

Course Assessment Answers

The following multiple-choice post-assessment will test your knowledge of the skills and concepts taught in *Operating System Security (10SS)*.

- Patrick has discovered that his Web server has a bug that makes the server subject to an attack that will result in root-level access. He has determined that he can download a file to patch this vulnerability. After downloading the file, he has tested it to see whether it has been trojanized. What security principle is Patrick addressing?
 - Non-repudiation.
 - Authentication.
 - Data confidentiality.
 - Data integrity.
- Which of the following explicitly specifies the use of “controls” to secure a system?
 - BS 7799.
 - ISO 7498-2.
 - Common Criteria.
 - TCSEC.
- In the interests of security, Peter has created a 17-character password for a share that contains sensitive files. Amy has tried to access this system using her Windows 9x system, but she cannot access the file. What is the most likely cause of the problem?
 - Windows 9x clients cannot access Windows 2000 shares.
 - Windows 9x clients cannot supply passwords longer than 14 characters.
 - Windows 9x clients cannot supply passwords longer than 15 characters.
 - The encryption level is set too high on the Windows 2000 server.
- What are the standard permissions of the /etc/shadow file in Linux?
 - 007.
 - 700.
 - 600.
 - 420.
- Which of the following commands allows you to determine a connection from the 192.168.2.3 IP address in Linux?
 - fport -i@192.168.2.3.
 - fport /dev/ttyS0 -i@192.168.2.3.
 - lsof -i | less @192.168.2.3.
 - lsof -i@192.168.2.3.

6. Consider the following partition structure in a Windows 2000 system:

Drive	File system
C:\	NTFS
D:\	NTFS
E:\	NTFS

A file named `secret.txt` is in the `C:\SECRET` directory. It has full permissions for the "secret" group, and read-only permissions for the Administrators group. The `D:\SECRET` directory has full permissions for the "secret" group, and no access permissions for the Administrators group. The `E:\SECRET` directory allows access to only the Administrators group.

This file is moved from the `C:\SECRET` directory to the `D:\SECRET` directory. Next, it is copied to the `E:\SECRET` directory. Which group will be able to write to this file?

- None.
 - The Administrators group.
 - The Secret and Administrators groups.
 - The Secret group.
7. Which of the following files can be used to limit access to portmapper?
- `/etc/securenets`
 - `/etc/security/console.apps/securenets`
 - `/etc/hosts.deny`
 - `/etc/securetty`
8. Gordon has issued the following command as root:
- ```
umask 222
```
- When he subsequently creates a new file, what permission bits will it have?
- 444.
  - 222.
  - 555.
  - 177.
9. The immutable bit has been set on a file named `/etc/shadow`. Which of the following commands will show it in a directory listing?
- `ls -l`
  - `ls -i`
  - `lsattr -l`
  - `lsattr`

10. In which of the following areas does the portmapper daemon contain a weakness?

- a. Authentication.
- b. Access control.
- c. Non-repudiation.
- d. Buffer overflow.

11. You want to disable interactive logon for the root account. How do you do so?

- a. Enter /bin/false into the shell value in the /etc/shadow file.
- b. Delete the root account from the /etc/shadow file.
- c. Enter /bin/false into the shell value in the /etc/passwd file.
- d. Delete the root account from the /etc/passwd file.

12. What security feature is unique to Windows 2000, as opposed to Windows Me?

- a. Discretionary access control.
- b. Auditing.
- c. Mandatory logon.
- d. Object reuse.