Review questions for midterm

1. What is defense in depth (from the first article we read)?

2. What are 4 basic authentication strategies?

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

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

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

6. What is access control?

7. What is the difference between DAC and MAC? What about DAC and RBAC?

8. List 3 or 4 common access rights that modern computers typically grant.

9. What is an access control matrix? How is this matrix stored on a computer?

10. What are the two main principles in the Bell-Lapadula MAC model?

11. Give two examples of data in the headers and footers of a packet that can be used to gain information about a system in order to hack into it.

12. What is the purpose of a firewall?

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

14. Why are proxies used? What are advantages and disadvantages?

15. What is a DMZ, and why is it useful? What type of systems generally exist in it?

16. What is the purpose of an intrusion detection system?

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

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

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

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

21. What is a message authentication code?

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

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

24. What does nmap do?

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

26. What is IP spoofing?

27. How does a buffer overflow attack work?

28. What is the difference between a virus and a worm?

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

30. Give at least three good reasons why companies should invest in security systems for their computing infrastructure.

31. Give at least three reasons why people do not properly secure their computers or computer infrastructure (despite the better reasons you gave in the previous problem).