TestHorse

Certified IT practice exam authority

Accurate study guides, High passing rate!
Testhorse provides update free of charge in one year!

http://www.testhorse.com

Exam : **HP0-P17**

Title : HP-UX 11i v3 Security Administration

Version : Demo

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

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>
Answer: 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
Answer: 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.

Answer: ACD

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

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

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

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: ADE

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: DE

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

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

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

13. Which tool is recommended for providing file integrity information?

A. hash

B. cksum

C. crypt

D. md5sum
Answer: D

14. How can you grant NFS filesystem access to specific users as opposed to all users? (Select two.)

A. Specify the desired users to the /etc/dfs/sharetab entry for the mount point using the format "-access=user1:user2:user3".

B. Add the desired users to an ACL and set the permissions of the shared filesystem such that only members of the ACL can access the data.

C. Add the desired users to a group and set the permissions of the shared filesystem such that only members of the group can access the data.

D. Add the desired users to a netgroup and specify the netgroup in the /etc/dfs/sharetab entry for the mount point using the format "-access=netgroup".
Answer: BC

15. Which product encrypts data on zx2-based Integrity servers?

A. HP-UX VxFS filesystem

B. HP-UX Encryption Module

C. HP-UX Trusted Computing Services

D. HP-UX Integrity Trusted Platform Module
Answer: C

16. Where can an HP-UX 11i v3 EVFS-encrypted backup tape from an HP Integrity rx7640 Server be restored and decrypted?

A. only on the HP-UX system where the tape was created

B. on any HP-UX system where the symmetric encryption key resides

C. on any HP-UX system where the backup owner's public key resides

D. on any HP-UX system where the backup owner's public/private key pair resides
Answer: D

17. Where are Trusted Computing Services (TCS) protected EVFS keys stored?

A. HP-UX kernel

B. EVFS volume

C. system stable storage

D. HP-UX root file system

E. Trusted Platform Module
Answer: D

18. Which statement is true regarding an HP-UX VxFS filesystem using ACLs?

A. Default ACLs can only be placed on a file.

B. Default ACLs have the same owner as the owner of the file the ACL controls.

C. A directory's ACL can have default entries that are applied to files subsequently.

D. An ACL has an owner that can be different from the owner of the file the ACL controls.
Answer: C

In order to restrict the access to the /etc/group file through FTP, which statement should be included in the /etc/ftpd/ftpaccess file?

Identify the features of the TCP Wrappers product. (Select three.)

A. noaccess /etc/group

B. noretrieve /etc/group

C. accessdeny /etc/group

D. suppressaccess /etc/group

Answer: B

A. enhances cryptographic authentication

B. provides protection against IP address spoofing

C. provides protection against hostname spoofing

D. provides data encryption on TCP "wrapped" connections

E. provides enhanced protection for RPC daemons using TCP/IP connections

F. provides enhanced security for daemons managed by inetd using TCP/IP connections

G. may be configured to provide enhanced security for any daemon using TCP/IP connections
Answer: BCF