Review questions for midterm

1. What are some of the most common attacks used to gain access to a user's password?

2. For each attack you listed in the previous problem, give at least one way we can defend against it.

3. What is IPSec, and why is it used?

4. What is the discrete log problem, and why is it important to public key cryptography?

5. How do Diffie-Hellman and RSA work? (Be prepared for questions as on the first homework.)

6. Give an iptables rule which drops all incoming tcp traffic on port 31337.

7. What is sudo, and why is it good in terms of security?

8. What is IP spoofing?

9. What are the two broad categories of encryption used on modern computer systems? Give an example of each.

10. What is the most common way to attack symmetric encryption?

11. Why is DES no longer used? (In other words, what is the reason that it is no longer considered secure?)

12. What is a salt, and why are they used when hashing passwords?

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

14. How does IPv6 address the issues in IPv4?

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

16. How does the Address Resolution Protocol translate IP addresses to MAC addresses?

17. What is ARP poisoning?

18. What is a BGP Blackhole attack? How are these attacks "fixed"?

19. What is a stateless firewall, and what is a stateful firewall?

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

21. Why is the C function gets() inherently insecure?

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

23. Describe how a stack overflow attack is executed.

24. What is a heap overflow attack?

25. What is an SQL injection attack?

26. What does fuzzing mean?

27. What is chroot jail?

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

29. What is address space layout randomization, and why is it used?

30. What is a canary? What types of attacks or errors won't they help defend against, and why?

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

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

33. What is a honeypot?

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

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

36. Why is WEP not considered secure at this point, and how does WPA address those issues?

37. What is the Guninski attack?

38. Give two security issues that come up immediately with the use of cookies.

39. How do you analyze logs (such as tcpdump ones from the lab) to find protocols and vulnerabilities? (Be prepared to sketch steps from the lab and/or analyze such logs).