Exam Code: HP0-P17

Exam Name: HP-UX 11i v3 Security Administration

Vendor: HP

Version: DEMO

Part: A

1: After running /usr/sbin/pwck, the following output is displayed:
smbnull:*:101:101::/home/smbnull:/sbin/sh
Login directory not found
What should you do to tighten the security?
A.Nothing - it is a valid system user ID.
B.Nothing - it is used by CIFS/Samba to represent "nobody" with a positive UID.
C.Edit the /etc/passwd entry to specify a dummy login directory and a false login shell.
D.Delete it from /etc/passwd. Opensource Samba installs it by default and it is not required on HP-UX.
Correct Answers: C

2: Which chatr syntax enables buffer overflow protection on a per-binary basis?
A.chatr +b enable <binary>
B.chatr -es enable <binary>
C.chatr +es enable <binary>
D.chatr +bo enable <binary>
E.chatr +es default <binary>
Correct Answers: C

3: What is the effect of the coreadm -e global-setid command?
A.edits the core dump file
B.reads and interprets the core dump file
C.enables the kernel for system crash dumps
D.enables setuid/setgid core dumps system wide
E.causes all running setuid programs to generate a core file
Correct Answers: D

4: Identify ways HP Process Resource Manager (PRM) can protect a system against poorly designed applications. (Select three.)
A.PRM can limit the amount of memory applications may consume.
B.PRM can limit the amount of swap space applications may consume.
C.PRM can limit the amount of disk bandwidth applications may consume.
D.PRM can limit the amount of CPU resources applications may consume.
E.PRM can limit the amount of network bandwidth applications may consume.
F.PRM can limit the number of inbound network connections to configured applications.
Correct Answers: A C D

5: What is a limitation of HP Process Resource Manager (PRM) as it applies to Denial of Service (DoS) attacks?
A.Processes must be grouped before they can be managed.
B.PRM does not perform memory capping; only entitlement and selection.
C.PRM only applies to time-shared processes; real-time processes are not affected.

D.PRM requires a separate configuration file for time-shared and real-time processes.
Correct Answers: C

6: After running kctune executable_stack=2, what happens if MyProg executes code from the stack?
A.MyProg continues running without incident.
B.MyProg is killed before a single instruction can be executed.
C.MyProg continues, but logs a warning to /var/adm/syslog/syslog.log.
D.MyProg continues, but a warning message is logged to the kernel message buffer.
Correct Answers: D

7: Click the Exhibit button.
You used the dmesg command to display the warning shown in the exhibit. Which kernel parameter setting makes this warning message appear?

```
WARNING: UID #123 may have attempted a buffer overflow attack.
PID#1234 (myprog) has been terminated.  See the '+es enable'
option of chatr(1).
```

A.kill_overflow is set to 1
B.exc_stack_code is set to 0
C.buffer_overflow is set to 1
D.executable_stack is set to 0
Correct Answers: D

8: Which benefits does chroot provide to an application from a security perspective? (Select three.)
A.forces an application to start in a specified directory
B.allows the users to do a cd above the specified directory
C.prevents an application from starting in a specified directory
D.prevents the users from doing a cd above the specified directory
E.allows the users of the application access to the directory and the directories below it
F.prevents the users of the application access to the directory and the directories below it
Correct Answers: A D E

9: Which commands configure an application to operate within a secure compartment? (Select two.)
A.privrun
B.privedit
C.setrules
D.cmdprivadm
E.setfilexsec
Correct Answers: D E

10: Some open source software tools use the /usr/local/sbin and /usr/local/src directories. What should you do with the /usr/local directory to maintain a secure system?

A.Verify that /usr/local and its subdirectories are not world writable.
B.Remove /usr/local/bin and /usr/local/sbin from the user's PATH variable.
C.Set permissions on /usr/local and its subdirectories to 047 so all users have access.
D.Use the swlist -l file | grep /usr/local command to see all files installed in those directories.
Correct Answers: A