Protection and Security

1. Differentiate between "protection" and "security" in an operating system.
2. Define Access control lists (ACL)
3. Define Capabilities list.
4. The access-control matrix can be used to determine whether a process can switch from, say, domain A to domain B and enjoy the access privileges of domain B. Is this approach equivalent to including the access privileges of domain B in those of domain A? Give a brief explanation of your answer.

5. Define the following, define
   - Digital Signatures
   - Message Digests
   - Certification authorities

6. We looked at a variety of software exploitation techniques. Describe 2
   - Buffer overflow attacks
     - Control Flow Attacks
     - Non-Control Flow Attacks
   - Memory Corruption Attacks
     - Format String Attack
     - Dangling pointers
   - Null Pointer Dereference Attacks
   - Integer Overflow attacks
   - Command Injection Attacks
   - Time of Check to Tome of Use Attacks

7. What is meant by an insider attack? Give an example of one.
8. Describe the Morris Worm, including the history and consequences. What did it do?
9. Describe the Sony Rootkit.
10. Describe the defense Java (JVM) security provides

11. We looked at a variety of malware techniques. Describe 1
    - Trojan Horse
    - Virus
    - Worm
    - Spyware
    - RootKits
12. We looked at a variety of defense techniques. Describe 1
    - Firewall
    - Antivirus
    - Code Signing
    - Jailing
    - Model-Based Intrusion Detection
    - Encapsulating Mobile Code
    - Java Security

1.