True/False

Indicate whether the statement is true or false.

1. Firewalls can be categorized by processing mode, phase of development, or structure.
2. A packet’s content is independent from the nature of the packet.
3. A Web server is often exposed to higher levels of risk when it is placed in the DMZ than when it is placed in the un-trusted network.
4. Circuit gateway firewalls usually look at data traffic flowing between one network and another.
5. A VPN allows a user to use the Internet as if it were a private network.
6. It is important that e-mail traffic reach your e-mail server and only your e-mail server.
7. Some firewalls can filter packets by the name of a particular protocol.
8. The screened subnet protects the DMZ systems and information from outside threats by providing a network of intermediate security.
9. All organizations with an Internet connection have some form of a router as the interface to the Internet at the DMZ between the organization’s internal networks and the external service provider.
10. There are limits to the level of configurability and protection that software firewalls can provide.
11. One method of protecting the residential user is to install a software firewall directly on the user’s system.
12. The SMC Barricade residential broadband router does not have an intrusion detection feature.
13. The Cisco security kernel contains three component technologies: the Interceptor/Packet Analyzer, the Security Verification ENgine (SVEN), and Kernel Proxies.
14. IDS responses can be classified as active or passive.
15. To determine which IDS would best meet the needs of a specific organization’s environment, first consider that environment, in technical, physical, and political terms.
16. All IDS vendors target users with the same levels of technical and security expertise.
17. Intrusion detection systems perform monitoring and analysis of system events and user behaviors.
18. A fully distributed IDS control strategy is the opposite of the centralized strategy.
19. An HIDS can detect many more types of attacks than a NIDS.
20. AppIDSs may be less susceptible to attack than other IDS approaches.
21. The statistical anomaly-based IDS collects statistical summaries by observing traffic that is known to be normal.
22. Nmap uses incrementing Time-To-Live packets to determine the path into a network as well as the default firewall policy.
23. A starting scanner is one that initiates traffic on the network in order to determine security holes.
24. 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.
25. A password is a series of characters from which a virtual password is derived.

**Modified True/False**
*Indicate whether the statement is true or false. If false, change the identified word or phrase to make the statement true.*

26. Address **grants** prohibit packets with certain addresses or partial addresses from passing through the device.

27. **SOHO** assigns non-routing local addresses to the computer systems in the local area network and uses the single ISP assigned address to communicate with the Internet.

28. When a dual-homed host approach is used, the bastion host contains **four** NICs.

29. A(n) **dual-homed** host probably has the ability to translate between many different protocols at their respective data link layers, including Ethernet, Token Ring, and Fiber Distributed Data Interface.

30. In a DMX configuration, connections into the trusted internal network are allowed only from the DMZ **bastion** host servers.

31. A(n) **perimeter** is a segment of the DMZ where additional authentication and authorization controls are put into place to provide services that are not available to the general public.

32. Most firewalls use packet **header** information to determine whether a specific packet should be allowed to pass through or should be dropped.

33. **Rings**, formally known as ICMP Echo requests, are used by internal systems administrators to ensure that clients and servers can reach and communicate.

34. The presence of external requests for **Telnet** services can indicate a potential attack.

35. **SESAME** may be obtained free of charge from MIT.

36. The popular use for **tunnel** mode VPNs is the end-to-end transport of encrypted data.

37. Alarm **filtering** is alarm clustering that is based on frequency, similarity in attack signature, similarity in attack target, or other similarities.

38. A(n) **server-based** version is focused on protecting the server or host’s information assets.

39. In the process of protocol **application** verification, the NIDSs look for invalid data packets.

40. Preconfigured, predetermined attack patterns are called **signatures**.

41. A(n) **log** file monitor is an approach to IDS that is similar to the NIDS.

42. A(n) **partially** distributed IDS control strategy, combines the best of the other two strategies.

43. A combination of **attractants** is meant to lure potential attackers into committing an attack.

44. A padded cell is a hardened **honey net**.
45. Enticement is the action of luring an individual into committing a crime to get a conviction.

46. For Linux or BSD systems, there is a tool called “scanner” that allows a remote individual to “mirror” entire Web sites.

47. Port fingers are tools used by both attackers and defenders to identify (or fingerprint) the computers that are active on a network, as well as the ports and services active on those computers, the functions and roles the machines are fulfilling, and other useful information.

48. A(n) port is a network channel or connection point in a data communications system.

49. When a prospective user, referred to in the area of access control as a(n) supplicant, seeks to use a protected system, logically access a protected service, or physically enter a protected space, he or she must engage in authentication and authorization activities to establish his or her identity and verify that he or she has permission to complete the requested activity.

50. The false detect rate is the percentage of or value associated with the rate at which supplicants who are not legitimate users are allowed access to systems or areas as a result of a failure in the biometric device.

Multiple Choice

Identify the choice that best completes the statement or answers the question.

51. _____ 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    c. Circuit gateways
   b. Application gateways d. MAC layer firewalls

52. _____ filtering requires that the filtering rules governing how the firewall decides which packets are allowed and which are denied are developed and installed.
   a. Dynamic    c. Stateful
   b. Static    d. Stateless

53. _____ firewalls keep track of each network connection between internal and external systems.
   a. Static    c. Stateful
   b. Dynamic    d. Stateless

54. The application gateway is also known as a(n) _____.
   a. application-level firewall    c. proxy firewall
   b. client firewall    d. All of the above

55. _____ firewalls are designed to operate at the media access control layer of the OSI network mode.
   a. MAC layer    c. Application gateways
   b. Circuit gateway    d. Packet filtering

56. ISA can use _____ technology.
   a. PNP    c. RAS
   b. Point to Point Tunneling Protocol    d. All of the above

57. _____ generates and issues session keys.
   a. VPN    c. AS
   b. KDC    d. TGS

58. Kerberos _____ provides tickets to clients who request services.
   a. KDS    c. AS
   b. TGS    d. VPN
59. Which of the following is a valid version of TACACS?
   a. TACACS  
   b. Extended TACACS  
   c. TACACS+  
   d. All of the above

60. 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

61. Telnet protocol packets usually go to TCP port ____.
   a. 7  
   b. 8  
   c. 14  
   d. 23

62. The dominant architecture used to secure network access today in large organizations is the ____ firewall.
   a. static  
   b. bastion  
   c. unlimited  
   d. screened subnet

63. In recent years, the broadband router devices that can function as packet filtering firewalls have been enhanced to combine the features of ____.
   a. UDPs  
   b. MACs  
   c. WANs  
   d. WAPs

64. A(n) ____ IDS is focused on protecting network information assets.
   a. network-based  
   b. host-based  
   c. application-based  
   d. server-based

65. ____ benchmark and monitor the status of key system files and detect when an intruder creates, modifies, or deletes monitored files.
   a. NIDSs  
   b. HIDSs  
   c. AppIDSs  
   d. SIDSs

66. Using _____, the system reviews the log files generated by servers, network devices, and even other IDSs.
   a. LFM  
   b. stat IDS  
   c. AppIDS  
   d. HIDS

67. Each TCP session consists of a(n) ____.
   a. FIN packet, a series of data, and ACK packets  
   b. SYN packet, a series of data, and FIN packets  
   c. SYN packet, and ACK packets  
   d. SYN packet, a series of data, and ACK packets

68. IDS researchers have used padded cell and honey pot systems since the late ____.
   a. 1960s  
   b. 1970s  
   c. 1980s  
   d. 1990s

69. An extension of the attractant-based technologies in the preceding section, trap and trace applications are growing in popularity. These systems are often simply referred to as ____.
   a. trace and treat  
   b. trap and trace  
   c. treat and trap  
   d. trace and clip

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

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

72. ____ 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
73. _____ is the validation of a supplicant’s identity.
   a. Authentication  c. Password
   b. Authorization   d. Passphrase

74. Once _____ tokens are synchronized with a server, both devices (server and token) use the same time or a
time-based database to generate a number that is displayed and entered during the user login phase.
   a. synchronous  c. symmetric
   b. asynchronous  d. asymmetric

75. The _____ is the level at which the number of false rejections equals the false acceptances, also known as the
equal error rate.
   a. BIOM  c. IIS
   b. REC   d. CER

Completion
Complete each statement.

76. A(n) ____________________ is an information security program that prevents specific types of information
    from moving between the outside world and the inside world.

77. A packet ____________________ firewall installed on a TCP/IP based network typically functions at the IP
    level and determines whether to drop a packet (deny) or forward it to the next network connection (allow)
    based on the rules programmed into the firewall.

78. The application firewall is also known as a(n) ____________________ server.

79. ____________________ firewalls combine the elements of other types of firewalls — that is, the elements of
    packet filtering and proxy services, or of packet filtering and circuit gateways.

80. Because the bastion host stands as a sole defender on the network perimeter, it is also commonly referred to
    as the ____________________ host.

81. ____________________ is the protocol for handling TCP traffic through a proxy server.

82. The firewall device is never accessible directly from the ____________________ network.

83. A(n) ____________________ filter is a software filter — technically not a firewall — that allows
    administrators to restrict access to content from within a network.

84. The Remote ____________________ Dial-In User Service) system centralizes the management of user
    authentication by placing the responsibility for authenticating each user in the central RADIUS server.

85. ____________________ authentication system is named after the three-headed dog of Greek mythology,
    which guarded the gates to the underworld.

86. In Kerberos a(n) ____________________ is an identification card for a particular client that verifies to the
    server that the client is requesting services and that the client is a valid member of the Kerberos system and
    therefore authorized to receive services.

87. The Secure European System for Applications in a(n) ____________________ Environment is the result of a
    European research and development project partly funded by the European Commission.

88. A(n) ____________________ Private Network is a private and secure network connection between systems
    that uses the data communication capability of an unsecured and public network.

89. Content filters are often called ____________________ firewalls.

90. SESAME uses ____________________ key encryption to distribute secret keys.
91. The ongoing activity from alarm events that are accurate and noteworthy but not necessarily significant as potentially successful attacks is called the ____________________.

92. The ____________________ port is also known as a switched port analysis port or mirror port.

93. HIDSs are also known as system ____________________ verifiers.

94. The ____________________-based IDS examines an application for abnormal events.

95. When a collection of honey pots connects several honey pot systems on a subnet, it may be called a(n) ____________________.

96. ____________________ is the process of attracting attention to a system by placing tantalizing bits of information in key locations.

97. The attack ____________________ is a series of steps or processes used by an attacker, in a logical sequence, to launch an attack against a target system or network.

98. Nmap is a utility that performs ____________________ scanning.

99. A token called a(n) ____________________ card contains a computer chip that can verify and validate a number of pieces of information instead of just a PIN.

100. The ____________________ error rate is the level at which the number of false rejections equals the false acceptances, also known as the equal error rate.
Study Guide_Info Security
Answer Section

TRUE/FALSE

1. ANS: T  PTS: 1  REF: 241
2. ANS: F  PTS: 1  REF: 243
3. ANS: F  PTS: 1  REF: 246
4. ANS: F  PTS: 1  REF: 246
5. ANS: T  PTS: 1  REF: 274
6. ANS: T  PTS: 1  REF: 264
7. ANS: T  PTS: 1  REF: 262
8. ANS: T  PTS: 1  REF: 259
9. ANS: F  PTS: 1  REF: 256
10. ANS: T  PTS: 1  REF: 255
11. ANS: T  PTS: 1  REF: 254
12. ANS: F  PTS: 1  REF: 252
13. ANS: T  PTS: 1  REF: 248
14. ANS: T  PTS: 1  REF: 297
15. ANS: T  PTS: 1  REF: 300
16. ANS: F  PTS: 1  REF: 303
17. ANS: T  PTS: 1  REF: 304
18. ANS: T  PTS: 1  REF: 307
19. ANS: F  PTS: 1  REF: 289
20. ANS: F  PTS: 1  REF: 295
21. ANS: T  PTS: 1  REF: 296
22. ANS: F  PTS: 1  REF: 322
23. ANS: F  PTS: 1  REF: 323
24. ANS: T  PTS: 1  REF: 327
25. ANS: F  PTS: 1  REF: 333

MODIFIED TRUE/FALSE

26. ANS: F, restrictions

   PTS: 1  REF: 243

27. ANS: F, NAT

   PTS: 1  REF: 249

28. ANS: F

   two
   2

   PTS: 1  REF: 257

29. ANS: T  PTS: 1  REF: 258
30. ANS: T  PTS: 1  REF: 259
31. ANS: F, extranet
   PTS: 1     REF: 259

32. ANS: T
   PTS: 1     REF: 262

33. ANS: F, Pings
   PTS: 1     REF: 265

34. ANS: T
   PTS: 1     REF: 265

35. ANS: F, Kerberos
   PTS: 1     REF: 273

36. ANS: F, transport
   PTS: 1     REF: 275

37. ANS: F, compaction
   PTS: 1     REF: 286

38. ANS: F, host-based
   PTS: 1     REF: 288

39. ANS: F, stack
   PTS: 1     REF: 290

40. ANS: T
    PTS: 1     REF: 295

41. ANS: T
    PTS: 1     REF: 296

42. ANS: T
    PTS: 1     REF: 308

43. ANS: T
    PTS: 1     REF: 314

44. ANS: F, pot
   PTS: 1     REF: 315

45. ANS: F, Entrapment
   PTS: 1     REF: 317

46. ANS: F, wget
   PTS: 1     REF: 319

47. ANS: F, scanners
   PTS: 1     REF: 320

48. ANS: T
    PTS: 1     REF: 321

49. ANS: T
    PTS: 1     REF: 332

50. ANS: F, accept
    PTS: 1     REF: 335

MULTIPLE CHOICE

51. ANS: A     PTS: 1     REF: 242
<table>
<thead>
<tr>
<th>ANS</th>
<th>PTS</th>
<th>REF</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>1</td>
<td>244</td>
</tr>
<tr>
<td>C</td>
<td>1</td>
<td>245</td>
</tr>
<tr>
<td>A</td>
<td>1</td>
<td>245</td>
</tr>
<tr>
<td>A</td>
<td>1</td>
<td>246</td>
</tr>
<tr>
<td>B</td>
<td>1</td>
<td>276</td>
</tr>
<tr>
<td>B</td>
<td>1</td>
<td>272</td>
</tr>
<tr>
<td>A</td>
<td>1</td>
<td>271</td>
</tr>
<tr>
<td>D</td>
<td>1</td>
<td>268</td>
</tr>
<tr>
<td>D</td>
<td>1</td>
<td>263</td>
</tr>
<tr>
<td>D</td>
<td>1</td>
<td>258</td>
</tr>
<tr>
<td>A</td>
<td>1</td>
<td>249</td>
</tr>
<tr>
<td>A</td>
<td>1</td>
<td>288</td>
</tr>
<tr>
<td>B</td>
<td>1</td>
<td>290-291</td>
</tr>
<tr>
<td>A</td>
<td>1</td>
<td>296</td>
</tr>
<tr>
<td>D</td>
<td>1</td>
<td>313</td>
</tr>
<tr>
<td>C</td>
<td>1</td>
<td>315</td>
</tr>
<tr>
<td>B</td>
<td>1</td>
<td>316</td>
</tr>
<tr>
<td>A</td>
<td>1</td>
<td>317</td>
</tr>
<tr>
<td>A</td>
<td>1</td>
<td>321</td>
</tr>
<tr>
<td>B</td>
<td>1</td>
<td>324</td>
</tr>
<tr>
<td>A</td>
<td>1</td>
<td>332</td>
</tr>
<tr>
<td>A</td>
<td>1</td>
<td>333</td>
</tr>
<tr>
<td>D</td>
<td>1</td>
<td>335</td>
</tr>
</tbody>
</table>

**COMPLETION**

76. ANS: firewall

    PTS: 1 REF: 241
77. ANS: filtering

    PTS: 1 REF: 242
78. ANS: proxy

    PTS: 1 REF: 245
79. ANS: Hybrid

    PTS: 1 REF: 247
80. ANS: sacrificial

    PTS: 1 REF: 256
81. ANS: SOCKS

    PTS: 1 REF: 259
82. ANS: public
untrusted

PTS: 1  REF: 264
83. ANS: content

PTS: 1  REF: 268
84. ANS: Authentication

PTS: 1  REF: 270
85. ANS: Kerberos

PTS: 1  REF: 271
86. ANS: ticket

PTS: 1  REF: 272
87. ANS: Multivendor

PTS: 1  REF: 273
88. ANS: Virtual

PTS: 1  REF: 274
89. ANS: reverse

PTS: 1  REF: 268
90. ANS: public

PTS: 1  REF: 273
91. ANS: noise

PTS: 1  REF: 285
92. ANS: monitoring

PTS: 1  REF: 289
93. ANS: integrity

PTS: 1  REF: 291
94. ANS: application

PTS: 1  REF: 294
95. ANS: honey net honeynet

PTS: 1  REF: 314
96. ANS: Enticement

PTS: 1  REF: 317
97. ANS: protocol
<table>
<thead>
<tr>
<th>PTS</th>
<th>REF</th>
<th>ANS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>318</td>
<td>Idle</td>
</tr>
<tr>
<td>1</td>
<td>322</td>
<td>smart</td>
</tr>
<tr>
<td>1</td>
<td>333</td>
<td>crossover</td>
</tr>
<tr>
<td>1</td>
<td>335</td>
<td></td>
</tr>
</tbody>
</table>