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. What is a SYN flood, and how can we defend against it?

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

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

7. 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?

8. 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)?

9. 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?

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

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

12. Describe how a stack overflow attack is executed.

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

14. What is a heap overflow attack?

15. What is an injection attack?

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

17. Name 3 things that hackers exploited in order to gain access to Paris Hilton's cell phone.

18. What is pretexting?

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

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

21. What is the difference between TCP Wrappers and iptables?

22. What is chroot jail?

23. How are mandatory access controls implemented in Linux?

24. What is SELinux? What is the difference between it and Novell AppArmor?

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

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

27. How is mandatory access control implemented in Windows?

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

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

30. What is a no execute bit, and how does it work?

31. What is stack randomization?

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

33. 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).

34. How did the FBI finally catch Kevin Mitnick?

35. What did the Digital Millennium Copyright Act do?

36. What is digital rights management?

37. Describe two or three of the main issues brought up by the lawsuit by Sony against Hotz, the hacker who cracked the PS3.

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

39. What is the main balance to find in auditing or logging of data? What are the 3 levels where auditing is used?

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

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

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

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

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

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

46. What is a honeypot?