Chapter 7 Study Guide

Indicate whether the statement is true or false.

1. NIDPSs can reliably ascertain if an attack was successful or not.
   a. True
   b. False

2. Intrusion detection consists of procedures and systems that identify system intrusions and take action when an intrusion is detected.
   a. True
   b. False

3. In DNS cache poisoning, valid packets exploit poorly configured DNS servers to inject false information to corrupt the servers' answers to routine DNS queries from other systems on the network.
   a. True
   b. False

4. Once the OS is known, all of the vulnerabilities to which a system is susceptible can easily be determined.
   a. True
   b. False

5. A false positive is the failure of an IDPS system to react to an actual attack event.
   a. True
   b. False

6. To use a packet sniffer legally, an administrator only needs permission of the organization's top computing executive.
   a. True
   b. False

7. A strategy based on the concept of defense in depth is likely to include intrusion detection systems, active vulnerability scanners, passive vulnerability scanners, automated log analyzers, and protocol analyzers.
   a. True
   b. False

8. Passive scanners are advantageous in that they require vulnerability analysts to get approval prior to testing.
   a. True
   b. False

9. A broadcast vulnerability scanner is one that initiates traffic on the network in order to determine security holes.
   a. True
   b. False

10. The Simple Network Management Protocol contains trap functions, which allow a device to send a message to the SNMP management console indicating that a certain threshold has been crossed, either positively or negatively.
   a. True
   b. False

Chapter 7 Study Guide

11. IDPS responses can be classified as active or passive.
    a. True
    b. False

12. An IDPS can be configured to dial a phone number and produce an alphanumeric page or other type of signal or message.
    a. True
    b. False

13. The process by which attackers change the format and/or timing of their activities to avoid being detected by the IDPS is known as a false attack stimulus.
    a. True
    b. False

14. Intrusion detection and prevention systems can deal effectively with switched networks.
    a. True
    b. False

15. A fully distributed IDPS control strategy is an IDPS implementation approach in which all control functions are applied at the physical location of each IDPS component..
    a. True
    b. False

16. Your organization's operational goals, constraints, and culture should not affect the selection of the IDPS and other security tools and technologies to protect your systems.
    a. True
    b. False

17. In order to determine which IDPS best meets an organization's needs, first consider the organizational environment in technical, physical, and political terms.
    a. True
    b. False

18. All IDPS vendors target users with the same levels of technical and security expertise.
    a. True
    b. False

19. The Metasploit Framework is a collection of exploits coupled with an interface that allows the penetration tester to automate the custom exploitation of vulnerable systems.
    a. True
    b. False

20. To assist in the footprint intelligence collection process, attackers may use an enhanced Web scanner that, among other things, can scan entire Web sites for valuable pieces of information, such as server names and e-mail addresses.
    a. True
    b. False

Chapter 7 Study Guide

21. Services using the TCP/IP protocol can run only on their commonly used port number as specified in their original Internet standard.
    a. True
    b. False

22. HIDPSs are also known as system integrity verifiers.
    a. True
    b. False

23. A passive IDPS response is a definitive action automatically initiated when certain types of alerts are triggered.
    a. True
    b. False

24. An HIDPS can detect local events on host systems and also detect attacks that may elude a network-based IDPS.
    a. True
    b. False

25. A HIDPS is optimized to detect multihost scanning, and it is able to detect the scanning of non-host network devices, such as routers or switches.
    a. True
    b. False

26. Administrators who are wary of using the same tools that attackers use should remember that most organizations prohibit use of open source or freeware software tools.
    a. True
    b. False

27. Intrusion detection and prevention systems perform monitoring and analysis of system events and user behaviors.
    a. True
    b. False

28. A HIDPS can monitor systems logs for predefined events.
    a. True
    b. False

29. The anomaly-based IDPS collects statistical summaries by observing traffic that is known to be normal.
    a. True
    b. False

30. Security tools that go beyond routine intrusion detection include honeypots, honeynets and padded cell systems.
    a. True
    b. False

Chapter 7 Study Guide

Indicate the answer choice that best completes the statement or answers the question.

31. Activities that scan network locales for active systems and then identify the network services offered by the host systems is known as _____.
a. port knocking b. doorknob rattling
c. footprinting d. fingerprinting

32. Using _____, the system reviews the log files generated by servers, network devices, and even other IDPSs.
a. LFM b. stat IDPS
c. AppIDPS d. HIDPS

33. Which of the following is NOT a described IDPS control strategy?
a. centralized b. fully distributed
c. partially distributed d. decentralized

34. Which of the following ports is commonly used for the HTTP protocol?
a. 20 b. 25
c. 53 d. 80

35. A(n) _____ is a software program or hardware appliance that can intercept, copy, and interpret network traffic.
a. packet scanner b. packet sniffer
c. honey pot d. honey packet

36. A(n) _____ is an event that triggers an alarm when no actual attack is in progress.
a. false neutral b. false attack stimulus
c. false negative d. noise

37. To use a packet sniffer legally, the administrator must _____.
a. be on a network that the organization owns b. be under direct authorization of the network's owners
c. have knowledge and consent of the content's creators d. all of the above

38. _____ is the process of classifying IDPS alerts so that they can be more effectively managed.
a. Alarm filtering b. Alarm clustering
c. Alarm compaction d. Alarm attenuation

39. _____ applications use a combination of techniques to detect an intrusion and then trace it back to its source.
a. Honeynet b. Trap and trace
c. HIDPS d. Packet Sniffer

40. Network Behavior Analysis system _____ sensors are typically intended for network perimeter use, so they would be deployed in close proximity to the perimeter firewalls, often between the firewall and the Internet border router to limit incoming attacks that could overwhelm the firewall.
a. inline b. offline
c. passive d. bypass

Chapter 7 Study Guide

41. To determine whether an attack has occurred or is underway, NIDPSs compare measured activity to known _____ in their knowledge base.
a. vulnerabilities b. fingerprints
c. signatures d. footprints

42. A(n) _____ IDPS is focused on protecting network information assets.
a. network-based b. host-based
c. application-based d. server-based

43. _____ are decoy systems designed to lure potential attackers away from critical systems.
a. Honeypots b. Bastion Hosts
c. Wasp Nests d. Designated Targets

44. Intrusion _____ activities finalize the restoration of operations to a normal state and seek to identify the source and method of the intrusion in order to ensure that the same type of attack cannot occur again.
a. prevention b. reaction
c. detection d. correction

45. Most network behavior analysis system sensors can be deployed in _____ mode only, using the same connection methods as network-based IDPSs.
a. passive b. active
c. reactive d. dynamic

46. In TCP/IP networking, port _____ is not used.
a. 0 b. 1
c. 13 d. 1023

47. _____ testing is a straightforward testing technique that looks for vulnerabilities in a program or protocol by feeding random input to the program or a network running the protocol.
a. Buzz b. Fuzz
c. Spike d. Black

48. _____ is the action of luring an individual into committing a crime to get a conviction.
a. Entrapment b. Enticement
c. Intrusion d. Padding

49. A _____ vulnerability scanner listens in on the network and identifies vulnerable versions of both server and client software.
a. passive b. aggressive
c. active d. secret

50. A _____ port, also known as a monitoring port, is a specially configured connection on a network device that is capable of viewing all of the traffic that moves through the entire device.
a. NIDPS b. SPAN
c. DPS d. IDSE

Chapter 7 Study Guide

51. _____ are usually passive devices and can be deployed into existing networks with little or no disruption to normal network operations.

a. NIDPSs b. HIDPSs

c. AppIDPSs d. SIDPSs

52. The ability to detect a target computer's _____ is very valuable to an attacker.

a. manufacturer b. operating system

c. peripherals d. BIOS

53. _____ benchmark and monitor the status of key system files and detect when an intruder creates, modifies, or deletes monitored files.

a. NIDPSs b. HIDPSs

c. AppIDPSs d. SIDPSs

54. Some vulnerability scanners feature a class of attacks called _____, that are so dangerous they should only be used in a lab environment.

a. aggressive b. divisive

c. destructive d. disruptive

55. A(n) _____ works like a burglar alarm in that it detects a violation (some system activities analogous to an opened or broken window) and activates an alarm.

a. IDPS b. WiFi

c. UDP d. DoS