

Version: 6.0

[Total Questions: 293]

Topic 1, Volume A

Question No : 1 - (Topic 1)

A security administrator has a requirement to deploy the Solaris Security Toolkit onto all Solaris servers in the department. In this environment, there are a variety of platforms and operating system versions deployed. Onto which two platforms and operating system combinations can the Solaris Security Toolkit be deployed in a supported configuration? (Choose two.)

- A. x86, Solaris 2.4
- B. x64, Solaris 9
- C. x86, Solaris 10
- D. SPARC, Solaris 2.6
- E. SPARC, Solaris 8

Answer: C,E

Question No : 2 - (Topic 1)

The company security policy now requires very detailed auditing of all actions. This includes capturing all executed commands together with their arguments and the environment variables. After activating auditing on all Solaris 10 systems, the security auditor complains about having to check the audit trail on each individual host. He asks for a central place to capture all audit trails. Using standard Solaris 10 security features, which is a solution to this problem?

- A. Configure auditd to send email with the events.
- B. Configure auditd to send the output using syslog to a central loghost.
- C. Configure auditd to store the audit trail using NFS on a central server.
- D. Configure auditd to store the audit trail using LDAP in a central directory.

Answer: C

Question No : 3 - (Topic 1)

Which two tasks does the Key Distribution Center (KDC) perform? (Choose two.)

- A. issues service tickets
- B. authenticates services
- C. issues ticket-granting-tickets
- D. validates passwords sent in clear text
- E. provides private sessions to services

Answer: A,C

Question No : 4 - (Topic 1)

Given:

jupiter:\$md5,rounds=2006\$2amXesSj5\$\$kCF48vfPsHDjIKNXeEw7V.:12210::: What is the characteristic of this /etc/shadow entry?

- A. User jupiter uses the md5 hash, with salt 2006\$2amXesSj5\$, and with the encrypted password \$kCF48vfPsHDjIKNXeEw7V.
- B. User jupiter uses the 2a hash, with 2006 iterations of the hash, with salt 2amXesSj5, and with the encrypted password kCF48vfPsHDjIKNXeEw7V.
- C. User jupiter uses the md5 hash, with 2006 iterations of the hash, with salt 2amXesSj5, and with the encrypted password kCF48vfPsHDjIKNXeEw7V.
- D. User jupiter uses the md5 hash, with 2006 iterations of the hash, with no salt, and with the encrypted password \$rQmXesSj5\$\$kCF48vfPsHDjIKNXeEw7V.

Answer: C

Question No : 5 - (Topic 1)

A security administrator is required to validate the integrity of a set of operating system files on a number of Solaris systems. The administrator decides to use the Solaris Fingerprint Database to validate configuration and data files as well as binaries and libraries. What command, available by default in Solaris 10, will help the security administrator collect the necessary information that will be used with the Solaris Fingerprint Database?

- A. md5sum

- B. digest
- C. encrypt
- D. elfsign
- E. cryptoadm

Answer: B

Question No : 6 - (Topic 1)

You are configuring a new system to be used as an intranet web server. After you have installed the minimal amount of packages and patched the system, you added the appropriate web server packages (SUNWapch2r and SUNWapch2u). By default, the web server daemon will be started using UID webservd and the basic privilege set. To comply with the company's policy of least privilege, you need to minimize the privileges that the web server will have. What will you modify to specify the privileges that the web service will run with?

- A. the PRIV_DEFAULT setting in /etc/security/policy.conf
- B. the defaultpriv setting of webservd in /etc/user_attr
- C. the privileges property of the web service in the SMF repository
- D. the privs property of the web service in /etc/security/exec_attr

Answer: C

Question No : 7 - (Topic 1)

After a recent audit, you have been requested to minimize an existing Solaris system which runs a third party database application. Which two should you do before starting to minimize the system? (Choose two.)

- A. Back up the system.
- B. Remove any unneeded patches.
- C. Install the SUNWrnet metacluster.
- D. Remove any unneeded packages.
- E. Confirm with the vendor of the database software that they support minimization.

Answer: A,E

Question No : 8 - (Topic 1)

Click the Exhibit button.

```
# ps -fp 734
      UID  PID PPID  C  STIME   TTY  TIME  CMD
webservd  734   1    0 00:26:43 ?    0:00
/usr/apache2/bin/httpd -k start

# pcred 734
734:   e/r/suid=80  e/r/sgid=80

# ppriv -S 734
734: /usr/apache2/bin/httpd -k start
flags = <none>
E: net_privaddr,proc_fork
I: net_privaddr,proc_fork
P: net_privaddr,proc_fork
L: zone
```

You maintain a minimized and hardened web server. The exhibit shows the current credentials that the web server runs with. You receive a complaint about the fact that a newly installed webbased application does not function. This application is based on a /bin/ksh cgi-bin script. What setting prevents this cgi-bin program from working?

- A. The system might NOT have /bin/ksh installed.
- B. The server is NOT allowed to call the exec system call.
- C. The server should run with uid=0 to run cgi-bin scripts.
- D. Some of the libraries needed by /bin/ksh are NOT present in the webserver's chroot environment.

Answer: B

Question No : 9 - (Topic 1)

One of the operators of the mainframe group was moved to the UNIX group and tasked to activate and configure password history. For every user, the last 10 passwords should be remembered in the history. In what file is the size of the password history configured?

- A. /etc/shadow
- B. /etc/pam.conf
- C. /etc/default/passwd

D. /etc/security/policy.conf

Answer: C

Question No : 10 - (Topic 1)

Within the context of file integrity, rules can be implemented to change the scope of the Basic Audit and Report Tool (BART) manifest. Given the rule file: /home/bert/docs *.og[dt] CHECK all IGNORE mtime Which two statements are valid? (Choose two.)

- A. All files on the system will be checked.
- B. The last modification time of all checked files will not be checked.
- C. Key words such as CHECK and IGNORE can NOT be used in a rule file.
- D. Only files with extension .ogt and .ogd in the directory /home/bert/docs will be checked.
- E. All files on the system will be checked, except for files with extensions .ogt and .ogd in the directory /home/bert/docs.

Answer: B,D

Question No : 11 - (Topic 1)

Solaris Auditing supports the selective logging of which two kinds of events? (Choose two.)

- A. file access by selected users
- B. access to selected files by all users
- C. selected users making outbound network connections
- D. password changes which do not meet the system password policy

Answer: A,C

Question No : 12 - (Topic 1)

A security administrator creates a directory called prevoy with the following access control policy: \$ getfacl prevoy # file: prevoy # owner:

secadm # group: secadm user::rwx group::r-x #effective:r-x mask:r-x other:r-x

default:user::r-- default:user:

sysadm:rw- default:group::r-- default:group:sysadm:rw- default:mask:rwx default:other:---

Into this directory, the security administrator creates a file called secrets. The ls command reports the following for the prevoy directory and secrets file: \$ ls -ld . secrets drwxr-xr-x+ 2 secadm secadm 512 Jun 6 16:38 . -r--r-----+ 1 secadm secadm

0 Jun 6 16:38 secrets Which two actions can be successfully taken by the sysadm role? (Choose two.)

- A. The sysadm role can read the secrets file.
- B. The sysadm role can write to the secrets file.
- C. The sysadm role can remove the secrets file.
- D. The sysadm role can create new files under the prevoy directory.
- E. The sysadm role can change the Access Control Lists of the prevoy directory.

Answer: A,B

Question No : 13 - (Topic 1)

The /etc/default/passwd file contains a number of configuration parameters that can be used to constrain the character composition of user passwords. What is one of the dangers of having password composition too tightly constrained?

- A. Password complexity rules apply only to the English alphabet.
- B. The entropy of the resulting password strings will be very high.
- C. Duplication of encrypted user password strings is much more likely.
- D. Limited password value possibilities can simplify brute force attacks.
- E. Passwords are harder to compute when using many character classes.

Answer: D

Question No : 14 - (Topic 1)

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/updatesmanager

Answer: C,E

Question No : 15 - (Topic 1)

To harden a newly installed Solaris OS, an administrator is required to make sure that syslogd is configured to NOT accept messages from the network. Which supported method can be used to configure syslogd like this?

- A. Run svcadm disable -t svc:/network/system-log.
- B. Edit /etc/default/syslogd to set LOG_FROM_REMOTE=NO.
- C. Edit /etc/rc2.d/S74syslog to start syslogd with the -t option.
- D. Edit /lib/svc/method/system-log to set LOG_FROM_REMOTE=NO.

Answer: B

Question No : 16 - (Topic 1)

Which are two advantages of the Service Management Facility compared to the init.d startup scripts? (Choose two.)

- A. It restarts processes if they die.
- B. It handles service dependencies.
- C. It has methods to start and stop the service.
- D. It specifies what the system should do at each run level.

Answer: A,B

Question No : 17 - (Topic 1)

You have been asked to implement defense in depth for network access to a system, where a web server will be running on an Internet-facing network interface. Which is NOT

contributing to the defense in depth?

- A. running the web server in a zone
- B. using svcadm to disable unused services
- C. using IP Filter to limit which network ports can be accessed from the Internet
- D. using VLANs on a single network interface instead of using multiple network interfaces
- E. using TCP wrappers to limit from which system SSH be used to connect to the system

Answer: D

Question No : 18 - (Topic 1)

A new security related patch has been released for the Solaris OS. This patch needs to be applied to the system that functions as your web server. The web server is configured to run in a non-global zone. Can you just use patch add to apply the patch to the global zone to update the web server zone?

- A. No, you need to shut down the web server zone first.
- B. Yes, patches will be automatically applied to all zones.
- C. No, you need to apply the patch to the web server zone separately.
- D. Yes, but you must make sure that the web server zone is booted first.

Answer: B

Question No : 19 - (Topic 1)

You decided it was worth maintaining an extremely paranoid policy when configuring your firewall rules. Therefore, you had your management approve the implementation of a security policy stance to deny all inbound connection requests to your corporate network. How is it possible that you still suffer from remote exploits that your adversaries are using to obtain interactive sessions inside your firewall?

- A. TCP splicing is easy to do.
- B. Internal software may be vulnerable.
- C. UDP vulnerabilities are well-known and exploited.
- D. ICMP hijacking attacks can still succeed through any firewall.

Answer: B

Question No : 20 - (Topic 1)

You have been asked to grant the user `envoy`, a member of the `staff` group, read and write access to the file `/app/notes` which has the following properties: `ls -l /app/notes -rw-rw---- 1 root app 0 Jun 6 15:11 /app/notes` Which options will NOT grant the user the ability to read and write the file?

- A. `usermod -G app envoy`
- B. `setfacl -m user:envoy:rw- /app/notes`
- C. `setfacl -m group:staff:rw- /app/notes`
- D. `usermod -K defaultpriv=basic,file_dac_read,file_dac_write envoy`

Answer: D

Question No : 21 - (Topic 1)

A security administrator has a requirement to make an encrypted backup copy of an application and its data, using the AES algorithm, so that it can be safely transmitted to a partner. Which two command sequences can be used to generate an encrypted backup of the files under `/app1`? (Choose two.)

- A. `crypt < /app1/* > app1.backup.aes`
- B. `encrypt -a aes -d /app1 -o app1.backup.aes`
- C. `tar cf - /app1 | gzip -d -e aes > app1.backup.aes`
- D. `ufsdump 0f - /app1 | crypt -a aes > app1.backup.aes`
- E. `ufsdump 0f - /app1 | encrypt -a aes -o app1.backup.aes`
- F. `tar cf - /app1 | openssl enc -out app1.backup.aes -aes-128-cbc`

Answer: E,F

Question No : 22 - (Topic 1)

A cryptographically signed patch provides system administrators with assurance that the patch possesses certain qualities. Which two qualities are assured when a patch signature

is verified? (Choose two.)

- A. The patch has a verified origin.
- B. The patch has NOT been modified since it was signed.
- C. The patch was created by a Sun Certified Systems Engineer.
- D. The contents of the patch have NOT been revealed to anyone who does NOT have a Sun service plan.

Answer: A,B

Question No : 23 - (Topic 1)

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.

Answer: D,E

Question No : 24 - (Topic 1)

Due to changes to the security policy of your organization, access restriction must be applied to systems. The changes specify that access to systems through the ftp protocol is NOT allowed according to the Human Resources department, which has the 10.10.10.0/24 address space assigned. TCP wrappers have been enabled for the ftp daemon, and these files have been configured: # cat /etc/hosts.allow in.ftpd: ALL # cat /etc/hosts.deny in.ftpd: 10.10.10.0/24 Despite the implemented configuration, Human Resources is still able to access systems through the ftp protocol. What action must be taken?

- A. The ftp daemon must be restarted.
- B. The inetd daemon must be restarted.
- C. The entry in the hosts.deny file is wrong and must be changed.
- D. The entry in the hosts.allow file is wrong and must be changed.

Answer: D

Question No : 25 - (Topic 1)

Packet filters and firewalls are an important component of any defense-in-depth security strategy. Which two types of threats can IP Filter be deployed as an effective countermeasure against? (Choose two.)

- A. a Christmas Tree scan
- B. an attempt to log in to a system using SSH by an unauthorized user
- C. an attempt to exploit a SQL injection vulnerability in a web storefront application
- D. an attempt to exploit a buffer overflow vulnerability in rpcbind, originating from a host on an authorized network
- E. an attempt to exploit a buffer overflow vulnerability in rpcbind, originating from a host on an unauthorized network

Answer: A,E

Question No : 26 - (Topic 1)

An Internet service provider is offering shell accounts on their systems. As a special service, customers can also apply for a root account to get their own virtual machine. The provider has implemented this by using zones, and the customers get root access to the non-global zone. One of their customers is developing cryptographic software and is using the ISP machine for testing newly developed Solaris crypto providers. What kind of testing is available to this developer?

- A. The developer is able to test newly developed user-level providers.
- B. The developer is able to test newly developed kernel software providers.
- C. The developer can NOT test newly developed providers in a non-global zone.
- D. The developer is able to do the same tests as if developing as root in the global zone.

Answer: A

Question No : 27 - (Topic 1)

A security administrator is required to periodically validate binaries against the Solaris Fingerprint Database. While attempting to capture MD5 file signatures for key Solaris OS files, the security administrator encounters the following error: digest: no cryptographic provider was found for this algorithm -- md5 What command should the administrator use to help determine the cause of the problem?

- A. crypt
- B. digest
- C. kcfadm
- D. openssl
- E. cryptoadm

Answer: E

Question No : 28 - (Topic 1)

Your company is running a DNS test server on the internal network. Access to this server must be blocked by using IP Filter. The administrator prefers that this access control is not obvious to someone trying to contact the server from the outside. Which rule implements the access control but hides the use of IP Filter to the outside?

- A. pass in quick on eri0 from 192.168.0.0/24 to any
- B. block in quick proto udp from any to any port = 53
- C. pass out quick on eri0 proto icmp from 192.168.1.2 to any keep state
- D. block return-icmp(port-unr) in proto udp from any to 192.168.1.2 port = 53

Answer: D

Question No : 29 - (Topic 1)

Which option is used in /etc/vfstab to limit the size of a tmpfs file system to 512MB to prevent a memory denial of service (DoS)?

- A. size=512m
- B. maxsize=512
- C. minsize=512
- D. swapfs=512mb

Answer: A

Question No : 30 - (Topic 1)

The Key Distribution Center (KDC) is a central part of the Kerberos authentication system. How should the system running the KDC be configured?

- A. It should be a hardened, minimized system.
- B. It should be a hardened, non-networked system.
- C. The KDC implementation employs cryptography and can therefore run securely on an ordinary multi-user system.
- D. For improved security, users must log in to the KDC before authenticating themselves, so it must be a multiuser system.

Answer: A

Question No : 31 - (Topic 1)

Which two components are part of the Solaris Cryptographic Framework? (Choose two.)

- A. single sign-on capabilities
- B. encryption and decryption
- C. random number generation
- D. Kerberos principle generation

Answer: B,C

Question No : 32 - (Topic 1)

The Solaris 10 cryptographic framework provides user-level commands to encrypt files. A combination of commands is reported below: `# tar cvf - /data | encrypt -a arcfour -k /tmp/key -o /tmp/backup` Which two statements are true? (Choose two.)

- A. The key can NOT be a file.
- B. The backup will be an encrypted file.

- C. arcfour is NOT a valid encryption algorithm.
- D. The tar command invocation is NOT correct.
- E. The /data directory is backed up and encrypted.

Answer: B,E

Question No : 33 - (Topic 1)

The security administrator wants to log all changes that are made to the device policy. Which Solaris 10 subsystem will be used to log changes to the device policy?

- A. syslog facility
- B. Fault Manager
- C. Solaris Auditing
- D. System Event facility

Answer: C

Question No : 34 - (Topic 1)

A system administrator is new to the Solaris cryptographic framework. During minimization and hardening, the system administrator discovered a running `/usr/lib/crypto/kcfd` and disabled this daemon. To verify the integrity of a Solaris binary, the system administrator is comparing the MD5 checksum of a binary with the information from the Solaris Fingerprint Database at SunSolve. To get the local checksum, he is using the command `digest`. What will happen when executing this command?

- A. The command will fail with an error.
- B. The command will run as usual and provide the MD5 sum.
- C. The command will run but won't be able to use any installed crypto accelerator hardware (if installed).
- D. The command will run slower because the kernel function can't be accessed, and the userland implementation (`libmd5.so.1`) will be used.

Answer: A

Question No : 35 - (Topic 1)

In which Solaris OS subsystem is User Rights Management implemented?

- A. Process Privileges
- B. Mandatory Access Control
- C. Service Management Facility
- D. Discretionary Access Control
- E. Role Based Access Control (RBAC)

Answer: E

Question No : 36 - (Topic 1)

It is corporate practice to use the Solaris Security Toolkit on all Sun systems. This has been successfully done for years, and the administrators are experienced with the tool. Starting with Solaris 10, the company now also uses Solaris zones. Which two statements regarding Solaris Security Toolkit are correct? (Choose two.)

- A. All minimization and hardening is done from the global zone.
- B. The Solaris Security Toolkit should be run in the non-global zone after installation.
- C. Configuration of the global zone does not impact hardening of the non-global zone.
- D. Hardening and auditing with the Solaris Security Toolkit can be done within each individual zone.

Answer: B,D

Question No : 37 - (Topic 1)

In which two ways can a service administrator specify the privilege set of a particular service in the Service Management Facility? (Choose two.)

- A. Set this using the svcs command.
- B. Import an updated service manifest.
- C. Modify the privilege set using svccfg.
- D. Change the privilege set by using svcprop.

Answer: B,C

Question No : 38 - (Topic 1)

Click the Exhibit button.

```
# Default definition for Password management
# Used when service name is not explicitly mentioned
# for password management
#
other password required pam_dhkeys.so.1
other password requisite      pam_authtok_get.so.1
other password requisite      pam_authtok_check.so.1
other password required pam_authtok_store.so.1
```

To implement dictionary checks at password-change time, your company has acquired a PAM module that performs these checks. Which two locations would put this module in the PAM stack when you install this module as an additional strength checking measure? (Choose two.)

- A. before the line containing pam_dhkeys.so.1
- B. after the line containing pam_authtok_check.so.1
- C. after the line containing pam_authtok_store.so.1
- D. before the line containing pam_authtok_check.so.1
- E. replace the line containing pam_authtok_check.so.1

Answer: B,D

Question No : 39 - (Topic 1)

On a system with these settings in audit_control: dir:/var/audit flags:lo,ex,nt naflags:na minfree:20 Which will NOT be a factor in the size of the audit trail generated by the system?

- A. the audit policy settings
- B. the number of active users
- C. the settings in audit_user
- D. the settings in audit_event
- E. the amount of memory in the system

Answer: E

Question No : 40 - (Topic 1)

The security administrator has created a Basic Audit and Report Tool (BART) control manifest for the /etc directory. A test manifest is created about one hour later, and the two manifests are compared. The administrator checks all attributes for the files in /etc. Which event will NOT be reported by comparing the two manifests with BART?

- A. A file link was removed.
- B. A file was added to the directory.
- C. Permissions on a file were changed.
- D. Permissions on a file were changed and then restored.
- E. A file was examined using vi, edited, restored to original, and saved.

Answer: D

Question No : 41 - (Topic 1)

A security administrator would like to restrict the number of simultaneous lightweight processes (LWPs) that the webadm role may have at any given time. The security administrator has created the following policy in /etc/projects:
user.webadm:10000::::task.max-lwps=(privileged,5,deny) What will be the impact if the webadm role attempted to start a sixth LWP?

- A. The LWP creation attempt will fail and an error code will be returned to the initiating process.
- B. The LWP will be created and webadm's oldest LWP will be suspended until sufficient resources become available.
- C. The LWP creation attempt will fail but the system will automatically retry until the LWP has been successfully created.
- D. The LWP creation attempt will suspend until sufficient resources become available allowing the LWP to be created.
- E. The LWP will be created but it will immediately be suspended until sufficient resources become available for it to run.

Answer: A

Question No : 42 - (Topic 1)

Which of the descriptions is a high-level overview of how Kerberos works?

- A. In a Kerberos environment, a user authenticates once to each service.
- B. In a Kerberos environment, a user authenticates once to a central authority.
- C. In a Kerberos environment, a user needs to type a password for each service.
- D. In a Kerberos environment, a user authenticates once to any service of its choosing and is then pre authenticated for all other services.

Answer: B

Question No : 43 - (Topic 1)

By default, what are two benefits of enabling Solaris Auditing in the global zone on a system where non-global zones (NGZ) have been deployed? (Choose two.)

- A. Audit daemons are started within each of the running NGZ.
- B. No one within an NGZ can modify the audit logs for that NGZ.
- C. Individual NGZ audit logs are accessible from within the NGZ.
- D. Audit configuration settings cannot be changed inside of an NGZ.

Answer: B,D

Question No : 44 - (Topic 1)

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).

Answer: E

Question No : 45 - (Topic 1)

Which item in the list would be specifically required for a VPN compared to a mode without encryption?

- A. Authentication Header (AH)
- B. Internet Key Exchange (IKE)
- C. Encapsulating Security Payload (ESP)
- D. Streams Control Transmission Protocol (SCTP)

Answer: C

Question No : 46 - (Topic 1)

A security administrator needs to configure a Solaris system to act as a firewall between your company's corporate network and the Internet, using Solaris IP Filter software to control the traffic passing between these two networks. Which is an efficient way to limit the software that can be run on this system?

- A. Use IPsec to limit execution of non-system binaries.
- B. Use the Solaris Security Toolkit and allow it to automatically minimize the system.
- C. Install Solaris using the Entire Distribution Metacluster, and remove any unneeded packages.
- D. Install Solaris using the Reduced Networking Core System Metacluster and add any extra required packages.

Answer: D

Question No : 47 - (Topic 1)

The development group would like to secure their network with IPsec. The number of hosts changes frequently, and they do not want to maintain preshared keys manually. The solution is to use IPsec with IKE and public keys. Which command is used to generate the IKE public/private key pair?

- A. ikeadm
- B. ikecert
- C. ipseckey
- D. cryptoadm
- E. ipsecconf

Answer: B

Question No : 48 - (Topic 1)

Click the Exhibit button.

```
sm          76 Tue Apr 19 10:41:00 MDT 2005
118735-01/.diPatch
sm          169 Tue Apr 19 10:41:02 MDT 2005
118735-01/patchinfo
sm          1991 Tue May 24 08:40:42 MDT 2005
118735-01/README.118735-01
sm          435 Tue Apr 26 15:24:32 MDT 2005
118735-01/SUNWnisu/pkgmap
sm          555 Tue Apr 26 15:24:32 MDT 2005
118735-01/SUNWnisu/pkginfo
sm          5768 Tue Apr 19 10:41:02 MDT 2005
118735-01/SUNWnisu/install/i.none
sm          37712 Tue Apr 26 15:23:10 MDT 2005
118735-01/SUNWnisu/reloc/usr/sbin/rpc.nisd_resolv
2047 Tue May 24 09:08:18 MDT 2005
META-INF/manifest.mf
2155 Tue May 24 09:08:18 MDT 2005
META-INF/es-signature.sf
3820 Tue May 24 09:08:26 MDT 2005
META-INF/es-signature.rsa

s = signature was verified
m = entry is listed in manifest
k = at least one certificate was found in keystore
i = at least one certificate was found in identity
scope
```

Based on this output from verifying a signed patch, which statement is correct?

- A. The patch is correctly signed.
- B. The patch signature manifest is invalid.
- C. The patch signature hash was NOT supplied.
- D. The patch signature is invalid, because NOT all files are signed.

Answer: A

Question No : 49 - (Topic 1)

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

Answer: A,B,D

Question No : 50 - (Topic 1)

Which naming service does NOT support password expiration?

- A. files
- B. NIS
- C. NIS+
- D. LDAP

Answer: B

Question No : 51 - (Topic 1)

Your company has acquired a small company and your task is to set up the first Solaris server in their network. As there is no existing JumpStart environment, you will have to start from scratch. Which metacluster is best suited for initial installation of a strict minimized system?

- A. Entire Distribution (SUNWCall)
- B. Core Software Support (SUNWreq)
- C. End User System Support (SUNWCuser)
- D. Reduced Networking Core System Support (SUNWCrnet)

Answer: D

Question No : 52 DRAG DROP - (Topic 1)

Click the Task button.

The Solaris 10 OS supports a number of password-related security controls, including minimum password length, password aging, password history, password complexity rules, and password dictionary lookup.

Place each password control item next to its appropriate description.

Password Control Description	Password Control Item
Prevents a user from selecting a commonly used word as a password	password length
Determines the minimum acceptable length of a user's password	password aging
Determines the minimum character class requirements for a user's password	password history
Determines how often a user's password must be changed	password complexity
Prevents a user from selecting a previously used password	password lookup

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

Answer:

Password Control Description	Password Control Item
password lookup	password length
password aging	password aging
password length	password history
password history	password complexity
password complexity	password lookup

Question No : 53 - (Topic 1)

The kernel calculates the effective set of privileges based on three other privilege sets. This calculation begins with the set of privileges inherited from the parent process. The effective set is then further constrained by two other sets of privileges. Which two describe the remaining privilege sets? (Choose two.)

- A. Permitted set - a subset of the inheritable set
- B. Limit set - the outside limit of privileges available to the process
- C. Basic set - the privileges which define the system security policy
- D. Implicit set - the set of privileges required by a process to function correctly
- E. Disallowed set - the set of privileges specifically withheld in the process owner's profile

Answer: A,B

Question No : 54 DRAG DROP - (Topic 1)

Click the Task button.

Place the RBAC database names on the correct descriptions.

Place the RBAC database names on the correct descriptions.

Descriptions	Database Names
Stores the name, description, help file location, and authorizations that are assigned to rights profiles	exec_attr
This database defines commands that require security attributes to succeed.	prof_attr
Contains user and role information that supplements the passwd and shadow databases	user_attr
Assigns authorizations to users, to roles, or to rights profiles	auth_attr

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

Answer:

Place the RBAC database names on the correct descriptions.

Descriptions	Database Names
prof_attr	exec_attr
exec_attr	prof_attr
user_attr	user_attr
auth_attr	auth_attr

Question No : 55 - (Topic 1)

You suspect that the /usr/bin/lbinary on a system might have been replaced with a "Trojan horse." You have been able to determine that the correct MD5 checksum for the real /usr/bin/l binary is: md5 (/usr/bin/l) = b526348afd2d57610dd3635e46602d2a Which standard Solaris command can be used to calculate the MD5 checksum for the /usr/bin/l file?

- A. md5 /usr/bin/lS
- B. sum -r /usr/bin/lS
- C. sum -a md5 /usr/bin/lS
- D. crypt -a md5 /usr/bin/lS
- E. digest -a md5 /usr/bin/lS

Answer: E

Question No : 56 - (Topic 1)

Which two statements regarding patching are correct? (Choose two.)

- A. A patching strategy should form part of your security policy.
- B. Only security patches should ever be installed on a secure system.
- C. Hardening a system can reduce the time required to apply patches.
- D. Minimizing a system can reduce the time required to apply patches.
- E. All patches should be installed as soon as possible after they are released.

Answer: A,D

Question No : 57 - (Topic 1)

Click the Exhibit button.

```
# ./jass-check-sum

Checking for file signature conflicts associated with
Toolkit run:
20060327184151

File Name                Saved CkSum              Current
CkSum
-----
-----
/etc/default/login      945ea2864f7ab9fb6e5
84c46adc914e3700ef24
/etc/passwd             ef3b98727a6b09dd8f1
d9f608df73db144a4913
```

What is the significance of the output generated by the jass-check-sum command?

- A. The two files were deleted since the last Solaris Security Toolkit run.
- B. The two files were created since the last Solaris Security Toolkit run.
- C. The two files were modified since the last Solaris Security Toolkit run.
- D. The two files were archived since the last Solaris Security Toolkit run.

Answer: C

Question No : 58 - (Topic 1)

For security reasons, one of the services your department provides has to be run in a separate zone. Which three of the zone's properties can differ from the global zone? (Choose three.)

- A. the zone's IP address
- B. the zone's system time
- C. the zone's domain name
- D. the zone's root password
- E. the zone's kernel patch level

Answer: A,C,D

Question No : 59 - (Topic 1)

Which three are examples of network security mechanisms? (Choose three.)

- A. IPsec
- B. syslog
- C. Kerberos
- D. TCP Wrappers
- E. Network File System
- F. Basic Security Module
- G. Role Based Access Control (RBAC)

Answer: A,C,D

Question No : 60 DRAG DROP - (Topic 1)

Click the Task button.

Place the Solaris facilities below on the feature they provide.

Place the Solaris facilities below on the feature they provide.

place here	Limit process visibility
place here	Provide minimum guaranteed performance
place here	Dedicate CPU resources
place here	Limit maximum CPU time

Solaris Facility

Resource Pools	Resource Controls	Solaris Zones	Fair Share Scheduler
----------------	-------------------	---------------	----------------------

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

Answer:

Place the Solaris facilities below on the feature they provide.

Solaris Zones	Limit process visibility
Fair Share Scheduler	Provide minimum guaranteed performance
Resource Pools	Dedicate CPU resources
Resource Controls	Limit maximum CPU time

Solaris Facility

Resource Pools	Resource Controls	Solaris Zones	Fair Share Scheduler
----------------	-------------------	---------------	----------------------

Question No : 61 - (Topic 1)

Which IPsec mechanism provides confidentiality for network traffic?

- A. AH
- B. IKE
- C. ESP
- D. SKIP

Answer: C

Question No : 62 - (Topic 1)

An administrator has applied patch 120543-02 to a server. Unfortunately, this patch is causing compatibility problems with one of the core applications running on that server. The patch needs to be backed out to solve the application problems. Which command performs the uninstallation of this patch?

- A. pkgrm 120543-02
- B. patchadm -d 120543-02

- C. patchremove 120543-02
- D. smpatch remove -i 120543-02
- E. rm -rf /var/sadm/patch/120543-02

Answer: D

Question No : 63 - (Topic 1)

Which are two advantages of the Service Management Facility compared to the init.d startup scripts? (Choose two.)

- A. It restarts processes if they die.
- B. It handles service dependencies.
- C. It has methods to start and stop the service.
- D. It specifies what the system should do at each run level.

Answer: A,B

Question No : 64 - (Topic 1)

Which action can a system administrator with the solaris.smf.modify.sendmail authorization execute?

- A. svcadm enable sendmail
- B. svcadm refresh sendmail
- C. svcadm disable sendmail
- D. svccfg -s sendmail listprop

Answer: D

Question No : 65 - (Topic 1)

You suspect that the /usr/bin/lis binary on a system might have been replaced with a "Trojan horse." You have been able to determine that the correct MD5 checksum for the real /usr/bin/lis binary is: md5 (/usr/bin/lis) = b526348afd2d57610dd3635e46602d2a Which

standard Solaris command can be used to calculate the MD5 checksum for the /usr/bin/lis file?

- A. md5 /usr/bin/lis
- B. sum -r /usr/bin/lis
- C. sum -a md5 /usr/bin/lis
- D. crypt -a md5 /usr/bin/lis
- E. digest -a md5 /usr/bin/lis

Answer: E

Question No : 66 - (Topic 1)

Click the Exhibit button.

```
# ps -fp 734
      UID  PID PPID  C  STIME   TTY  TIME  CMD
webservd  734  1    0 00:26:43 ?    0:00
/usr/apache2/bin/httpd -k start

# pcred 734
734:  e/r/suid=80  e/r/sgid=80

# ppriv -S 734
734: /usr/apache2/bin/httpd -k start
flags = <none>
E: net_privaddr,proc_fork
I: net_privaddr,proc_fork
P: net_privaddr,proc_fork
L: zone
```

You maintain a minimized and hardened web server. The exhibit shows the current credentials that the web server runs with. You receive a complaint about the fact that a newly installed webbased application does not function. This application is based on a /bin/ksh cgi-bin script. What setting prevents this cgi-bin program from working?

- A. The system might NOT have /bin/ksh installed.
- B. The server is NOT allowed to call the exec system call.
- C. The server should run with uid=0 to run cgi-bin scripts.
- D. Some of the libraries needed by /bin/ksh are NOT present in the webserver's chroot environment.

Answer: B

Question No : 67 DRAG DROP - (Topic 1)

Click the Task button.

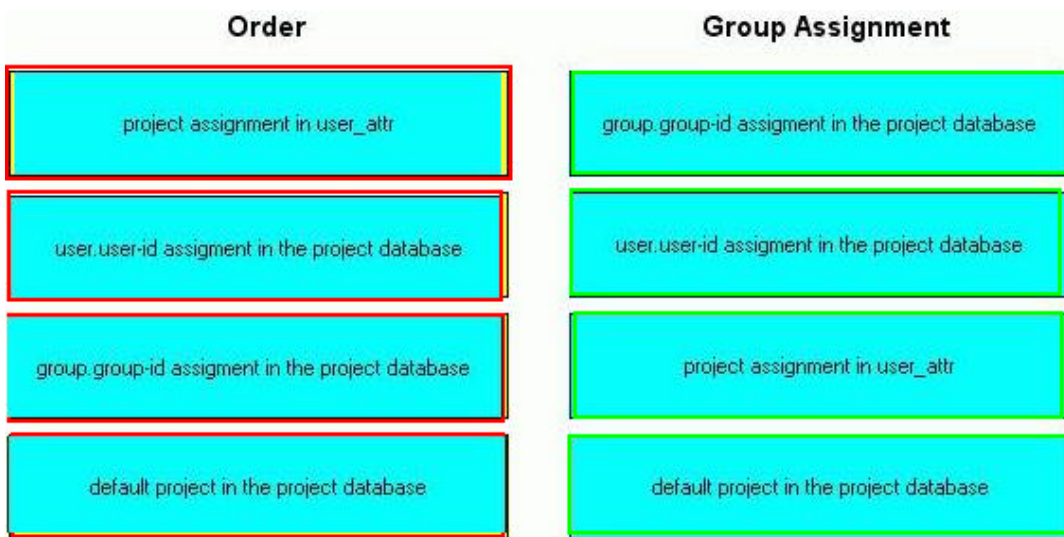
When a user logs into a Solaris 10 system, a default project for the use is located.

Place the locations in the order in which the Solaris OS searches for the user's default project.

Order	Group Assignment
1st	group.group-id assignment in the project database
2nd	user.user-id assignment in the project database
3rd	project assignment in user_attr
4th	default project in the project database

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

Answer:



Question No : 68 - (Topic 1)

A Solaris 10 system has IP Filter enabled and configured. A section of the /etc/ipf/ipf.conf configuration file is reported below: block return-rst in quick proto tcp from any to any port = 23 flags S block return-icmp (port-unr) in proto udp from any to any port > 3000 Which two statements are true? (Choose two.)

- A. The system blocks TCP RST packets.
- B. The system will block incoming telnet connections and returns a TCP RST packet.
- C. The system will block all incoming echo requests and replies with an ICMP port unreachable packet.
- D. The system does NOT return ICMP-type packets for UDP incoming connections received on ports greater than 3000.
- E. The system will block and replay with an ICMP port unreachable packet to UDP connections received for ports greater than 3000.

Answer: B,E

Question No : 69 - (Topic 1)

Which two statements are true about roles in the Solaris 10 OS? (Choose two.)

- A. Roles can only be assumed by authorized users.
- B. su is the only way that a user can assume a role.

- C. Roles require the use of passwords for authentication.
- D. rolemod can be used to allow roles to access other roles.
- E. Roles do NOT have their own UID, GID, or home directory.

Answer: A,B

Question No : 70 - (Topic 1)

A system administrator wants to remove most of the basic privileges for ordinary users and adds the following line to the appropriate configuration file to achieve this:

```
PRIV_DEFAULT=basic,!proc_info,!proc_session,!
```

file_link_any It would be shorter to list the two remaining privileges specified in Solaris 10. Should the administrator have written this instead?

```
PRIV_DEFAULT=proc_exec,proc_fork
```

- A. Yes, the shorter form is preferred.
- B. Yes, both forms will always be equivalent.
- C. No, the basic set might change in future releases.
- D. No, both forms are wrong. You cannot remove basic privileges.

Answer: C

Question No : 71 - (Topic 1)

A security administrator has been asked to construct a Solaris Security Toolkit security profile (that is, driver) to enable Solaris Auditing. If the security administrator starts with the secure.driver profile, which Finish script must be added to enable Solaris Auditing?

- A. enable-bsm.fin
- B. install-bsm.fin
- C. enable-auditing.fin
- D. install-auditing.fin

Answer: A

Question No : 72 - (Topic 1)

Which two statements about the digest and mac commands are true? (Choose two.)

- A.** The mac command can use the Digital Encryption Standard (DES) in cipher-block chained (CBC) mode. The digest command can NOT.
- B.** The mac command uses a distinct class of hash functions called message authentication codes (MACs). MAC functions combine the input file with a key supplied by the user, returning a fixed length digest.
- C.** The mac command uses a distinct class of hash functions called MACs. A MAC function combines the input file with a randomly generated salt, and returns a digest.
- D.** The digest command requires that the user supply a key. The mac command does NOT. The digest command takes an input file, combines it with the key, and a variable length digest is returned.

Answer: A,B

Question No : 73 - (Topic 1)

The company you work for is leasing zones to customers to run their applications in. You want each customer to be able to run the zoneadm command to start their zone in case of accidental shutdown, and also zlogin so they can access the console of their zone. Which are three reasons why you should NOT create accounts for them in the global zone and grant them the Zone Management profile? (Choose three.)

- A.** They will be able to reboot the global zone.
- B.** They will be able to reboot other customers' zones.
- C.** They will be able to log in to other customers' zones.
- D.** They will be able to see processes in other customers' zones.
- E.** They will be able to disable auditing in other customers' zones.

Answer: B,C,D

Question No : 74 - (Topic 1)

In which location is the signature for a signed binary found?

- A. the ELF header
- B. a trailer attached to the file
- C. stored in a system database
- D. added to the binary at compile time
- E. created and stored in memory at system boot

Answer: A

Question No : 75 - (Topic 1)

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 bandwidth in use by a particular user
- E. generate an overview of all the applications executed by a particular user

Answer: C,E

Question No : 76 - (Topic 1)

To enforce security within your organization, access restrictions to systems must be applied. In particular, restrictions to the telnet protocol must be configured. Which action must be taken to enable TCP wrappers for the telnet protocol?

- A. `svcadm tcp_wrappers start`
- B. `svcadm enable tcp_wrappers`
- C. `inetadm -m telnet=tcp_wrappers`
- D. `inetadm -m telnet tcp_wrappers=true`

Answer: D

Question No : 77 - (Topic 1)

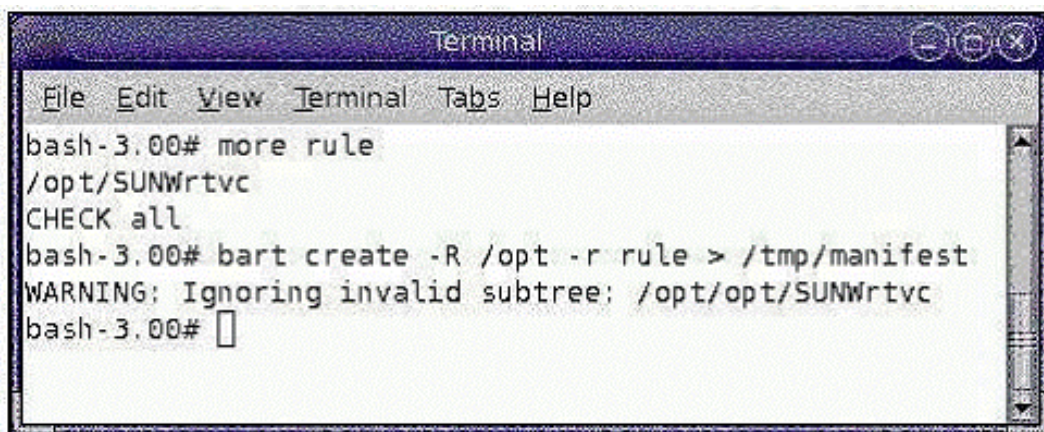
To improve accountability on a Solaris system, the security administrator decides to configure the root account to be a Solaris role. What are two considerations that the security administrator should understand before making this change? (Choose two.)

- A. Only authorized users will be able to access root.
- B. root will no longer be able to use the su command.
- C. New privileges will need to be assigned to the root role.
- D. Scheduled cron jobs for the root role will no longer run.
- E. root will no longer be able to log in at the system console.

Answer: A,E

Question No : 78 - (Topic 1)

Click the Exhibit button.



```
Terminal
File Edit View Terminal Tabs Help
bash-3.00# more rule
/opt/SUNWrtvc
CHECK all
bash-3.00# bart create -R /opt -r rule > /tmp/manifest
WARNING: Ignoring invalid subtree: /opt/opt/SUNWrtvc
bash-3.00#
```

The Exhibit shows the contents of a file named rule, and the output of a Basic Audit and Report Tool (BART) command. The purpose of the command is to create a manifest file of the directory /opt/SUNWrtvc, but unfortunately the command did not succeed. What caused the error from BART?

- A. BART creates only manifest files for the entire system.
- B. The -r rule option has to be removed from the command.
- C. The -R /opt option has to be removed from the command.
- D. The subcommand create has to be removed from the command.

Answer: C

Question No : 79 - (Topic 1)

For security reasons, one of the services your department provides has to be run in a separate zone. Which three of the zone's properties can differ from the global zone? (Choose three.)

- A. the zone's IP address
- B. the zone's system time
- C. the zone's domain name
- D. the zone's root password
- E. the zone's kernel patch level

Answer: A,C,D

Question No : 80 - (Topic 1)

A system administrator wants to share NFS file systems to two different sets of systems. Both sets of systems require integrity checks and Kerberos authentication. The second set of systems also requires encryption. What option is open to the system administrator?

- A. Use an NFS server in two different zones, sharing the same data.
- B. Share the same file system with different sec options for both sets of clients.
- C. Share the file system only with NFSv4, because older NFS versions do not support this.
- D. Logically divide the file system into two separate file systems, each shared with different sec options.

Answer: B

Question No : 81 - (Topic 1)

The digital signature of a patch provides an integrity check of the patch. Which is a requirement for signed patches?

- A. The system administrator needs to sign the patch.
- B. All patches need to be signed by Sun Microsystems.
- C. Signed patches need to be downloaded through SSL.
- D. Vendors can sign patches only with approval from Sun Microsystems.

E. The system administrator can specify which Certification Authorities are trusted for signed patches.

Answer: E

Question No : 82 - (Topic 1)

Which two are concerned with security threats? (Choose two.)

- A. integrity
- B. scalability
- C. performance
- D. confidentiality

Answer: A,D

Question No : 83 - (Topic 1)

On a system with these settings in audit_control: dir:/var/audit flags:lo,ex,nt naflags:na minfree:20 Which will NOT be a factor in the size of the audit trail generated by the system?

- A. the audit policy settings
- B. the number of active users
- C. the settings in audit_user
- D. the settings in audit_event
- E. the amount of memory in the system

Answer: E

Question No : 84 - (Topic 1)

Which prints out all world-writable files?

- A. find / -perm -a=w -print

- B. find / -perm -o=w -print
- C. find / -perm -u=w -print
- D. find / -perm -a=777 -print

Answer: B

Question No : 85 - (Topic 1)

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.

Answer: D,E

Question No : 86 - (Topic 1)

After minimizing and hardening a system, application software was installed but could not run. The administrator already found that /usr/lib/libz.so.1 is missing on the system. The package containing this library needs to be installed, but the administrator does not know the name of the corresponding package. The system is booted from the installed OS and the installation media is mounted. Which command can be used to find the name of the package which needs to be installed?

- A. find Solaris_10 -name libz.so.1 -print
- B. grep libz.so.1 /var/sadm/install/contents
- C. grep libz.so.1 Solaris_10/Product/*/pkgmap
- D. grep libz.so.1 Solaris_10/Product/.clustertoc

Answer: C

Question No : 87 - (Topic 1)

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.

Answer: D

Question No : 88 DRAG DROP - (Topic 1)

Click the Task button.

Place the RBAC database names on the correct descriptions.

Place the RBAC database names on the correct descriptions.	
Descriptions	Database Names
Stores the name, description, help file location, and authorizations that are assigned to rights profiles	exec_attr
This database defines commands that require security attributes to succeed.	prof_attr
Contains user and role information that supplements the passwd and shadow databases	user_attr
Assigns authorizations to users, to roles, or to rights profiles	auth_attr

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

Answer:

Place the RBAC database names on the correct descriptions.

Descriptions	Database Names
prof_attr	exec_attr
exec_attr	prof_attr
user_attr	user_attr
auth_attr	auth_attr

Question No : 89 - (Topic 1)

An application file system stores unchanging data only. How should this file system be mounted defensively in /etc/vfstab?

- A. /dev/dsk/c0t3d0s6 /dev/rdisk/c0t3d0s6 /data ufs 2 yes ro,nosuid,anon=0
- B. /dev/dsk/c0t3d0s6 /dev/rdisk/c0t3d0s6 /data ufs 2 yes nodevices,noexec,ro
- C. /dev/dsk/c0t3d0s6 /dev/rdisk/c0t3d0s6 /data ufs 2 yes nosuid,noxattr,noexec
- D. /dev/dsk/c0t3d0s6 /dev/rdisk/c0t3d0s6 /data ufs 2 yes noexec,nosuid,nodevices

Answer: B

Question No : 90 - (Topic 1)

After returning from training, the security administrator is getting asked by his coworkers about the features of Solaris auditing. He starts with some basic information. Which three statements are correct? (Choose three.)

- A. Auditing is a new feature of Solaris 10.
- B. Auditing can be configured for each zone.
- C. Auditing can be configured for an individual user.
- D. Auditing can be configured for each individual file.
- E. Auditing can be used to record logins and logouts.

Answer: B,C,E

Question No : 91 - (Topic 1)

An application that you are installing needs to be able to run the snoop command, which normally requires root access. Which two Solaris features could you use to allow this application to run without giving it full root access to your system? (Choose two.)

- A. Solaris Zones
- B. Kerberos-enabled snoop
- C. Trusted Extensions snoop
- D. Process Rights Management
- E. Role Based Access Control (RBAC)

Answer: D,E

Question No : 92 - (Topic 1)

Which three are useful tools to monitor the integrity of a system? (Choose three.)

- A. bart
- B. logadm
- C. elfsign
- D. cryptoadm
- E. Solaris Fingerprint Database

Answer: A,C,E

Question No : 93 - (Topic 1)

A startup company suspects that one of its sales people is accessing confidential research and development files, which are kept on a Solaris 10 system, and leaking their contents to the press. Which measure can the system administrator put in place to detect this activity?

- A. Solaris Auditing