Review questions for final

1. List some of the data in an IPv4 packet header which is relevant from a security standpoint.

2. What is Network Address Translation (NAT)? What is subnetting?

3. How does the Address Resolution Protocol translate IP addresses to MAC addresses? What is ARP poisoning?

4. From a security standpoint, how do routers, switches, and hubs differ?

5. What is a man-in-the-middle attack?

6. What is the simple security property in the Bell-Lapadula model? What is the *-property? How do these work together to ensure data integrity? What is the ds-property?

7. How does the Biba Integrity model differ from the Bell-Lapadula? What are the 3 rules in this system (analogous to the ones in the previous problem)?

8. What is the Clark-Wilson integrity model designed for (as opposed to the Biba and Bell-Lapadula models)? What are the two main concepts in this model?

9. Describe the Chinese wall model, and give an example of where it might be used.

10. Why is C more vulnerable to buffer overflow attacks than python, perl, or other higher level languages?

11. Describe how a stack overflow attack is executed.

12. How can computers defend against stack overflows? Give an example of a run-time defense and a compile-time defense.

13. What is a heap overflow attack?

14. What is an injection attack?

15. Describe how cross site scripting works, and how programs can defend against it.

16. What type of access control does Linux generally support, and what impact does this have on security?

17. When securing a computer system, why do we limit how many applications are running?

18. What is chroot jail?

19. How are mandatory access controls implemented in Linux?

20. What is SELinux?

21. Briefly describe the functions of the following components on a Windows machine: Security reference monitor, local security authority, and security account manager

22. Give one reason local accounts can be better than domain accounts, and one reason why domain accounts may be preferable to local accounts.

23. How is mandatory access control implemented in Windows?

24. What are the governing principles of hardening systems in Windows? How and why are these different than the main principles in Linux system design?

25. How does windows prevent against buffer overflow attacks? What about heap overflow attacks?

26. What is a no execute bit, and how does it work? Name one type of overflow attack this won't help against.

27. What is stack randomization?

28. Name 3 categories of crime recognized by the international community.

29. Give two or three of the unique challenges facing law enforcement professionals when it comes to cybercrime (as opposed to other types of criminal activity).

30. What did the Digital Millennium Copyright Act do?

31. What is digital rights management?

32. What is computer forensics? What are the key elements used in computer forensics?

33. What is the main balance to find in auditing or logging of data?

34. What are the 3 options for storing log data, and the advantages and drawbacks of each?

35. Name and describe some types of distributed denial of service (DDoS) attacks.

36. What are the best ways to prevent or defend against DDoS attacks? Why aren't these methods more commonly implemented?

37. What are reflection and amplifications attacks (in the context of DDoS)?

38. What is an intrusion detection system? What are the main goals of any intrusion detection system?

39. What are the two kinds of intrusion detection systems?

40. What is anomaly detection, and what is signature detection?

41. How do network intrusion detection systems work, and where do they monitor traffic?

42. What is the difference between an inline sensor and a passive sensor?

43. What is a honeypot?

44. What features does a "trusted" OS add to operating systems functionality?

45. Describe what is meant by terms such as "kernalization" and "virtualization", and give examples of where each has been implemented.

46. What is the orange book, and what are the classifications it provided? What were some of the inherent flaws that led to disuse of its system?

47. How does the Common Criteria, and how does it classify trusted systems?

48. What is TPM and trusted computing? What are common hardware implementations of these that are used?

49. What is the goal of the host identity protocol? Why hasn't it been put into widespread use, and where has it been successfully used?

50. How does TLS work to layer security onto inherently insecure HTTP protocols? Give at least two ways it might fail to work.

51. How does DNSSEC work, and what does it protect (and not protect) against? Where is it supported, and why doesn't everyone use it?

52. Describe the purpose of onion routing, and briefly explain how it works.

53. List a few problems that are specific to wireless security. How are they handled in common wireless communication protocols, and with what tools?