CSH6 CH 15 REVIEW QUESTIONS

1. A decades-old network has connections to workstations using RJ-45 serial multi-wire cabling. What kind of network is this?
2. Which of the following nontechnical penetration techniques is/are often part of social engineering?
3. An element of the communications grid appears to hover 22,236 miles over a fixed spot on the earth. This device is a _____.
4. Where can we best intercept and interpret complete messages sent as streams of unencrypted packets traveling over a packet-switching network?
5. A corporation has a TCP/IP network that is restricted entirely to employees of the firm. What kind of network is this?
6. What does "incremental information leveraging" include?
7. Which of the following is/are elements of effective defenses against system penetration?
8. Which of these devices filters inbound and outbound packets?
9. What's one of the most dangerous errors one can make when setting up voice mail in an organization?
10. Which of the following transmission media have the highest bandwidth?
11. Which of the following describes a datagram protocol?
12. Which of the following nontechnical penetration techniques is/are often part of social engineering?
13. Which of the following nontechnical penetration techniques is/are often part of social engineering?
14. What kind of network do hackers and spies attack using a "sniffer"?
15. What is the single most common exploit class for penetrating systems today?
16. Which of the following nontechnical penetration techniques is/are often part of social engineering?
17. Which of the following nontechnical penetration techniques is/are often part of social engineering?
18. Which of these is "van Eck freaking" or "van Eck phreaking"?
19. What's a "canonical password"?
20. Which of these factors would facilitate wiretapping of an asynchronous network inside an office building?
21. Which of these factors would facilitate wiretapping of an asynchronous network inside an office building?
22. What's the problem with "off-premises extensions"?
23. What do we call a system that monitors the security perimeter and notifies admins about attacks and intrusions?
24. What's the problem with "off-premises extensions"?
25. What does laser interferometry permit?

26. A corporation has a TCP/IP network that is restricted to employees of the firm and to selected customers. What kind of network is this?
27. What's the key vulnerability of unencrypted microwave transmissions?
28. What do we call the unauthorized, imperceptible transfer of data to criminals or other unauthorized personnel?
29. What is one of the most serious consequences of improperly used e-mail?
30. Which of the following nontechnical penetration techniques is/are often part of social engineering?
31. What's the problem with "off-premises extensions"?
32. What is TEMPEST in discussions of information assurance?
33. Which of these factors would facilitate wiretapping of an asynchronous network inside an office building?
34. A particular transmission medium has enormous bandwidth, is difficult and expensive to tap, and allows for time-domain reflectometry to identify taps and breaks. Which is it?
35. Why should PBX managers disable DISA?
36. What is the term for a hidden, unrecognized linkage that allows data leakage?
37. Which of the following networks is most difficult to tap?
38. A network protocol splits a message into sections that are indivually transmitted at different frequencies. This approach is called a _____.

