Chapter 6 Study Guide

Indicate whether the statement is true or false.

1. Packet-filtering firewalls scan network data packets looking for compliance with the rules of the firewall’s database or violations of those rules.

   a. True

   b. False

2. A content filter, also known as a reverse firewall, is a network device that allows administrators to restrict access to external content from within a network.

   a. True

   b. False

3. Packet filtering firewalls scan network data packets looking for compliance with or violation of the rules of the firewall’s database.

   a. True

   b. False

4. Using an application firewall means the associated Web server must be exposed to a higher level of risk by placing it in the DMZ.

   a. True

   b. False

5. Authentication is the process of validating a supplicant’s purported identity.

   a. True

   b. False

6. Some firewalls can filter packets by protocol name.

   a. True

   b. False

7. Syntax errors in firewall policies are usually extremely difficult to identify.

   a. True

   b. False

8. The application layer firewall is firewall type capable of performing filtering at the application layer of the OSI model, most commonly based on the type of service.

   a. True

   b. False

9. Good policy and practice dictates that each firewall device, whether a filtering router, bastion host, or other firewall implementation, must have its own set of configuration rules.

   a. True

   b. False

10. It is important that e-mail traffic reach your e-mail server and only your e-mail server.

   a. True

   b. False

Chapter 6 Study Guide

11. Internet connections via dial-up lines are regaining popularity due to recent technological developments.
    a. True
    b. False

12. The DMZ can be a dedicated port on the firewall device linking a single bastion host.
    a. True
    b. False

13. A firewall cannot be deployed as a separate network containing a number of supporting devices.
    a. True
    b. False

14. Circuit-level gateways usually look at data traffic flowing between networks rather than preventing direct connections between networks.
    a. True
    b. False

15. Though not used as much in Windows environments, terminal emulation is still useful to systems administrators on Unix/Linux systems.
    a. True
    b. False

16. Lattice-based access control is a form of access control in which users are assigned a matrix of authorizations for particular areas of access.
    a. True
    b. False

17. Task-based controls are associated with the assigned role a user performs in an organization, such as a position or temporary assignment like project manager.
    a. True
    b. False

18. When Web services are offered outside the firewall, HTTP traffic should be blocked from internal networks through the use of some form of proxy access or DMZ architecture.
    a. True
    b. False

19. Even if Kerberos servers are subjected to denial-of-service attacks, a client can still request additional services.
    a. True
    b. False

20. The ability of a router to restrict traffic to a specific service is an advanced capability and not considered a standard feature for most routers.
    a. True
    b. False

Chapter 6 Study Guide

21. All organizations with a router at the boundary between the organization's internal networks and the external service provider will experience improved network performance due to the complexity of the ACLs used to filter the packets.
    a. True
    b. False

22. A VPN, used properly, allows a user to use the Internet as if it were a private network.
    a. True
    b. False

23. Firewalls can be categorized by processing mode, development era, or structure.
    a. True
    b. False

24. The RADIUS system decentralizes the responsibility for authenticating each user, by validating the user's credentials on the NAS server.
    a. True
    b. False

25. Most current operating systems require specialized software to connect to VPN servers, as support for VPN services is no longer built into the clients.
    a. True
    b. False

26. Accountability is the matching of an authenticated entity to a list of information assets and corresponding access levels.
    a. True
    b. False

27. Good firewall rules include requiring that all data that is not verifiably authentic should be denied.
    a. True
    b. False

28. A content filter is essentially a set of scripts or programs that restricts user access to certain networking protocols and Internet locations.
    a. True
    b. False

29. Discretionary access control is an access control approach whereby the organization specifies use of resources based on the assignment of data classification schemes to resources and clearance levels to users.

    a. True
    b. False

Chapter 6 Study Guide

30. The screened subnet protects the DMZ systems and information from outside threats by providing a network with intermediate security, which means the network is less secure as the general public networks but more secure than the internal network.

a. True

b. False

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

31. In SESAME, the user is first authenticated to an authentication server and receives a token. The token is then presented to a privilege attribute server as proof of identity to gain a(n) __________.

a. VPN b. ECMA

c. ticket d. PAC

32. The __________ is an intermediate area between a trusted network and an untrusted network.

a. perimeter b. DMZ

c. domain d. firewall

33. Telnet protocol packets usually go to TCP port __________ whereas SMTP packets go to port __________.

a. 23, 52 b. 80, 52

c. 80, 25 d. 23, 25

34. The service within Kerberos that generates and issues session keys is known as __________.

a. VPN b. KDC

c. AS d. TGS

35. Which of the following is not a major processing-mode category for firewalls?

a. Packet-Filtering Firewalls b. Application Gateways

c. Circuit Gateways d. Router Passthru

36. The dominant architecture used to secure network access today is the __________ firewall.

a. static b. bastion

c. unlimited d. screened subnet

37. In most common implementation models, the content filter has two components: __________.

a. encryption and decryption b. filtering and encoding

c. rating and decryption d. rating and filtering

38. __________ firewalls are designed to operate at the media access control sublayer of the data link layer of the OSI network model.

a. MAC layer b. Circuit gateway

c. Application gateways d. Packet filtering

39. Kerberos __________ provides tickets to clients who request services.

a. KDS b. TGS

c. AS d. VPN

Chapter 6 Study Guide

40. __________ filtering requires that the filtering rules governing how the firewall decides which packets are allowed and which are denied be developed and installed with the firewall.

a. Dynamic b. Static
c. Stateful d. Stateless

41. __________ access control is a form of __________ access control in which users are assigned a matrix of authorizations for particular areas of access.

a. lattice-based, discretionary b. arbor-based, nondiscretionary
c. arbor-based, discretionary d. lattice-based, nondiscretionary

42. __________ and TACACS are systems that authenticate the credentials of users who are trying to access an organization’s network via a dial-up connection.

a. RADIUS b. RADIAL
c. TUNMAN d. IPSEC

43. __________ firewalls examine every incoming packet header and can selectively filter packets based on header information such as destination address, source address, packet type, and other key information.

a. Packet-filtering b. Application gateways
c. Circuit gateways d. MAC layer firewalls

44. Which of the following version of TACACS is still in use?

a. TACACS b. Extended TACACS
c. TACACS+ d. All of the above

45. __________ is the protocol for handling TCP traffic through a proxy server.

a. SOCKS b. HTTPS
c. FTP d. Telnet

46. Known as the ping service, ICMP is a(n) __________ and should be ___________.

a. essential feature, turned on to save money b. common method for hacker reconnaissance, turned off to prevent snooping
c. infrequently used hacker tool, turned off to prevent snooping d. common method for hacker reconnaissance, turned on to save money

47. A(n) __________ is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.

a. SVPN b. VPN
c. SESAME d. KERBES

48. In __________ mode, the data within an IP packet is encrypted, but the header information is not.

a. tunnel b. transport
c. public d. symmetric

49. The application gateway is also known as a(n) __________.

a. application-level firewall b. client firewall
c. proxy firewall d. All of the above

Chapter 6 Study Guide

50. A __________ filtering firewall can react to an emergent event and update or create rules to deal with the event.

a. dynamic   b. static
c. stateful   d. stateless

51. Since the bastion host stands as a sole defender on the network perimeter, it is commonly referred to as the __________ host.

a. trusted   b. domain
c. DMZ   d. sacrificial

52. The restrictions most commonly implemented in packet-filtering firewalls are based on __________.

a. IP source and destination address
b. Direction (inbound or outbound)
c. TCP or UDP source and destination port requests
d. All of the above

53. The primary benefit of a VPN that uses _________ is that an intercepted packet reveals nothing about the true destination system.

a. intermediate mode   b. tunnel mode
c. reversion mode   d. transport mode

54. __________ inspection firewalls keep track of each network connection between internal and external systems.

a. Static   b. Dynamic
c. Stateful   d. Stateless

55. The proxy server is often placed in an unsecured area of the network or is placed in the __________ zone.

a. fully trusted   b. hot
c. demilitarized   d. cold