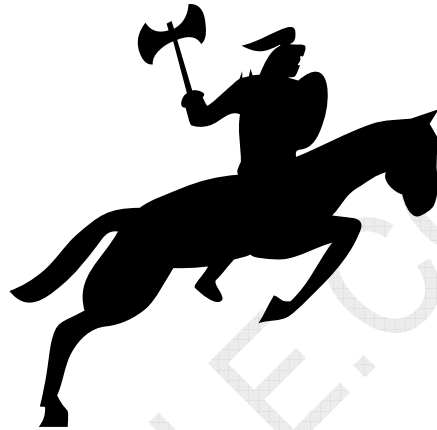


Easy CramBible Lab



HP0-P17

HP-UX 11i v3 Security Administration

**** Single-user License ****

This copy can be only used by yourself for educational purposes

Web: <http://www.crambible.com/>

E-mail: web@crambible.com

Important Note
Please Read Carefully**Study Tips**

This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions.

Go through the entire document at least twice so that you make sure that you are not missing anything.

Latest Version

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 90 days after the purchase. You should check your member zone at CramBible an update 3-4 days before the scheduled exam date.

Here is the procedure to get the latest version:

1. Go to www.CramBible.com
2. Click on Member zone/Log in
3. The latest versions of all purchased products are download from here. Just click the links.

For most updates, it is enough just to print the new questions at the end of the new version, not the whole document.

Feedback

Feedback on specific questions should be send to web@CramBible.com. You should state: Exam number and version, question number, and login ID.

Our experts will answer your mail promptly.

Copyright

Each pdf file contains a unique serial number associated with your particular name and contact information for security purposes. So if we find out that a particular pdf file is being distributed by you, CramBible reserves the right to take legal action against you according to the International Copyright Laws.

THE TOTAL NUMBER OF QUESTIONS IS 120.

QUESTION NO: 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.

Answer: C

QUESTION NO: 2 Which `chattr` syntax enables buffer overflow protection on a per-binary basis?

- A. `chattr +b enable <binary>`
- B. `chattr -es enable <binary>`
- C. `chattr +es enable <binary>`
- D. `chattr +bo enable <binary>`
- E. `chattr +es default <binary>`

Answer: C

QUESTION NO: 3 What is the effect of the `coreadm -e global-setuid` 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

Answer: D

QUESTION NO: 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.

Answer: A, C, D

QUESTION NO: 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.

Answer: C

QUESTION NO: 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.

Answer: D

QUESTION NO: 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

Answer: D

QUESTION NO: 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

Answer: A, D, E

QUESTION NO: 9 Which commands configure an application to operate within a secure compartment? (Select two.)

- A. privrun
- B. privedit
- C. setrules
- D. cmdprivadm
- E. setfilexsec

Answer: D, E

QUESTION NO: 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.

Answer: A

QUESTION NO: 11 Encrypted Volume and File System (EVFS) uses which type of key to encrypt data?

- A. digital certificate
- B. RSA-1024 bit public key
- C. RSA-2048 bit private key
- D. AES-128 bit symmetric key
- E. AES-256 bit asymmetric key

Answer: D

QUESTION NO: 12 Identify where Encrypted Volume and File System (EVFS) protects data.

- A. in transit
- B. in the kernel
- C. over the network
- D. on the storage device

Answer: D

QUESTION NO: 13 Which tool is recommended for providing file integrity information?

- A. hash
- B. cksum
- C. crypt
- D. md5sum