

# ITBU 443: Threats and Counter Measures, Homework 17

Chapter 23, *Computer Security, Principles and Practices*

## Readings

Read chapter 23 in the *Computer Security, Principles and Practices* book.

## Discussion Questions

Answer the discussion questions in writing.

1. List the three general approaches that organizations use to secure networks and hosts.
2. What is an *authentication server*? Please be specific.
3. What is a Kerberos Realm?
4. Describe some differences between Kerberos 4 and Kerberos 5.
5. What is an X.509 certificate?
6. What is a *proxy certificate*?
7. Describe how the *certificate revocation list* works.
8. The book notes that MD5 and SHA1 are not used because of *collisions*. What is a collision, and why is that a problem?
9. What is *certificate pinning*?
10. What is PKIX?
11. (Not in book) What is the current status of the PKIX Working Group?