1. What are the differences between rule-based intrusion detection and statistical anomaly detection?
2. What are the functions of audit records? How can they be used?
3. What is a honeypot?

4. What can a firewall do and what cannot a firewall do?
5. What is packet filtering firewall, stateful inspection firewall, application level proxy and circuit-level proxy? What are the strength and weaknesses of these firewalls respectively?
6. What is a DMZ? Why an internal firewall and external firewall are needed?

7. What functions (or services) can IPSec provide?
8. How does IPSec provide security?
9. How do AH and ESP work? What are the differences between them?
10. What attacks or what kinds of attacks can AH and ESP prevent?
11. How keys are exchanged in IPSec?