Study Guide_Info Security

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
b. Application gateways
c. Circuit 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
b. Static
c. Stateful
d. Stateless

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

____ 54. The application gateway is also known as a(n) ____.
a. application-level firewall
b. client firewall
c. proxy 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
b. Circuit gateway
c. Application gateways
d. Packet filtering

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

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

____ 58. Kerberos ____ provides tickets to clients who request services.
a. KDS
b. TGS
c. AS
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
b. Authorization
c. Password
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
b. asynchronous
c. symmetric
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
b. REC
c. IIS
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

52. ANS: B PTS: 1 REF: 244
53. ANS: C PTS: 1 REF: 245
54. ANS: A PTS: 1 REF: 245
55. ANS: A PTS: 1 REF: 246
56. ANS: B PTS: 1 REF: 276
57. ANS: B PTS: 1 REF: 272
58. ANS: B PTS: 1 REF: 272
59. ANS: D PTS: 1 REF: 271
60. ANS: D PTS: 1 REF: 268
61. ANS: D PTS: 1 REF: 263
62. ANS: D PTS: 1 REF: 258
63. ANS: D PTS: 1 REF: 249
64. ANS: A PTS: 1 REF: 288
65. ANS: B PTS: 1 REF: 290-291
66. ANS: A PTS: 1 REF: 296
67. ANS: D PTS: 1 REF: 313
68. ANS: C PTS: 1 REF: 315
69. ANS: B PTS: 1 REF: 316
70. ANS: A PTS: 1 REF: 317
71. ANS: A PTS: 1 REF: 321
72. ANS: B PTS: 1 REF: 324
73. ANS: A PTS: 1 REF: 332
74. ANS: A PTS: 1 REF: 333
75. ANS: D PTS: 1 REF: 335

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

PTS: 1 REF: 318

98. ANS: Idle

PTS: 1 REF: 322

99. ANS: smart

PTS: 1 REF: 333

100. ANS: crossover

PTS: 1 REF: 335