CSH6 CH 18 REVIEW QUESTIONS

1. What did Johnny [x]chaotic do in August 1998?
2. An attacker sends huge numbers of requests asking for confirmation that there is a device on a specific IP address and how long it takes for the response. This technique is characteristic of which DoS attack?
3. An attacker sends spoofed UDP packets to the broadcast address of a large network which responds to the victim's address with a flood of packets. This attack is known as a ___
4. The database process being run by Alice locks the order master using an unconditional loc. The database process being run by Bob locks the order detail using an unconditional lock. Alice's process then puts an unconditional lock on the order detail and Bob's process uses an unconditional lock on the order master. This situation is an example of a ___
5. What was the name of the worm that started in the IBM internal networks and escaped into BITNET to cause widespread DoS?
6. How do the CAPTCHAs that so many email-list managers use help reduce subscription bombing?
7. Which of the following attacks uses a buffer overflow?
8. Which of the following is thought to be the first DDoS tool?
9. Why do bounds violations in interpreters cause the greatest risk of harmful results?
10. An impossible condition causes the operating system to halt. Attacks using such situations are known as ___
11. Which sentence is spelled correctly?
12. What is a _bounds violation_ in programming?
13. Which phrase is spelled correctly?
14. Where can system administrators locate the latest information on new vulnerabilities, including new buffer overflows?
15. Why is it often difficult to measure the actual costs of a denial-of-service attack on a commercial Website system?
16. Why doesn't packet filtering work against DDoS?
17. Which of the following is/are used to describe a compromised system used in a DDoS attack?
18. One of the key methods for increasing resistance to DoS attacks is to ___
19. An attacker sends a SYN packet to a target, which responds with a SYN/ACK and waits for the ACK – which never arrives. This sequence is characteristic of which DoS attack?
20. Which of the following illustrates a denial-of-service problem?
21. In DoS attack, carefully crafted packets have their source and destination address ports set to the same address. This technique is used in ___
22. What kind of people are currently using DDoS attacks?
23. Which of the following is/are (a) possible consequence of a bounds violation in code?
24. In March 1999, the fastest-spreading MS-Word macro virus up to that time infected people's computers and sent email to the 50 most-used addresses in the victims' address books. This was the ___
25. Which of the following is/are (a) recommended approach(es) to reducing vulnerability to DoS attacks?
26. Which of the following is/are (a) DDoS tool(s)?
27. Roughly how much damage was estimated to have been caused by David L. Smith's spreading of the fast-spreading Word macro virus he launched in early 1999?

28. The database process being run by Alice locks the order master using an unconditional loc. The database process being run by Bob locks the order detail using an unconditional lock. Alice's process then puts an unconditional lock on the order detail and Bob's process uses an unconditional lock on the order master. This situation results in a ___

29. Unknown criminals used a SYN-flood in September 1996 to damage which ISP?

30. In DoS attack, carefully crafted packets result in overlaps when reassembled by the receiving system and crash the system. This technique is used in ___

31. Why does obligatory user lockout after, say, three incorrect passwords risk a DoS on the system if the IT department HelpDesk has to manually reset each locked account?

32. Which of the following is a ping-flood attack?

33. In November 1988, a significant proportion of the computers using the primitive Internet were taken offline due to the ___

34. An attacker crafts a series of packets in which the total size once assembled exceeds the maximum data-block size of 64KB. This attack is called a ___

35. Many packet-flooding attacks use ICMP. What is ICMP?

36. When an incident involves exhausting resources on a computer system or network and results in degraded performance or complete loss of functionality, we call this situation a ___

37. In DoS attack, carefully crafted packets have their source and destination address ports set to the same address. Receiving such packets causes ___

38. What is the fundamental problem leading to buffer overflows?

39. What is the technique in which criminals or agents form a bond of apparent friendship with a target who can provide insider information and progress to a sexual relationship as they strengthen (false) trust?

40. Which of the following technical defenses can best reduce the success of social-engineering attacks?

41. What kind of encryption can support better resistance to social engineering?

42. What is/are (an) ATE activity/activities that can be helpful in preparing a workforce to oppose social-engineering attacks?

43. What is the term applied to the way social engineers typically wear uniforms, carry badges, learn insider vocabulary, and assume a confident air of entitlement as they pretend to belong to an organization or have positional authority?

44. Which of the following is/are (a) notoriously successful social engineer(s)?

45. What can the organization do to ensure that employees can cope with a social engineer who tries to intimidate an employee by pretending to be an angry high-placed executive irritated by the published security policies?

46. What is the informal professional consensus about social engineering attack rates and success rates?