

ITBU 443: Threats and Counter Measures, Homework 12

Chapter 12, *Computer Security, Principles and Practices*

Readings

Read chapter 12 in the *Computer Security, Principles and Practices* book.

Discussion Questions

Answer the discussion questions in writing.

1. How do you secure a base operating system?
2. Why is it important to promptly apply all patches, from a security point of view?
3. Why would you want to automate patching? Why would you *not* want to automate patching?
4. Should you remove unneeded applications and services from a server? Why or why not?
5. What is the type of access control implement in UNIX and Linux systems?
6. (Not in book) Explain the `chmod` command. Are these permissions the same: `rw-rw-r--` and `664`? Why or why not?
7. What is the `suid` command used for?
8. Should you rotate log files? Why or why not?
9. What is a *chroot jail*?
10. What is virtualization?
11. Name two ways that Linux and Windows security mechanisms differ.