List of the Possible Questions (Part I)

I: Honeypots and honeynets

#1: What are the major challenges in utilizing output data from honeypots (mention two examples).
#2: What are the major challenges in configuring honeypots (mention two examples)?
#3: What are the major legal and ethical issues in using honeypots (mention two examples)?

II. Tunneling

#4: What are the two primary motivations for using “tunneling” (good purposes)?
#5: What is VPN (Virtual Private Network)?
#6: How is VPN (Virtual Private Network) realized (implemented)?
#7: Why is tunneling a trouble (security threat) to security administrators?
#8: What is “M-Bone”?
#9: How does “M-Bone” work?
#10: What is “6-Bone”?
#11: How does “6-Bone” work?
#12: What is “soft-Ether”?

III. IP-Sec protocol overview

#13: What are “application-level security implementations”? What are “protocol-level security implementations”?
#14: What are the four security functions IPSec perform?
#15: What are the primary advantages in using “protocol-level security implementations”?
#16: What are the four security issues “data integrity” in IPSec provides protection for?