Vendor: Oracle

Exam Code: 1Z0-881

Exam Name: Oracle Solaris 10 Security Administrator Certified Expert Exam

Version: DEMO

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

2.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

3.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

4.Given:
jupiter:$md5,rounds=2006$2amXesSj5$$kCF48vfPsHDjlKNXeEw7V.:12210:::::: What is the characteristic of this /etc/shadow entry?
A. User jupiter uses the md5 hash, with salt 2006$2amXesSj5$, and with the encrypted password $kCF48vfPsHDjlKNXeEw7V.
B. User jupiter uses the 2a hash, with 2006 iterations of the hash, with salt 2amXesSj5, and with the encrypted password kCF48vfPsHDjlKNXeEw7V.
C. User jupiter uses the md5 hash, with 2006 iterations of the hash, with salt 2amXesSj5, and with the encrypted password kCF48vfPsHDjlKNXeEw7V.
D. User jupiter uses the md5 hash, with 2006 iterations of the hash, with no salt, and with the encrypted password $rQmXesSj5$$kCF48vfPsHDjlKNXeEw7V.

Answer: C

5.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

6.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 webserverd 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

7.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

8.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

9.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

10.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

11.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

12.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

13.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

14.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
Answer: C,E

15.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

16.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

17.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

18.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 nonglobal 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

19.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

20.You have been asked to grant the user ennovy, 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 ennovy
B. setfacl -m user:ennovy:rw- /app/notes
C. setfacl -m group:staff:rw- /app/notes
D. usermod -K defaultpriv=basic,file_dac_read,file_dac_write ennovy
Answer: D